Amstutz Jonas BJ

Von: Kohler Muster Isabel - RE SO <Isabel.Kohler@santesuisse.ch>
Gesendet: Dienstag, 4. April 2017 15:08
An: Amstutz Jonas BJ
Cc: Dubois Camille BJ; Bacher Bettina BJ; Füzesséry-Minelli Simone
Betreff: Revision des DSG; Stellungnahme santésuisse, Die Schweizer Krankenversicherer
Anlagen: Stellungnahme_santésuisse_Totalrevision_DSG_2017-03-27 _Original_definitiv.docx

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zum revidierten DSG Stellung nehmen zu können.

Gerne lassen wir Ihnen im Anhang die Stellungnahme von santésuisse zukommen mit der Bitte um Berücksichtigung unserer Anliegen und Anmerkungen.

Sehr gerne stehen wir Ihnen für Fragen zur Verfügung. Besten Dank und

Freundliche Grüsse

Isabel Kohler Muster

_____

santésuisse
Die Schweizer Krankenversicherer
Isabel Kohler Muster
Rechtsdienst
Leiterin Rechtsdienst
lic. iur., Fürsprecherin
Römerstrasse 20
4502 Solothurn

Tel. +41 32 625 4131
Fax +41 32 625 41 51
Isabel.Kohler@santesuisse.ch
www.santesuisse.ch
Blog: www.monsieur-sante.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : **santésuisse, Die Schweizer Krankenversicherer**

Abkürzung der Firma / Organisation :

Adresse : Römerstrasse 20, 4502 Solothurn

Kontaktperson : Isabel Kohler Muster

Telefon : 032 625 41 31

E-Mail : isabel.kohler@santesuisse.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	santésuisse stellt fest, • dass die vorliegende Revision vor allem aufgrund der Entwicklungen im Datenschutzrecht auf Ebene Europarat und Europäische Union eingeleitet wurde und nicht, weil der Datenschutz in der Schweiz mangelhaft geregelt ist; • dass der Entwurf vor allem neue Formulierungen und Begriffe aus dem Europäischen Raum übernimmt, inhaltlich jedoch mit ein paar Ausnahmen im Vergleich zum bisherigen Recht keine massgebenden Neuerungen bringt *(z.B. im Bereich der Einwilligung wird nur wiederholt, was bis heute schon gilt; ebenfalls bleibt das bisherige Regelungskonzept mit den Bearbeitungsgrundsätzen bestehen);* • dass die schweizerische Revision sogar über die scheinbar notwendigen Anpassungen aus dem EU-Raum hinausgeht *(z.B. die Data Breach Notifications oder die strengen strafrechtlichen Sanktionsbestimmungen, welche sogar fahrlässige Verstösse von Mitarbeitenden gegen das DSG unter Strafe stellen)*; • dass sich die Krankenversicherer nicht sehr gut im revidierten Datenschutzgesetz wiederfinden und deshalb davon ausgegangen werden muss, dass keine umfassende Koordination hin zum KVG/VVG stattgefunden hat *(z.B. die Abgrenzung zur DSGVO wenn Schweizer Krankenversicherer Daten von Personen in der EU bearbeiten und damit zugleich auch der Aufsicht der nationalen EU-Datenschutzbehörden unterstehen);* • dass die revidierten Bestimmungen für die Krankenversicherer (erneut) grossen administrativen Mehraufwand bringen ohne konkreten Nutzen für den Versicherungsnehmer mit Blick auf den heutigen Datenschutz *(z.B. die Bestimmungen über den Auslandtransfer oder die Bestimmungen über die Datenschutz-Folgenabschätzungen)*; • dass der vorgegebene Zeitdruck zur Revision (frühestes Inkrafttreten Gesetz und Verordnung wohl erst per 1.1.2019) eine parallele Erarbeitung der Ausführungsbestimmungen zu den parlamentarischen Beratungen (schätzungsweise vom Herbst 2017 bis Herbst 2018) bedingen würde, wodurch zahlreiche der revidierten Bestimmungen gesetzgeberisch legitimiert werden müssten, ohne dass hierzu Klarheit hinsichtlich der konkreten Umsetzung herrscht, was zu zahlreichen Umsetzungsfragen und –problemen führen wird *(z.B. unklare erweiterte Informations- und Aufklärungspflichten, welche bei Nichtbefolgung strafrechtlich scharf sanktioniert werden, oder die Regeln zur automatisierten Einzelfallentscheidung, im Rahmen derer nicht geklärt ist, über was genau alles zu informieren ist; weiter das neue Institut der „good practice" als Soft Law).*

	Insgesamt entsteht der Eindruck, dass die Schweiz unter Zugzwang das Datenschutzgesetz revidiert ohne die vorgeschlagenen Anpassungen für die konkrete Umsetzung genau reflektiert zu haben. Dies ist gefährlich und kann das eh schon stark reglementierte Krankenversicherungswesen in der Erfüllung seiner gesetzlich statuierten Aufgaben (noch mehr) lähmen. **Fazit:** **santésuisse lehnt die Revision des Datenschutzgesetzes in der vorliegenden Form ab.** **santésuisse befürwortet eine für die Gesetzesanwender klare und durchdachte Revision in denjenigen Bereichen, welche aufgrund der Europäischen Vorgaben für die Schweiz zwingend sind, d.h. ohne die die Schweiz gewichtige Nachteile vor allem im wirtschaftlichen grenzüberschreitenden Geschäftsverkehr erleiden würde.** Im Detail siehe nachfolgend:

Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE DSG) und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
	VE DSG	4	3		<u>Datenbearbeitungsgrundsätze:</u> Gemäss Abs. 3 dürfen Daten nur so bearbeitet werden, als dies mit dem Zweck zu vereinbaren ist. D.h., dass die Weiterbearbeitung aus Sicht der betroffenen Person *„nicht berechtigterweise als unerwartet, unangebracht oder beanstandbar erscheinen kann“.* Diese Bestimmung darf nicht dazu führen, dass die Krankenversicherer von der Aufsichtsbehörde einfach zu Datenlieferungen verpflichtet werden können, sofern eine solche Lieferung nicht berechtigterweise als unterwartet, unangebracht oder beanstandbar aus Sicht der betroffenen Person erscheinen kann. Der Entscheid, was gestützt auf diese Bestimmung aus Sicht der betroffenen Person nicht berechtigterweise als unerwartet, unangebracht oder beanstandbar erscheinen kann, muss deshalb in der Kompetenz der Krankenversicherer stehen. Denn nur so stimmt Kompetenz und Verantwortung überein. Bestraft werden bei Datenschutzverletzungen nämlich die Krankenversicherer, welche diese Datenbearbeitung (Weiterbearbeitung) vorgenommen haben und nicht z.B. die Aufsichtsbehörde, welche diese Daten eingefordert hat. **Die Bestimmung ist dahingehend zu präzisieren.**
	s.o.	5	3	c und d jeweils Ziff. 1	<u>Bekanntgabe ins Ausland:</u> Gemäss dieser Bestimmung dürfen die Krankenversicherer Personendaten nur dann ins Ausland bekannt geben, wenn ein geeigneter Schutz gewährleistet ist u.a. durch standardisierte Garantien, insbesondere durch Vertrag (lit. c) oder verbindliche unternehmensinterne Datenschutzvorschriften (lit. d), welche der Datenschutzbeauftragte vorgängig genehmigt hat. Das Verfahren zur Genehmigung durch den Datenschutzbeauftragten kann gemäss den neuen Vorschriften bis zu 6 Monaten dauern, wobei die Frist erst mit Zustellung der vollständigen Unterlagen zu laufen beginnt, wodurch es auch länger als 6 Monate gehen kann.

					Die Krankenversicherer bezweifeln, dass diese lange Frist „geschäftsfördernd“ ist. Es besteht die grosse Gefahr, dass dadurch nicht standardisierte Datenexportverträge in der Praxis völlig unattraktiv werden, da die Auftragsbearbeiter im Ausland nicht bis zu einem halben Jahr oder noch länger warten werden bis sie den Auftrag ausführen können. **Die Frist ist deshalb zu kürzen auf 30 Tage, wie dies für die verbindlich unternehmensinternen Datenschutzvorschriften bis anhin der Fall war.**
	s.o.	6	2		<u>Bekanntgabe von Personendaten ins Ausland in Ausnahmefällen:</u> Der Verantwortliche oder der Auftragsbearbeiter müssen neu dem Beauftragten mitteilen, wenn sie Personendaten nach Abs. 1 lit. b, c und d ausnahmsweise ins Ausland bekannt geben. Dazu gehören auch Fälle, in denen der Export durch Vertragsabschluss oder Vertragserfüllung oder ein ausländisches Rechtsverfahren gerechtfertigt wird. Die Krankenversicherer sind mit dieser Informationspflicht nicht einverstanden, denn unter Umständen müssen die Krankenversicherer dadurch sensible Geschäftsgeheimnisse preisgeben, wozu es absolut keinen Grund gibt. Zudem ist fraglich, was der Datenschutzverantwortliche mit all diesen Informationen will, geschweige denn dass er diese vernünftig bearbeiten kann.
	s.o.	8 und 9			<u>Empfehlungen der guten Praxis („good practice“) sowie deren Einhaltung</u> Der Datenschutzbeauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren (Abs. 1). Der Verantwortliche oder interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen (Abs. 2). Die Empfehlungen werden veröffentlicht (Abs. 3). **Dieses schweizerisch neuartige „Institut“ lehnen die Krankenversicherer in der vorliegenden Form ab**. Es sind zu viele Unklarheiten und Nachteile damit verbunden. Es stellt sich die Frage, wie der Prozess hier genau laufen soll? Gemäss Gesetzesvorschlag sollen „interessierte Kreise“ solche Empfehlungen ausarbeiten können und zur Genehmigung eingeben. Die vorgeschlagene Formulierung lässt zu, dass irgendwelche „interessierten“ Kreise für andere Betroffene solche Empfehlungen ausarbeiten könnten, obschon sie selber gar nicht betroffen sind und der Bedarf nach solchen

					Empfehlungen für die Betroffenen gar nicht vorhanden ist. Dies kann zu absurden Konstellationen führen. Beispielsweise kann ein Krankenversicherer für die Versicherungsbranche Empfehlungen aus seiner Optik ausarbeiten und genehmigen lassen. Hält er sich an die vom Datenschutzbeauftragen genehmigte Empfehlung, gilt sie fortan als „soft law" für alle Krankenversicherer, obschon nicht jede Versicherungsgesellschaft die gleiche Unternehmensstruktur bzw. –organisation hat. Zwischen kleinen/mittleren Krankenversicherer und grossen gibt es bedeutende Unterschiede, denen individuell, d.h. nach dem Kriterium der Grösse Rechnung zu tragen ist. Sie können nicht in einen Topf geworfen werden. Rechtsunsicherheiten sind vorprogrammiert. „Soft law" ist hier fehl am Platz und es fehlt am rechtsstaatlich korrekten Rechtsetzungsprozess zwecks Akzeptanz durch die direkt Betroffenen. Es gibt nicht einmal die Möglichkeit sich gegen solche „genehmigten" Empfehlungen, die durchaus materiellen Charakter haben, wehren zu können. Es ist kein Beschwerderecht der Betroffenen vorgesehen. Über die Geltung von Empfehlungen sollte wenn schon eine neutrale Stelle, zusammengesetzt aus Vertretern aus der Praxis, urteilen und nicht der Datenschutzbeauftragte selber. **Die Bestimmungen zur Good practice sind deshalb gänzlich zu streichen.** **Sollte diesem Streichungsantrag nicht nachgekommen werden, dann sind die Bestimmungen wie folgt anzupassen:** ***Art. 8 Abs. 1:*** ***Der Beauftragte erarbeitet nicht bindende Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die betroffenen Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs.*** ***Art. 8 Abs. 2:*** ***Die Verantwortlichen sowie die interessierten Kreise können ihre eigenen Empfehlungen ausarbeiten. Sie können diese dem Beauftragten zur Konsultation vorlegen.*** *Art. 8 Abs. 3 ist zu streichen!* *Art. 9 ist ebenfalls zu streichen!*
	s.o.	10			Zertifizierung:

					Die Krankenversicherer befürworten die Möglichkeit, dass auch nur einzelne Teile wie Datenbearbeitungssysteme, Produkte und Dienstleistungen zertifiziert werden können. Wichtig ist, dass keine Zertifizierungspflicht besteht, sondern bloss eine fakultative Möglichkeit zur Zertifizierung. Damit eine abschliessende Beurteilung vorgenommen werden kann, fehlen jedoch die klärenden Ausführungsbestimmungen, erwähnt in Abs. 2.
	s.o.	12	1	a	<u>Daten einer verstorbenen Person:</u> **Lit. a ist zu streichen und an Stelle die bisherige Bestimmung wieder aufzunehmen!** Diese Bestimmung ist durch die Krankenversicherer nicht umsetzbar. Die Krankenversicherer erhalten die Information, dass eine verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat, nicht bzw. nicht automatisch. Sie haben davon in den meisten Fällen gar keine Kenntnisse. Die bisherige sehr wichtige, praxistaugliche und für die Krankenversicherer gut umsetzbare gesetzliche Vermutung/Fiktion ist wichtig für die Krankenversicherer und stehen zu lassen.
	s.o.	12	2		**Abs. 2 ist zu streichen!** Diesen Absatz braucht es nicht. Die Krankenversicherer machen die Prüfung, ob keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen bereits im Rahmen der Prüfung des schutzwürdigen Interesses nach Absatz 1. Auch die Definition, wann ein schutzwürdiges Interesse gegeben ist, bringt nichts für die Umsetzung, denn das Problem bei den eingesetzten Erben und somit die Unklarheit besteht weiterhin. Sollte Abs. 2 entgegen dem Willen der Krankenversicherer trotzdem stehen bleiben, muss zumindest die gesetzliche Vermutung des schutzwürdigen Interesses rausgestrichen werden.
	s.o.	13	3 und 4		<u>Informationspflicht bei der Beschaffung von Personendaten:</u> **Die Informationspflichten gemäss Abs. 3 und 4 gehen zu weit und sind zu streichen**! Diese sind durch die Krankenversicherer nicht oder äusserst schwerlich umsetzbar und ziehen einen riesigen administrativen Mehraufwand nach sich, der in keinem Verhältnis zum eigentlichen Zweck der Tätigkeit

					der Krankenversicherer steht. (Z.B. beim Wechsel im Fall von Outsourcing-Verträge im Unfallversicherungsgeschäft).
	s.o.	13	5		Werden die Daten nicht gespeichert, muss die betroffene Person spätestens bei der ersten Bekanntgabe an Dritte informiert werden. Das Gesetz geht hier lediglich von elektronischen Daten aus. Was ist mit Daten auf Papier? Muss dann nicht informiert werden? Überdies müsste die Person z.B. bei jeder Akteneinsicht informiert werden. Ist dies sinnvoll und so gewollt? **Die Bestimmung ist unklar und schlecht umsetzbar und deshalb zu streichen.**
	s.o.	15	1		<u>Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung</u>: Es ist unklar, ob nun alle eingeführten Systeme zur automatisierten Abrechnung unter „automatisierte Datenbearbeitung“ fallen. Falls ja, dann müssten die Krankenversicherer jedes Mal, wenn sie solche Daten bearbeiten, die betroffene Person informieren. Das kann nicht der Zweck dieser Bestimmung sein. **Sie ist deshalb zu konkretisieren.**
	s.o.	15	2		Möglichkeit der betroffenen Person, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern. Diese Bestimmung, welche die Krankenversicherer vorwiegend im VVG-Bereich betrifft, ist völlig uferlos und nicht im Sinne des Versicherungsnehmers. **Sie geht zudem über die Verpflichtung im Übereinkommen SEV 108 hinaus.** Sie kann unter Umständen für den Versicherungsnehmer zu hohen Kosten führen und den Krankenversicherer in seinen Abläufen lähmen und hemmen. Dieses „menschliche rechtliche Gehör“ wird dazu führen, dass der Krankenversicherer die damit einhergehenden Kosten aufgrund der enormen Zusatzaufwendungen auf den Versicherungsnehmer überwälzen wird, was sich in der Prämie niederschlagen wird. Ebenfalls ist nicht klar, über was alles zu informieren ist. Hier benötigt es Präzisierungen. Sind davon ebenfalls die für den automatisierten Einzelentscheid bearbeiteten Personendaten gemeint, wird die Umsetzung dieser Bestimmung uferlos. Solche Angaben sind lediglich auf Rückfrage zu liefern.

					Diese Bestimmung ist zu präzisieren bzw. an die Bestimmung im Übereinkommen SEV 108 anzupassen.
	s.o.	16	1		Vorgängige Datenschutz-Folgenabschätzung bei erhöhtem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person: Was bedeutet „erhöhtes Risiko“? Sind z.B. besonders schützenswerte Daten ein Risiko? Falls dies der Fall ist, dann müssten die Krankenversicherer diese Folgenabschätzungen bei jedem einzelnen Fall durchführen. Diese würde 80% der Tätigkeiten der Krankenversicherer betreffen und das System völlig lahmlegen. **Die Bestimmung muss zwingend präzisiert und angepasst werden.**
	s.o.	16	3 und 4		Benachrichtigung des Datenschutzbeauftragten über jedes einzelne Ergebnis der Datenschutz-Folgenabschätzung: **Diese Bestimmungen in Abs. 3 und 4 gehen zu weit und sind nicht umsetzbar. Sie sind deshalb zu streichen!** Zudem wird der Datenschutzbeauftragte niemals die vorgesehene Frist von 3 Monaten einhalten können, womit der Krankenversicherer in seinen Abläufen und Tätigkeiten völlig gelähmt ist.
	s.o.	17	1		Meldung von Verletzungen des Datenschutzes: **Diese Bestimmung ist rechtlich überflüssig,** da sie sich bereits aus der korrekten Anwendung des Bearbeitungsgrundsatzes ergibt, wonach im Rahmen einer Datenbearbeitung jeweils angemessene technische und organisatorische Massnahmen zu treffen sind, um eine unbefugte Datenbearbeitung zu verhindern **und ist deshalb zu streichen.** Zudem ist die Formulierung unklar, sodass das Risiko besteht, dass alles gemeldet werden muss. Wenn überhaupt, dann sind lediglich „Datenunfälle“ zu melden bzw. Verletzungen des Datenschutzes, die erhebliche Risiken mit sich bringen.
	s.o.	19		a	Weitere Pflichten; Dokumentation der Datenbearbeitung: Es ist nicht klar, was genau mit „Dokumentation der *Datenbearbeitung*“ gemeint ist. Bevor hierzu keine Klarheit herrscht, kann nicht zugestimmt werden. Im bisherigen Gesetz wurde von „Datensammlung“ gesprochen (vgl. Art. 11a DSG). Art. 11a DSG wird mit VE DSG gestrichen. **Es ist genau zu klären,**

					was die neue Begrifflichkeit mitumfasst sowie bei Anpassung eine solche bezüglich aller Bestimmungen im VE DSG zu machen (vgl. z.B. Art. 20, 36).
	s.o.	19		b	Diese Informationspflicht geht viel zu weit und kann nicht umgesetzt werden, weshalb sie zu streichen ist.
	s.o.	20	2		Auskunftsrecht: **Für diese Auskunftspflicht müssen in der Verordnung zwingend Ausnahmen formuliert werden, wenn der Umfang zu gross wird**. **Zudem muss dieses jederzeitige Auskunftsrecht der betroffenen Person kostenpflichtig bleiben für spezielle Fälle wie bis anhin**. Die heute geltende Regelung für Ausnahmen der Kostenlosigkeit ist sinnvoll, erfolgsbringend und deshalb zwingend zu übernehmen. Angesprochen sind Fälle mit besonders grossem Arbeitsaufwand sowie querulatorische Anfragen. Die maximale Kostenbeteiligung kann weiterhin bei CHF 300.- liegen (vgl. Art. 2 VDSG).
	s.o.	20	3		**Diese Bestimmung ist zu streichen!** Sie beschränkt auf unverhältnismässige Weise die Autonomie bzw. die Wirtschaftsfreiheit der Krankenversicherer und kann zu Verletzungen von Geschäftsgeheimnissen führen. Sollte diese Bestimmung trotzdem nicht gestrichen werden, ist zumindest eine Koordination zu Art. 19 lit. a vorzunehmen.
	s.o.	21	1		Einschränkung des Auskunftsrechts: Gemäss dieser Bestimmung müssen die Krankenversicherer als Bundesorgane z.B. gegenüber Leistungserbringern wie Ärzten eine anfechtbare Verfügung erlassen. Ist dies die Meinung des Gesetzgebers?
	s.o.	36	1		Register: **Dieser Abs. 1, wonach dem Datenschutzbeauftragten sämtliche „Datenbearbeitungstätigkeiten“ zu melden sind, ist zu streichen**, da völlig uferlos. Zudem ist nicht klar, was genau unter

					„Datenbearbeitungstätigkeiten“ zu verstehen ist (vgl. hierzu unsere Anmerkungen zu Art. 19 lit. a oben). Diese Meldungen interessieren den Datenschutzbeauftragten gar nicht. Bis anhin mussten lediglich „Sammlungen“ gemeldet werden und nicht jegliche Tätigkeiten (vgl. Kommentierung zu Art. 19 lit. a oben). Was will der Datenschutzbeauftragte denn mit all diesen Daten machen? Der bisherige Art. 11a DSG beinhaltete in Abs. 5 lit. e rechtssetzungssystematisch korrekt eine Ausnahme der Anmeldung von Datensammlungen beim Datenschutzbeauftragten sowohl für Bundesorgane (KVG) wie auch Private (VVG), wenn es einen betrieblichen Datenschutzverantwortlichen gab, der die Einhaltung der Datenschutzvorschriften überwachte und ein Verzeichnis der Datensammlungen führte. In Art. 36 ist nur noch von „Bundesorganen“ die Rede. Es ist von der Rechtssetzungssystematik her nicht klar, wo sich nun die äquivalente Bestimmung für „Private“ befindet und ob es überhaupt noch eine solche Ausnahme gibt. Für die Krankenversicherer ist es wichtig, dass eine solche Ausnahme weiterhin bestehen kann. Die heutige Regelung des betriebsinternen Datenschutzverantwortlichen funktioniert bei den Krankenversicherern gut und hat sich eingependelt. **Es gibt keinen Grund, diese Ausnahme abzuschaffen. Die Krankenversicherer halten daran fest. Eine entsprechende Bestimmung ist wieder aufzunehmen.**
	s.o.	41	3	a und b	<u>Untersuchung:</u> Gemäss lit. a und b kann der Datenschutzbeauftragte ohne Vorankündigung Räumlichkeiten der Krankenversicherer inspizieren sowie Zugang zu allen notwendigen Daten und Informationen verlangen, sofern er findet, dass er nicht genügende Informationen von den Krankenversicherern erhalten hat. Diese Machtkumulation und erhebliche Kompetenzausweitung beim Datenschutzbeauftragten lehnen die Krankenversicherer strikte ab! Es kann nicht sein, dass der Datenschutzbeauftragte selber bestimmen kann, wann er genügende Informationen hat und falls nicht, diese gerade selber einholen bzw. durchsetzen kann. Mit einer solchen Bestimmung wird die Rechtstaatlichkeit und die Rechtssicherheit ausgehebelt. **Die Krankenversicherer verlangen deshalb eine Streichung von lit. a und b. oder aber dann die rechtsstaatlich korrekte Ausübung dieses Eingriffsrechts des Datenschutzbeauftragten im Rahmen einer anfechtbaren Verfügung, deren Rechtmässigkeit durch eine unabhängige Stelle überprüft werden kann.**

	s.o.	41	4		Abs. 4 gibt dem Datenschutzbeauftragten die Kompetenz auch ausserhalb eines Untersuchungsverfahrens zu überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten. Bis anhin war eine solche Kompetenz an ein offizielles Verfahren geknüpft, im Rahmen dessen eine Sachverhaltsabklärung gemacht wurde. **Diese neue Bestimmung benötigt Präzisierungen und Erklärungen. Ebenfalls ist zwingend, dass die Betroffenen (Krankenversicherer) darüber in Kenntnis gesetzt werden.**
	s.o.	42			Vorsorgliche Massnahmen: Auch hier handelt es sich um eine (Verfügungs-)Kompetenzerweiterung zugunsten des Datenschutzbeauftragten. Neu soll der Datenschutzbeauftragte selber vorsorgliche Massnahmen mittels Verfügung anordnen können. Es entzieht sich den Kenntnissen der Krankenversicherer, weshalb diese Kompetenz zugunsten des Datenschutzbeauftragten erweitert wurde. Auch die Erläuterungen zu Art. 42 schweigen sich darüber aus. **Die Krankenversicherer lehnen diese Kompetenzerweiterung ab. Das Bundesverwaltungsgericht soll weiterhin für die Anordnung von vorsorglichen Massnahmen zuständig sein!**
	s.o.	44			Verfahren: Vgl. hierzu die Bemerkungen zu Art. 42 oben. Vorsorgliche Massnahmen sind aus rechtsstaatlichen Gründen lediglich durch das Bundesverwaltungsgericht anzuordnen und einer Beschwerde gegen eine solche Verfügung darf in keinem Falle die aufschiebende Wirkung entzogen werden. **Abs. 3 ist zu streichen, der übrige Artikel 44 gemäss den Bemerkungen zu Art. 42 anzupassen.**
……	s.o.	45			Anzeigepflicht: **Diese Bestimmung geht weiter als das Europäische Recht und ist deshalb zu streichen!**

	s.o.	50			Strafbestimmungen: **Die präsentierten Strafbestimmung im Rahmen der DSG-Revision, welche primär auf private, strafrechtliche Sanktionen gegen einzelnen Organe und sogar Mitarbeitende gerichtet sind, werden strikte abgelehnt**. Eine Busse von bis zu CHF 500‘000.- für Privatpersonen entbehrt jeglicher Verhältnismässigkeit und ist nicht zielführend, auch mit Blick auf die Sanktionierung anderer Straftaten. Anstelle von solch hohen Bussen sollte überlegt werden, allenfalls bedingte Strafen auszusprechen. Zudem wären Verwaltungssanktionen ebenso greifend. Auch die Bussenhöhe bei fahrlässige Begehung (Abs. 4) von bis zu CHF 250‘000.- ist bei weitem zu hoch angesetzt.
	s.o.	52			Verletzung der beruflichen Schweigepflicht: Die Abgrenzung dieser Bestimmung hin zu Art. 321 StGB ist nicht klar bzw. zu wenig klar und dementsprechend zu präzisieren.
	s.o.	53			Übertretungen in Geschäftsbetrieben: Auch hier ist nicht nachvollziehbar, warum primär Mitarbeitende als Privatpersonen sanktioniert werden und nicht primär gegen die Unternehmung vorgegangen wird, allenfalls erst sekundär gegen die Mitarbeitenden.
	s.o.				Übergangsbestimmungen: Generell wird festgestellt, dass Übergangsbestimmungen lückenhaft sind zum Beispiel im Bereich der neuen Informations- und Auskunftspflichten. Es muss davon ausgegangen werden, dass die notwendigen Übergangsbestimmungen für alle Sachverhalte, die es zu erfassen gilt, aus zeitlichen Gründen noch nicht erbracht bzw. durchdacht werden konnten. Die Krankenversicherer vertreten in Anlehnung an die generellen Bemerkungen einleitend ganz oben im Dokument, dass sich die Schweiz hier keinen unnötigen Zeitdruck schaffen muss zuungunsten der Klarheit bei der Umsetzung. **Es ist deshalb eine genügend lange Umsetzungsfrist von mindestens**

					2 Jahren für alle Bearbeitungstätigkeiten vorzusehen und es sind alle notwendigen Sachverhalte übergangsrechtlich zu erfassen.
	s.o.	59		a	Übergangsbestimmungen: Diese Bestimmung ist gemäss unseren Bemerkungen zu Art. 16 (Datenschutz-Folgenabschätzung) oben anzupassen.
	KVG	84			Änderung des KVG: Im Einleitungssatz soll das Wort „Persönlichkeitsprofile“ ersatzlos gestrichen werden. Weshalb genau dies geschieht und weshalb hier eine ersatzlose Streichung erfolgt, obschon im VE DSG erklärt wird, wonach dieser Begriff durch das Wort „Profiling“ ersetzt wird, ist aus den Erläuterungen nicht ersichtlich. Dazu fehlen Ausführungen. Die Krankenversicherer müssen deshalb davon ausgehen, dass damit eine massive Einschränkung im Rahmen der Durchführung des KVG erfolgt. Denn der Begriff 'Profiling' definiert auch die Auswertung von nicht-personenbezogenen Daten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Es gibt keinen Grund, weshalb dies inskünftig nicht mehr möglich sein soll. Weiter soll im Interesse der Rechtssicherheit auch im KVG von besonders schützenswerten *Personen*daten die Rede sein, damit die Begriffe im DSG und im KVG einheitlich verwendet werden. Ebenso gilt es im Hinblick auf Art. 27 Abs. 2 VE-DSG im KVG eine Grundlage für den Erlass von automatisierten Einzelentscheidungen zu schaffen. Eine Informations- und Anhörungspflicht bei automatisierten Einzelentscheidungen würde zu einem enormen administrativen Mehraufwand mit entsprechenden Kosten führen – und dies ohne den Versicherten einen erkennbaren Nutzen zu bringen. Art. 84 KVG ist deshalb wie folgt zu formulieren: *Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten **im Sinne von Artikel 3 Buchstaben a und b**, einschliesslich besonders schützenswerter **Personen**daten **im Sinne von Artikel 3 Buchstabe c DSG** zu bearbeiten oder bearbeiten zu lassen, **das Profiling im Sinne von***

					Artikel 3 Buchstabe f DSG durchzuführen und automatisierte Einzelentscheidungen im Sinne von Artikel 15 Abs. 1 DSG zu erlassen**, die sie benötigen, **soweit dies notwendig ist,** um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:* *Lit. a (….)* *(…)* ***Neu c^{bis}: Managed Care Massnahmen durchzuführen; ***Neu c^{ter}: alternative Versicherungsmodelle in Zusammenarbeit mit den Leistungserbringern sowie deren Verbänden zu betreiben*** Weiter sollte Art. 84 mit einem Abs. 2 ergänzt werden wie folgt: ***^{2}Das Profiling im Sinne von Artikel 3 Buchstabe f DSG soll insbesondere durchgeführt werden, um mit Einwilligung der Versicherten Case-Management-Massnahmen zu ergreifen. Die Einwilligung der Versicherten hat in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu erfolgen.*** Die neue Bestimmung ist notwendig, da Bundesorgane (und damit auch KVG-Versicherer) gemäss Art. 27 Abs. 3 VE-DSG nur noch im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten dürfen - und auch dies nur unter bestimmten Voraussetzungen. Von *'ausnahmsweise'* und *'im Einzelfall'* kann aber bei Case-Management-Massnahmen wohl kaum die Rede sein. Es besteht somit die Gefahr, dass die stetig an Bedeutung gewinnenden Case-Management-Massnahmen als Folge der Revision des DSG nicht mehr zulässig sind, weil sie nicht zu den Aufgaben gehören, die das KVG von Gesetzes wegen den Versicherern überträgt, sondern um freiwillige Wiedereingliederungsbemühungen des KVG-Versicherers. Mit der vorgeschlagenen Ergänzung wird ausdrücklich präzisiert, dass solche Massnahmen die Einwilligung der Versicherten in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht, erfordern.
	KVG	84a	1	***neu b^{ter}***	Datenbekanntgabe: Ergänzung von Art. 84a Abs. 1 mit

					(…) ***Neu a^{bis}: Leistungserbringern der Pflege im Rahmen der Verwaltung von alternativen Versicherungsmodellen*** (…) ***Neu b^{ter}: Leistungserbringern der Pflege sowie deren Verbände im Rahmen der Verwaltung von alternativen Versicherungsmodellen*** ***Neu b^{quater}: Privatversicherern, wenn die Daten für die Koordination der Beurteilung und Berechnung von Leistungsansprüchen erforderlich sind;*** (…) Art. 26 Abs. 2 VE-DSG sieht zwar vor, dass der Bundesrat auf dem Verordnungsweg die Kontrolle und die Verantwortung regelt, wenn Bundesorgane zusammen mit anderen Bundesorganen oder mit Privaten Daten bearbeiten. Diese geplante Regelung auf Verordnungsstufe dient jedoch lediglich der Kontrolle und Verantwortung, ist jedoch keine ausreichende Grundlage dafür, um eine notwendige und praktikable Zusammenarbeit zwischen den Grund- und Zusatzversicherern zu garantieren.
	KVG	84a	5	b	Ergänzung von Art. 84a Abs. 5 lit. b wie folgt: *Personendaten, sofern die betroffene Person im Einzelfall schriftlich **in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht**, eingewilligt hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse des Versicherten vorausgesetzt werden darf.* Die Eidgenössischen Räte haben in ihrem Rückweisungsbeschluss vom März 2013 betreffend die VVG-Revision verlangt, dass bei der Erarbeitung einer neuen Vorlage dem elektronischen Geschäftsverkehr Rechnung getragen wird. Dies im Hinblick auf die Tatsache, dass die Digitalisierung im gesamten Versicherungswesen Einzug gehalten hat. Es gilt daher, nicht nur im VVG, sondern auch im KVG die Bestimmungen technologieneutral zu formulieren und Begriffe, die den elektronischen Geschäftsverkehr behindern, konsequent zu eliminieren. Der VE-DSG als solcher behindert den elektronischen Geschäftsverkehr zwar grundsätzlich nicht, da das Erfordernis der Schriftlichkeit nur in einer einzigen

					Bestimmung betreffend die Auftragsdatenbearbeitung vorgesehen ist. Die Änderung von Art. 84a Abs. 5 lit. b KVG ist jedoch notwendig, da das KVG als Spezialgesetz dem DSG vorgeht

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung

Amstutz Jonas BJ

Von: Joanne Siegenthaler-Arcidiacono <joanne.siegenthaler@sav-fsa.ch>
Gesendet: Freitag, 31. März 2017 12:48
An: Amstutz Jonas BJ
Cc: Rene Rall
Betreff: Consultation - révision LPD - DSG Revision
Anlagen: FSA_SAV_Prise de position_Revision_LPD_DSG_2017_0331.pdf; FSA_SAV_Prise de position_Revision_LPD_DSG_2017_0331.DOC

Monsieur,
Mesdames, Messieurs,

Veuillez trouver en pièce jointe, sous format électronique Word et pdf, la prise de position de la Fédération Suisse des Avocats (FSA-SAV) dans la consultation mentionnée sous rubrique concernant la révision de la LPD, ouverte jusqu'au 4 avril 2017.
Nous vous remercions de bien vouloir prendre en compte les remarques de la Fédération Suisse des Avocats et demeurons à disposition pour toute question.

Avec nos meilleures salutations,

Joanne Siegenthaler
lic. iur. LL.M., médiatrice
Secrétariat général

Fédération Suisse des Avocats
Marktgasse 4
Case postale
3001 Berne

Tel. +41 (0) 31 313 06 06
Fax +41 (0) 31 313 06 16
www.sav-fsa.ch

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Avis donné par

Nom / société / organisation : Fédération Suisse des Avocats, Schweizerischer Anwaltsverband

Abréviation de la société / de l'organisation : FSA - SAV

Adresse : Marktgasse 4, Case postale, 3001 Berne

Personne de référence : René Rall, Secrétaire général FSA-SAV

Téléphone : 031 / 313 06 06

Courriel : info@sav-fsa.ch

Date : 31 mars 2017

Remarques importantes :

1. Nous vous prions de ne pas modifier le formatage de ce formulaire !
2. Utilisez une ligne par article, alinéa et lettre ou par chapitre du rapport explicatif.
3. Veuillez faire parvenir votre avis au **format Word** d'ici au 4 avril 2017 à l'adresse suivante : jonas.amstutz@bj.admin.ch

Nous vous remercions de votre collaboration!

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Table des matières

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Remarques générales

nom/société	remarque / suggestion :
FSA	Le 11 septembre 2014, le Conseil de l'Union européenne a adopté le rapport du comité d'évaluation concernant la protection des données en Suisse qui contient une recommandation qui invite la Suisse à renforcer les pouvoirs du préposé en lui attribuant des pouvoirs décisionnels et de sanctions. C'est également la tendance dans les autres pays. Malheureusement l'avant-projet ne renforce pas réellement les pouvoirs du PFPDT. Ce point doit être corrigé et de vrais pouvoirs de sanction (procédure administrative) doivent être donnés au PFPDT.
FSA	La révision de la LPD doit aussi prendre en compte les évolutions européennes, en particulier le projet de règlement européen vie privée (e-privacy) et communications qui entrera en vigueur le 25 mai 2018 . Les cookies techniques ou limités à une session et dont les données ne sont pas partagées ne doivent pas nécessiter de consentement.
FSA	En anglais, l'abréviation DPA est habituellement utilisée pour Data Protection Autorithy. Il serait préférable d'utiliser FADP pour Federal Act on Data Protection.
FSA	L'art. 45c LTC est la seule disposition applicable aux cookies. Elle devrait être intégrée dans la révision de la LPD. Une lecture stricte exigerait une information pour chaque cookie ou traceur qui ne sert pas à fournir ou facturer des services de télécommunications. Le texte doit être adapté et prendre en compte le projet de règlement européen vie privée et communications. Les cookies techniques ou limités à une session et dont les données ne sont pas partagées ne doivent pas nécessiter de consentement.
FSA	Le PFPDT doit pouvoir prononcer des amendes et celles-ci doivent viser les entreprises (cf. article Plaidoyer).
FSA	Il est particulièrement important que la loi entre en vigueur rapidement, tant pour assurer la conformité avec la Directive que pour éviter d'avoir une situation d'incertitudes sur les obligations en Suisse alors que les entreprises suisses et étrangères se mettent en conformité au niveau européen (Règlement). Sinon il y a un risque sérieux que les entreprises suisses et étrangères ne se mettent en conformité qu'une seule fois, ne prenant pas ou mal en compte les exigences suisses.

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

FSA	La communication d'informations et la collaboration avec le préposé ne doit pas représenter un risque pour les responsables de traitement tant sous l'angle technique de la sécurité des données (le préposé doit prendre les mesures techniques et organisationnelles adéquates) que sous l'angle juridique (violation de l'obligation de confidentialité, utilisation dans des procédures, communications entre autorités). Une garantie de confidentialité doit être ajoutée dans la loi, pour permettre au responsable de traitement de s'exprimer librement avec le préposé, sans crainte de sanction ni de violation de ses obligations de confidentialité.
FSA	
FSA	
FSA	
FSA	
FSA	
FSA	
FSA	
FSA	
FSA	

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

nom/société	loi	art.	al.	let.	remarque / suggestion :
FSA	LPD	2			Le Tribunal fédéral a retenu, en vertu de la théorie des effets, que les images prises en Suisse et publiées d'une façon qui permet d'y accéder en Suisse également ont un lien prépondérant avec la Suisse, même si les images sont traitées à l'étranger et ne sont pas mises en ligne directement depuis la Suisse (ATF 138 II 346, cons. 3.3). Même si la LPD ne définit pas son champ d'application territorial comme le fait le RGDP, cette jurisprudence doit continuer à s'appliquer.
FSA	LPD	2	2	c	Si la LPD ne s'applique plus aux traitements des données par les autorités judiciaires, également lorsque les procédures ne sont plus pendantes, des normes supplémentaires doivent être prévues dans le CPP et le CPC. Le CPP ne traite par exemple que des procédures pendantes (art. 101 CPP, voir également 95ss CPP). Les droits de la personne dont les données sont traitées sans qu'elle ne soit partie à la procédure ne sont pas non plus pris en compte. Le droit de consulter le dossier est réservé aux parties (art. 53 CPC). La LPD doit s'appliquer avant l'ouverture et dès la clôture de la procédure et à l'activité non juridictionnelle des tribunaux. Cela évite également un risque d'abus du droit d'accès.
FSA	LPD	2	3		La compétence de surveillance des tribunaux devrait être données au PFPDT jusqu'à ce qu'une autorité indépendante soit prévue par la loi. L'autorité de surveillance administrative des tribunaux pourrait jouer ce rôle.
FSA	LPD	3		f	L'inclusion de données non personnelles et de données traitées manuellement (pas automatiquement) devrait être abandonnée, car elle donne lieu à une définition trop large du profilage. Si l'évaluation de n'importe quelles données peut être considérée comme du profilage, il faudrait systématiquement obtenir le consentement pour ce type de traitement, ce qui serait impossible en pratique. De plus, ce n'est pas nécessaire d'étendre aux données non personnelles, puisque la notion de données personnelles couvre déjà les données de personnes déterminables. En tout état de cause, l'inclusion

					de ces autres données (non personnelles) mènerait à des difficultés pratiques. La notion de profilage devrait ainsi être identique à celle utilisée dans le RGPD et donc être limitée à l'exploitation automatisée de données et que pour des données personnelles.
FSA	LPD	4	3		Le terme « clairement » est flou et devrait être supprimé.
FSA	LPD	4	6		Ce qui est entendu par l'expression clair du consentement n'est en réalité pas très clair et devrait donc être supprimé. La notion de caractère « express » du consentement doit être précisée dans le rapport explicatif. Il ne se justifie pas de demander un caractère express pour toute activité de profilage, mais seulement lorsqu'il concerne des données sensibles. En effet, le profilage est « ressenti » comme quelque chose de menaçant ; la plupart du temps le profilage est cependant inoffensif.
FSA	LPD	5	2		L'art. 5 al. 2 devrait être complété pour préciser que dans un tel cas il ne peut pas être tenu responsable en cas d'atteinte à la personnalité, même si un tribunal devait remettre en cause le choix du Conseil fédéral. Idem si des contrats sont approuvés par le PFPDT.
FSA	LPD	5	2 et 3		L'exception de l'al. 3 lit a devrait être supprimée car ces pays doivent être ajoutés automatiquement à la liste de l'al. 2. Un responsable de traitement doit néanmoins avoir la possibilité de démontrer que le traitement peut être sûr dans un pays qui ne figure pas sur la liste. L'avant-projet ne distingue pas dans quels cas il s'agit d'une communication exceptionnelle au sens de l'art. 6 et il n'est pas possible de savoir si une communication basée sur le consentement peut avoir lieu de manière régulière. Est-ce-que l'acceptation de conditions générales d'un service fourni via Internet est toujours valable, cas échéant seulement pour une communication exceptionnelle ou aussi pour une communication ordinaire?
FSA	LPD	5	4		Le délai est trop long et devrait être réduit à 30 jours à compter de la communication des garanties.

FSA	LPD	5	6		Cette disposition devrait être supprimée puisqu'elle n'amène aucune plus-value. De plus, le RGPD ne contient pas un tel devoir d'information.
FSA	LPD	6	1	a	Les termes « en l'espèce » sont trop restrictifs. Selon les principes généraux, il suffit que le consentement se réfère à un état de fait récurrent. Dès lors, les termes « en l'espèce » peuvent être supprimés. Il ne fait d'ailleurs pas de doute que le consentement doit porter sur le transfert et qu'un simple consentement au traitement ne serait pas suffisant.
FSA	LPD	6	1	b	Le traitement en lien avec les contrats devrait, à l'instar de ce qui est prévu dans le RGPD, inclure le traitement de données qui est seulement fait dans l'intérêt de la personne concernée, ainsi que les traitements par des personnes qui sont de toute autre manière impliquées dans le contrat (par exemple personnes de contact).
FSA	LPD	6	2		L'art. 6 al. 2 va engendrer un nombre important de notifications que le PFPDT aura peine à gérer. On peut se demander si elles sont vraiment utiles.
FSA	LPD	7	1	b	Une obligation légale de garder le secret ne doit pas interdire la sous-traitance. Pourtant, la portée de l'art. 320 CP est largement contestée en doctrine. La norme semble interdire toute délégation de traitement, alors que cela est donc justifié par la Sozialadäquanz. L'introduction du récent art. 26a OIAF permet à des fournisseurs externes de prestations informatiques d'avoir accès à des données de l'administration qui ne sont pas accessibles au public et qui sont donc couvertes par le secret de fonction, ce qui semble contraire à l'art. 320 CP. La portée du secret de fonction doit être clarifiée dans le Code pénal parallèlement à la révision de la LPD et les conditions de l'outsourcing à l'étranger pour les données de l'administration clairement redéfinies. La sécurité du droit ne permet pas d'avoir un art. 26a OIAF qui permet la délégation de traitement, un art. 320 CP inadapté au monde numérique actuel et la LPD qui renvoie à d'autres normes. Le consentement obtenu sous l'angle de 6 al. 1 ch. a doit également être valable sous l'angle du secret. La réserve des secrets doit être clarifiée car la situation actuelle ne doit pas être remise en cause.

					A défaut de clarifier les exigences de l'article 7, il conviendrait de limiter cette disposition aux questions de sécurité des données (cf. art. 7 al. 2).
FSA	LPD	8			La publication de recommandations très concrètes par le PFPDT est un élément positif. En revanche, le fait qu'il s'agisse de bonnes pratiques non contraignantes est problématique car les responsables de traitement ne sauront pas s'il s'agit d'un objectif idéal (bonnes pratiques) ou simplement du minimum légal à atteindre (art. 8). En outre, contrairement aux normes de la RGPD qui prévoit que ce sont les associations et autres organismes qui élaborent les codes de conduite, il s'agit ici du PFPDT, ce qui contredit le but de l'autoréglementation. Cela pourrait également créer un risque que le PFPDT utilise ses recommandations de bonnes pratiques pour promouvoir sa propre interprétation. Les recommandations ne devraient donc émaner que des responsables de traitement (et éventuellement être approuvées par le PFPDT).
FSA	LPD	7	3		Cette exigence n'apporte pas plus de protection car l'accord sera donné de manière globale et préalablement. En cas d'intérêt particulier, et même sans cette disposition, un engagement contractuel est toujours possible. Cet alinéa peut être supprimé ou bien cette présomption légale devrait être réglée de façon expresse.
FSA	LPD	9			L'art. 9 est inutile car les recommandations de bonnes pratiques n'ont pas de force obligatoire. Il doit donc être supprimé.
FSA	LPD	10			La certification doit couvrir comme aujourd'hui les systèmes.
FSA	LPD	11	2		La sécurité des données est un élément difficile à mettre en place pour un responsable de traitement. Il est important que le Conseil fédéral et le PFPDT donnent des critères précis et des recommandations techniques non seulement des principes généraux comme actuellement (art. 11 al. 2).

FSA	LPD	12			Ces questions importantes doivent être réglées dans le Code civil. Elles doivent être supprimées sous réserve d'une volonté contraire du défunt ou d'une obligation légale de conserver. Dans tous les cas le secret professionnel doit être respecté.
FSA	LPD	13	4		Si l'on peut saluer l'obligation d'avoir l'accord du responsable de traitement pour sous-déléguer un traitement, l'information de la personne concernée doit être plus limitée (art. 13 al. 4). Il n'est pratiquement pas envisageable de communiquer la liste de l'identité et les coordonnées de tous les sous-traitants, ainsi que les données ou catégories de données concernées.
FSA	LPD	13	4		Si l'on peut attendre du responsable du traitement qu'il informe de l'existence de sous-traitants et communique sur demande l'identité de ces derniers, il ne paraît en pratique pas envisageable que le responsable du traitement doive informer toutes les personnes dont les données sont traitées à chaque fois qu'il y a un changement de sous-traitant. Cela est d'autant plus vrai que nombre de sous-traitants n'auront un accès que limité voire incident aux données. L'exigence d'information doit être réduite pour être praticable, voire purement et simplement supprimé car l'art. 13 al. 4 va au-delà du RGPD et mènerait à des communications par trop extensives.
FSA	LPD	14			Le commentaire de l'art. 14 semble indiquer qu'une information n'est pas nécessaire lorsque la personne a rendu les données accessibles. Cela devrait être précisé dans la loi, y compris s'il s'agit des données rendues publiquement accessibles ou communiquées au responsable de traitement. A l'instar de l'art. 24, il convient d'énumérer les cas dans lesquels les intérêts privés prépondérants existent généralement.
	LPD	15	2		Pour que la personne puisse faire valoir ses droits d'accès de manière utile, un minimum d'informations doit être transmis à la personne et en particulier les critères pris en compte pour prendre la décision et les données la concernant. L'al. 2 vise plus la protection des consommateurs que la protection de la personnalité et n'a pas sa place ici. Il doit être supprimé. Les droits d'actions classiques de la LPD demeurent.

FSA	LPD	16			Aucune méthodologie n'est imposée pour l'analyse d'impact préalable (art. 16). Cela devrait être précisé dans la loi, sinon il y a un risque que le PFPDT en refuse une ou en impose une sans base légale. Si l'intention est au contraire que le PFPDT établisse une procédure, la loi devrait le prévoir. Le risque accru exigeant une analyse d'impact préalable doit être précisé. Le commentaire retient un risque accru si une utilisation abusive des données peut porter atteinte à la personnalité, à la dignité ou au bien-être de la personne. C'est pourtant le cas de presque la totalité des utilisations abusives de données, ce qui revient à généraliser l'analyse préalable. L'analyse d'impact va demander un travail important aux responsables de traitement. Il conviendrait donc d'aller au bout du processus et de donner plus de poids à l'avis du PFPDT. Si le PFPDT donne son accord ou ne s'exprime pas dans le délai de trois mois dès la communication, le responsable de traitement doit pouvoir partir du principe que le traitement décrit est conforme et qu'il ne peut pas faire ensuite l'objet d'une procédure ou de sanction pour ce traitement. Les objections du PFPDT ne jouent pas grand rôle non plus, puisqu'il n'y a pas de sanction. L'analyse d'impact ne doit concerner que le responsable de traitement et pas le sous-traitant. L'obligation de communiquer au préposé le résultat doit être limitée aux cas où l'analyse retient un risque accru pour la personnalité. En outre, le contenu de la communication au PFPDT doit être réglementé et la confidentialité être assurée, notamment eu égard aux exigences de la LTrans. Il s'agit aussi de veiller au fait que l'analyse d'impact peut contenir des secrets d'affaires pouvant intéresser la concurrence.
FSA	LPD	17			La notion de perte de données utilisée à l'art. 17 n'est pas satisfaisante et peut être comprise comme une suppression des données. Or elle doit couvrir toutes les pertes de maîtrise sur les données, y compris les potentiels accès et copies. Le risque est d'ailleurs plus grand si les données sont copiées et pas simplement supprimées. Le même problème se pose à l'art. 11 LPD. La notion de pertes de données doit en outre être limitée aux cas de violations de sécurité à l'exemple de la RGPD. En l'état, l'art. 17 va plus loin que la RGPD et la convention STE 108.
FSA	LPD	17	1		Selon le texte de l'avant-projet, le responsable du traitement doit notifier sans délai au préposé tout

					traitement non autorisé, le non-respect de cette obligation étant une infraction pénale. Or, rédigé ainsi, le responsable du traitement devrait aussi notifier tout traitement non autorisé qu'il a lui-même effectué par exemple une utilisation de données dans un but autre que celui annoncé. Cela peut violer le droit de ne pas s'auto-incriminer. De plus, le responsable du traitement devrait choisir entre respecter cette disposition et être sanctionné pour avoir violé la LPD, ou ne rien dire pour éviter d'être sanctionné. Le texte devrait être modifié pour adresser les failles de sécurités et traitements non-autorisés de tiers. Les délais doivent être clarifiés et assouplis. De manière générale, on devrait renforcer ces dispositions en s'inspirant du RGPD. Cela est nécessaire à assurer la protection des données et l'intérêt de la place économique Suisse.
FSA	LPD	18			Au niveau de la systématique, l'art. 18 alinéa 1er appartient à l'art. 11 et l'art. 18 al. 2 à l'art. 4.
FSA	LPD	18			La protection des données dès la conception n'est pas suffisante et une interdiction doit être faite aux fabriquants et développeurs de prévoir des portes dérobées (backdoors) et toutes autres mesures permettant un accès aux données à l'insu de la personne concernée.
FSA	LPD	19			Le devoir de documentation de tous les processus de traitement (art. 19) est une mesure qui peut être lourde pour les responsables de traitement et il est important qu'elle soit détaillée dans la loi. Si une ordonnance peut préciser certaines modalités, les éléments principaux doivent être décrits dans la LPD. La communication de la durée de conservation dans le cadre du droit d'accès est illusoire, car elle n'est souvent pas définie en pratique. Il convient d'y renoncer. Quant à l'al. 3, il devrait être supprimé et au besoin intégré à l'art. 15 pour une meilleure coordination. Le secret d'affaire du responsable de traitement va souvent s'opposer à la communication des critères retenus. La simple mention des données traitées peut déjà lui poser des difficultés.
FSA	LPD	19			La section 4 ne traite que du droit d'accès, elle devrait donc s'appeler droit d'accès plutôt que droits de la personne concernée.

FSA	LPD	19		b	Les devoirs de cette disposition vont trop loin, car il y a constamment des rectifications, effacements, etc. (par exemple une suppression de données qui n'est plus nécessaire). Par ailleurs, ce devoir ne devrait pas s'étendre au devoir d'informer en cas de violation de la protection des données ou de limitation du traitement. L'information en cas de violation de la protection des données irait également à l'encontre du principe *nemo tenetur*. Le devoir d'informer devrait donc être limité aux situations où l'accès à cette information a été requis et motivé. A cet égard, la référence à des « efforts disproportionnés » n'est pas suffisante. De plus, la référence au sous-traitant devrait être supprimée. Il n'aurait parfois même pas l'accès aux informations nécessaires (par exemple au caractère exact des données). Enfin, les modalités d'exercice ne sont pas clairement définies.
FSA	LPD	20			Cette disposition devrait contenir des mesures visant à éviter les abus dans l'utilisation du droit d'accès. Des exceptions à la gratuité du droit d'accès devraient, par exemple, être prévues.
FSA	LPD	20	1	b	Il faudrait limiter la portée aux « catégories » de données personnelles traitées (cf. art. 15, paragraphe 1, lettre b RGPD).
FSA	LPD	20	1	e	Il ne devrait pas être nécessaire d'énumérer de façon détaillée toutes les décisions individuelles automatisées qui ont eu lieu par le passé. Une information générale sur les décisions automatisées devrait suffire. Ainsi, l'art. 20 al. 3 devrait être supprimée.
FSA	LPD	20	3		Les informations à fournir sur la base de cet alinéa sont trop extensives et constituent une intrusion à la liberté des entreprises. Ces devoirs d'information devraient à tout le moins être limités aux cas de décisions individuelles automatisées.
FSA	LPD	21	1		Cette disposition renvoie à l'art. 14. Il devrait être possible d'invoquer de façon générale un intérêt privé prépondérant, même en cas de communication de données personnelles à des tiers.

FSA	LPD	22			L'art. 22 prévoit des exceptions au droit d'accès en faveur des médias. Une mention des autres secrets (par exemple le secret professionnel) serait judicieuse.
FSA	LPD	23	2		L'art. 23 al. 2 prévoit des cas d'atteinte à la personnalité. Le lit. b. vise les traitements contre la manifestation expresse de la volonté de la personne concernée, le lit. d le profilage sans le consentement exprès de la personne concernée, alors que la lit. c concerne la communication à des tiers de données sensibles (indépendamment du consentement). Le lit. c devrait seulement viser les cas où la communication a lieu sans consentement.
FSA	LPD	24	2	a	Cela devrait également couvrir le traitement de données par les personnes impliquées dans le contrat, par ex. les personnes de contact.
FSA	LPD	25			Le projet ne prévoit pas d'actions en exécution du droit d'accès (mentionnées pourtant à l'art. 15 al. 4 de la LPD actuelle). Il faudrait l'ajouter à l'art. 20 ou 25. Alors que l'on pourrait imaginer qu'une action puisse, indirectement, se fonder sur les droits de la personne concernée issue de la protection de sa personnalité (et donc sur la voie de l'art. 25), le rapport explicatif semble faire une distinction entre l'action en exécution du droit d'accès et, justement, les actions de l'art. 25, cf. commentaire du rapport p. 67 et 86 (§ 8.2.9.1 relatif au for), qui est d'ailleurs le seul endroit du rapport mentionnant l'existence d'une action en exécution du droit d'accès.
FSA	LPD	31			L'art. 31 prévoit que les organes fédéraux proposent aux Archives fédérales de reprendre toutes les données personnelles dont ils n'ont plus besoin en permanence. Il ne tient pas compte des organes qui doivent archiver eux-mêmes leurs données conformément à l'art. 4 al. 3 LAr et l'annexe 2 OLAr. Ces dispositions doivent être coordonnées.
FSA	LDP	34	4		L'art. 34 al. 4 devrait aussi être applicable aux privés !
FSA	LPD	37			Si le PFPDT dispose de son propre budget (art. 37), rien ne le lui garantit et le parlement pourrait le réduire drastiquement par mesure de rétorsion. L'indépendance de ses locaux et de son personnel

					n'est pas non plus garantie. On ne peut pas réellement parler d'un renforcement de son indépendance.
FSA	LPD	37	1		Pour assurer l'indépendance du PFPDT, il doit être élu par le Parlement. Le projet prévoit seulement une ratification du choix fait par le Conseil fédéral, ce qui laisse la possibilité au Conseil fédéral de sanctionner un préposé sortant et ne laisse pas de réel choix à l'assemblée.
FSA	LPD	40	3		Aucun arbitrage n'est prévu en cas de désaccord entre autorités au sens de l'art. 40 al. 3. Une compétence similaire à la cour des plaintes selon le CPP devrait être donnée par exemple au TAF.
FSA	LPD	41			L'art. 41 prévoit que le PFPDT peut requérir des renseignements et des documents. En cas de non coopération, le PFPDT peut inspecter des locaux et exiger l'accès à des documents. Le renvoi à l'art. 17 PA indique également que des témoins peuvent être entendus, mais l'art. 14 PA doit encore être complété. L'art. 44 renvoie également à la PA. Il conviendrait donc de préciser les moyens d'enquête du PFPDT et d'adapter la terminologie avec l'art. 12 PA (documents, renseignements des parties, renseignements ou témoignages de tiers, visite des lieux, expertises). La participation de l'organe fédéral ou de la personne privée visée aux mesures d'enquête et son droit d'être entendu doivent être garantis.
FSA	LPD	41			Selon le commentaire, les mesures provisoires semblent également viser l'administration des preuves, alors que ces dernières sont traitées à l'art. 41. Il y a dès lors un risque que des moyens envisagés dans les mesures provisoires pour l'obtention des preuves ne soient pas reconnus.
FSA	LPD	41	3		Aucun moyen de contrainte n'est donné au PFPDT. La possibilité doit lui être donnée de demander l'assistance de la police fédérale ou cantonale pour mener des perquisitions si la personne ou l'organe visé refuse de coopérer. Les moyens de l'art. 41 al. 3 ne doivent pas être limités aux cas où la personne visée ne coopère pas, sinon il serait facile de faire disparaître des preuves.
FSA	LPD	41	5		Le dénonciateur sera informé de l'issue de la procédure mais n'a pas qualité de partie. Cela n'est pas satisfaisant pour le dénonciateur dont les données sont concernées et la possibilité d'être partie à la

					procédure devrait lui être accordée. Sinon il devra ouvrir une procédure civile parallèle. Il y aurait ainsi une procédure civile et une procédure administrative portant sur le même objet et avec les mêmes buts, ce qui va doubler les efforts nécessaires pour arriver au même but. En l'absence de procédure collective, un responsable de traitement pourra devoir faire front à une procédure devant le PFPDT et une série de procédures civiles ouvertes devant différentes autorités pour le même traitement. Cela va engendrer des coûts inutiles et représente surtout un risque de décisions contradictoires.
FSA	LPD	42			Les mesures provisoires de l'art. 42 permettent de préserver des preuves. Il s'agit toutefois seulement d'une mesure temporaire. La possibilité, au fond, d'administrer le moyen de preuve doit être prévue par la loi. Sinon il n'y a aucune raison de préserver provisoirement des preuves qui au final ne peuvent pas être utilisées.
		44	1		Le renvoi à la procédure administrative ne doit pas être limité aux art. 42 et 43 LPD, mais doit couvrir toute l'activité d'enquête et décisionnelle. Dans le domaine de la protection des données, les mesures provisoires peuvent être lourdes de conséquences. Or, l'expérience a montré que le PFPDT prend de telles mesures sans suffisamment prendre en compte les conséquences potentielles. Dès lors, une vérification indépendante est primordiale et l'effet suspensif devrait exister jusqu'à ce que cela ait lieu. Le tribunal devrait décider de retirer ou non l'effet suspensif au cas par cas.
FSA	LPD	48			L'information du public doit être prévue dans la loi, et non seulement une information au dénonciateur. Toutes les décisions doivent être rendues accessibles car il s'agit d'une source de jurisprudence importante. L'art. 48 restreint actuellement trop les possibilités d'information.
FSA	LPD	49			Le PFPDT doit aussi avoir la possibilité d'élaborer des outils, notamment informatiques, s'ils sont dans l'intérêt du public. On peut penser ainsi à certains outils par exemple proposés ou recommandés par la CNIL. Sans disposition ad hoc dans la loi, il pourrait être reproché au PFPDT, s'il développe un logiciel open source mis gratuitement à disposition des personnes intéressées, d'avoir une activité qui n'est pas prévue par la loi et de créer une distorsion de concurrence. Il y a pourtant beaucoup de situations

					où les solutions commerciales ne prennent pas suffisamment en compte la protection des données.
FSA	LPD	50 ss			Le commentaire de l'art. 51 indique que cette disposition ne s'applique pas aux organes fédéraux, ce qui ne figure pas clairement dans le texte de la loi. Ce devrait aussi être le cas pour l'article 50. On peut en effet se demander si la notion de personne privée est à opposer à un organe fédéral ou si elle fait référence à la personne individuelle au sein d'une entreprise ou d'un organe fédéral. La personne privée pourrait donc être un fonctionnaire. Cela devrait être précisé, même si à notre sens, seule la société, éventuellement un organe fédéral, devrait être punissable. En outre, tenir la personne privée pénalement responsable serait contre-productif, augmenterait de façon disproportionnée la charge administrative des entreprises et ne serait réellement avantageuse que pour les experts externes en matière de protection des données. De plus, au vu de la complexité croissante du domaine de la protection des données (problématiques transfrontières, division du travail, etc.), il apparaît illusoire de chercher à sanctionner la personne privée. En outre, cela mènerait à l'existence de deux procédures parallèles : par le PFPDT ainsi que par l'autorité pénale cantonale compétente ; cette dernière n'aurait d'ailleurs vraisemblablement pas le savoir-faire nécessaire à cette fin. Le fait que certaines dispositions (art. 11, 16, 18, 19 al. 1) présument un pouvoir discrétionnaire pose la question de savoir si elles peuvent même être sanctionnées. Par ailleurs, il n'est pas nécessaire, voire disproportionné, de sanctionner les infractions commises par négligence. Il serait plus judicieux de recourir à des amendes administratives imposées par le PFPDT. Dans ce cas, l'art. 43 devrait être adapté, de façon similaire aux dispositions de la LCart.
		50	2	E	Doit être complété par « décision du préposé à lui signifier sous la menace de la peine prévue au présent article ».
FSA	LPD	51			Le commentaire de l'art. 51 indique que cette disposition ne s'applique pas aux organes fédéraux, ce qui ne figure pas clairement dans le texte de la loi. On peut en effet se demander si la notion de personne privée est à opposer à l'organe fédéral ou si elle fait référence à la personne individuelle au sein d'une entreprise ou d'un organe fédéral. La personne privée pourrait donc être un fonctionnaire.

					Cela devrait être précisé, même si à notre sens, seule la société, éventuellement l'organe fédéral, devrait être punissable.
FSA	LPD	52			A lire le commentaire, il faudrait préciser que les lettres de l'art. 52 sont alternatives et non cumulatives. Il est de plus fondamental de préciser que cet article ne concerne pas la révélation à un sous-traitant. En outre, le durcissement du devoir de discrétion ne se justifie pas. Cela imposerait des obligations excessives aux entreprises et l'on ne voit pas par exemple pourquoi une société de ventes en ligne serait soumise à une obligation de confidentialité comparable à celle des médecins et avocats.
FSA	LPD	56			Le RGPD prévoit que des amendes peuvent être infligées également à des entitées étrangères. Ainsi une autorité d'un Etat Membre pourrait infliger une amende à une société suisse, sans que cette dernière n'ait participé à la procédure. Il serait utile de préciser que les traités internationaux visés à l'art. 56 ne peuvent pas servir à faire exécuter en Suisse une sanction prononcée à l'étranger.
FSA	LPD	59			Cette disposition est insuffisante, car nombre d'autres dispositions ont été modifiées et nécessitent des dispositions transitoires. Une période transitoire générale de deux ans devrait être prévue.
FSA	CP	179 novies			L'art.179*novies* prévoit dans sa nouvelle version que celui qui aura soustrait des données personnelles qui ne sont pas accessibles à tout un chacun sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. La notion « qui ne sont pas accessibles à tout un chacun » devrait être remplacée par celle de l'art. 143 CP (soustraction de données) à savoir « qui ne lui étaient pas destinées ».
FSA	CO	328b			La portée de l'art. 328b CO et du renvoi à la LPD divise la doctrine. La révision de la LPD doit aussi traiter de cette question et modifier au besoin l'art. 328b CO.
FSA	LJAr	3		a	Le projet de loi sur les jeux d'argent définit les jeux d'argent comme les jeux qui, moyennant une mise d'argent ou la conclusion d'un acte juridique, laissent espérer un gain pécuniaire ou un autre avantage appréciable en argent. L'actuel art. 1 al. 2 de la loi sur les loteries et les paris professionnels contient

					une définition similaire. Le "paiement" en données personnelles n'est pas considéré comme une mise. Cette disposition doit être complétée de sorte que la mise à disposition obligatoire de données personnelles utilisables dans un autre but que la communication du gain laissant espérer une chance de gain pécuniaire doit être considérée de la même manière qu'une mise en argent.

SBB CFF FFS

Konzernleitung · Hilfikerstrasse 1 · CH-3000 Bern 65

Bundesamt für Justiz
Bundesrain 20
3003 Bern

E-Mail: jonas.amstutz@bj.admin.ch

Bern, 27. März 2017

Stellungnahme der SBB zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes

Sehr geehrte Damen und Herren

Wir danken für die Möglichkeit zur Stellungnahme zur Totalrevision des Datenschutzgesetzes. Für die SBB als vertrauenswürdiger Mobilitätsdienstleister ist der verantwortungsvolle Umgang mit Kundendaten von zentraler Bedeutung. Datennutzung und Datenschutz müssen jedoch in einem ausgewogenen Verhältnis stehen.

Um ihren Kunden durchgehende Mobilitätsketten anzubieten, vernetzt sich die SBB noch stärker mit anderen Mobilitätsdienstleistern im In- und Ausland. Wir begrüssen deshalb die Stossrichtung des Vorentwurfs, europäisches Recht soweit nachzuvollziehen, als es für den ungehinderten Datenaustausch zwischen der Europäischen Union und der Schweiz erforderlich ist. Die Regulierung sollte jedoch nicht über das europäische Schutzniveau hinausgehen.

Die SBB bedarf wie jedes Unternehmen klarer und gut umsetzbarer rechtlicher Rahmenbedingungen. Einige Bestimmungen des Vorentwurfes genügen dieser Anforderung nicht, weil sie nur mit unverhältnismässigem Aufwand umsetzbar oder für eine direkte Anwendung zu unbestimmt sind. Weiter gilt es auch die Gesamtsystemkosten der Bahn zu berücksichtigen, deren Anstieg wir für Kunden und öffentliche Hand eindämmen müssen. Hier sollte die Vorlage der besonderen Herausforderung des öffentlichen Verkehrs mehr Rechnung tragen.

SBB AG
Konzernleitung
Hilfikerstrasse 1 · 3000 Bern 65 · Schweiz
Telefon +41 51 285 00 10
andreas.meyer@sbb.ch · www.sbb.ch

Dementsprechend haben wir den Vorentwurf bezüglich Verhältnismässigkeit, Praxistauglichkeit und den Herausforderungen des öffentlichen Verkehrs analysiert und Änderungsbedarf identifiziert. Im Folgenden legen wir unsere wichtigsten Anliegen zu einzelnen Artikeln dar. Für die konkreten Änderungsanträge verweisen wir auf die Anlage.

I. Verhältnismässigkeit

Profiling *(Art. 3 lit. f)*

Die Definition des Profilings ist auf *automatisierte* Auswertungen von Daten oder Personendaten zu beschränken. Die manuelle Erstellung einer Mitarbeiterbeurteilung oder die manuelle Auswertung eines Kundendossiers bedürfen nicht dieses besonders hohen Schutzes, der über das EU-Recht hinausgeht und zu unverhältnismässigem Aufwand führt.

Überprüfung der Daten auf ihre Richtigkeit *(Art. 4 Abs. 5)*

Die Pflicht zur Korrektur oder Ergänzung von Personendaten muss verhältnismässig sein. Die heutige Regelung in Art. 5 Abs. 1 Satz 2 DSG sieht vor, „alle *angemessenen* Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die (…) unrichtig oder unvollständig sind". Dies ist nach wie vor sachgerecht.

Dem Verantwortlichen sollte ferner keine Pflicht zur Vernichtung auferlegt werden, wenn er unrichtige oder unvollständige Personendaten nicht überprüfen kann. Das ist auch eine Frage der Praxistauglichkeit. Personendaten sollten in diesem Fall für die Bearbeitung gesperrt werden können und nicht zwingend vernichtet werden müssen.

Bekanntgabe ins Ausland *(Art. 6 Abs. 1 lit. a)*

Es genügt, wenn die betroffene Person in die Bekanntgabe ihrer Daten ins Ausland generell einwilligt. Eine Einwilligung für jeden *Einzelfall* führt zu unverhältnismässig hohem Aufwand und entspricht keinem klaren Schutzbedürfnis.

Daten einer verstorbenen Person *(Art. 12 Abs. 1 lit. a)*

Es ist zu konkretisieren, dass die verstorbene Person die Einsicht in die Daten zu Lebzeiten gegenüber dem Verantwortlichen nicht ausdrücklich untersagt hat. Ansonsten obliegt es dem Verantwortlichen den Willen des Erblassers umfänglich zu identifizieren, was sehr aufwendig und teils gar nicht möglich sein würde.

Datenschutz-Folgenabschätzung *(Art. 16)*

Nach dem Grundsatz der Verhältnismässigkeit und im Interesse effizienter Verfahren für alle Beteiligten sind Datenschutz-Folgenabschätzungen und entsprechende Meldungen an den Beauftragten nur bei erheblichen Risiken vorzuschreiben.

Meldepflicht bei Datenschutzverletzungen *(Art. 17 Abs. 1)*

Die Meldepflicht des Verantwortlichen gegenüber dem Beauftragten sollte nur bei *hohem* Risiko für Persönlichkeit oder Grundrechte bestehen. Entsprechend dem europäischen Recht ist eine konkrete Frist vorzugeben.

Dokumentation der Datenbearbeitung *(Art. 19 lit. a)*

Die detaillierte Dokumentation jeder Datenbearbeitung, z.B. mit ausführlichen Logs, führt zu einem unverhältnismässigen Aufwand. Das Schutzziel lässt sich auch mit milderen Massnahmen erreichen, beispielsweise mit einem Verzeichnis über die Verarbeitungsaktivitäten. Es gibt keinen Grund, über diese europäische Anforderung hinauszugehen.

II. Praxistauglichkeit

Automatisierte Einzelentscheidung *(Art. 15)*

Es ist unklar, was eine automatisierte Einzelentscheidung ist. Da die daraus resultierenden Verpflichtungen erhebliche Auswirkungen auf künftige Geschäftsmodelle haben, ist eine eindeutige gesetzliche Definition mit einem klar abgegrenzten Anwendungsbereich erforderlich.

Strafbestimmungen *(Art. 50 ff.)*

Die Strafbarkeit fahrlässiger Verletzungen des Datenschutzgesetzes lehnen wir ab. In Kombination mit der mangelnden Bestimmtheit einiger Tatbestände führt dies für Mitarbeitende sowie Unternehmen zu nicht kalkulierbaren und unzumutbaren Risiken; dies zeigt sich insbesondere bei der sehr schwer einzuhaltenden detaillierten Dokumentationspflicht gemäss Art. 19 VE-DSG.

Die strafrechtliche Verantwortlichkeit der handelnden natürlichen Person ist nicht sachgerecht. Vielmehr sind Verwaltungsbussen gegen das Unternehmen, wie sie beispielsweise bei Kartellrechtsverstössen üblich sind, das geeignete Instrument. Statt einer Kann-Bestimmung zur Entlassung der natürlichen Person aus der strafrechtlichen Verantwortlichkeit in bestimmten Fällen ist diese zwingend und für alle Fälle vorzusehen, in denen die Person für ein Unternehmen gehandelt hat.

Übergangsbestimmung *(Art. 59)*

Die angemessene Übergangsfrist von zwei Jahren muss für alle neuen und veränderten Pflichten des Verantwortlichen sowie des Auftragsbearbeiters gelten. Die Herausforderungen, die mit der Totalrevision auf die Unternehmen zukommen, sind stark voneinander abhängig, weshalb unterschiedliche Umsetzungsfristen zu vermeiden sind.

III. Herausforderung öffentlicher Verkehr

Auskunftsrecht über Entscheidungen *(Art. 20 Abs. 1 und 3)*

Die kostenlose Bearbeitung von Auskunftsgesuchen durch die Unternehmen des öffentlichen Verkehrs steht in gewissen Fällen im Missverhältnis zum grossen Aufwand. In diesen Fällen muss der Auskunftsersuchende an den Kosten beteiligt werden können.

Anders als bei der Mehrheit der Wirtschaft findet das Kerngeschäft der Transportunternehmen quasi im öffentlichen Raum statt. So ist die SBB regelmässig mit sehr aufwendigen Auskunftsgesuchen zur Videoüberwachung konfrontiert. Die Transportpolizei muss die entsprechende Videosicherung vornehmen, die Sequenz sichten und aufbereiten, sämtliche Personen im Hintergrund manuell anonymisieren und die Bilder in einem kompatiblen Format auf ein passendes Speichermedium übertragen. Zudem besteht das Risiko, dass beispielsweise Gegner von Videoüberwachungen das System durch gezielte Mehrfachanfragen faktisch lahmlegen.

Zusätzlich ist das Auskunftsrecht der betroffenen Person nach Absatz 3 bei Entscheidungen des Verantwortlichen auf den relevanten Fall der automatisierten Einzelentscheidung zu beschränken.

Wir danken Ihnen für die Kenntnisnahme und Berücksichtigung unserer Anliegen. Für Fragen stehen Ihnen Luca Arnold (luca.arnold@sbb.ch) sowie die Unterzeichnenden gerne zur Verfügung.

Andreas Meyer
CEO SBB AG

Kathrin Amacker
Leiterin Kommunikation
Mitglied der Konzernleitung SBB AG

Anlage:
- Änderungsanträge zum Vorentwurf

Kopie an (per E-Mail):
- Toni Eder, Generalsekretär UVEK, toni.eder@uvek.admin.ch
- Peter Füglistaler, Direktor BAV, peter.fueglistaler@bav.admin.ch
- Dr. Serge Gaillard, Direktor EFV, serge.gaillard@efv.admin.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : SBB AG

Abkürzung der Firma / Organisation : SBB AG

Adresse : Hilfikerstrasse 1, 3000 Bern 65

Kontaktperson : Luca Arnold, Leiter Regulation & Internationales SBB

Telefon : 079 878 66 95

E-Mail : luca.arnold@sbb.ch

Datum : 27. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SBB AG	Für die SBB als vertrauenswürdiger Mobilitätsdienstleister ist der verantwortungsvolle Umgang mit Kundendaten von zentraler Bedeutung. Datennutzung und Datenschutz müssen jedoch in einem ausgewogenen Verhältnis stehen. Um ihren Kunden durchgehende Mobilitätsketten anzubieten, vernetzt sich die SBB noch stärker mit anderen Mobilitätsdienstleistern im In- und Ausland. Wir begrüssen deshalb die Stossrichtung des Vorentwurfs, europäisches Recht soweit nachzuvollziehen, als es für den ungehinderten Datenaustausch zwischen der Europäischen Union und der Schweiz erforderlich ist. Die Regulierung sollte jedoch nicht über das europäische Schutzniveau hinausgehen. Die SBB bedarf wie jedes Unternehmen klarer und gut umsetzbarer rechtlicher Rahmenbedingungen. Einige Bestimmungen des Vorentwurfes genügen dieser Anforderung nicht, weil sie nur mit unverhältnismässigem Aufwand umsetzbar oder für eine direkte Anwendung zu unbestimmt sind. Weiter gilt es auch die Gesamtsystemkosten der Bahn zu berücksichtigen, deren Anstieg wir für Kunden und öffentliche Hand eindämmen müssen. Hier sollte die Vorlage der besonderen Herausforderung des öffentlichen Verkehrs mehr Rechnung tragen. Dementsprechend haben wir den Vorentwurf bezüglich Verhältnismässigkeit, Praxistauglichkeit und den Herausforderungen des öffentlichen Verkehrs analysiert und Änderungsbedarf identifiziert. Im Folgenden legen wir unsere wichtigsten Anliegen zu einzelnen Artikeln dar. Für die konkreten Änderungsanträge verweisen wir auf die Anlage.

	I. Verhältnismässigkeit **Profiling** *(Art. 3 lit. f)* Die Definition des Profilings ist auf *automatisierte* Auswertungen von Daten oder Personendaten zu beschränken. Die manuelle Erstellung einer Mitarbeiterbeurteilung oder die manuelle Auswertung eines Kundendossiers bedürfen nicht dieses besonders hohen Schutzes, der über das EU-Recht hinausgeht und zu unverhältnismässigem Aufwand führt. **Überprüfung der Daten auf ihre Richtigkeit** *(Art. 4 Abs. 5)* Die Pflicht zur Korrektur oder Ergänzung von Personendaten muss verhältnismässig sein. Die heutige Regelung in Art. 5 Abs. 1 Satz 2 DSG sieht vor, „alle *angemessenen* Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die (…) unrichtig oder unvollständig sind“. Dies ist nach wie vor sachgerecht. Dem Verantwortlichen sollte ferner keine Pflicht zur Vernichtung auferlegt werden, wenn er unrichtige oder unvollständige Personendaten nicht überprüfen kann. Das ist auch eine Frage der Praxistauglichkeit. Personendaten sollten in diesem Fall für die Bearbeitung gesperrt werden können und nicht zwingend vernichtet werden müssen. **Bekanntgabe ins Ausland** *(Art. 6 Abs. 1 lit. a)* Es genügt, wenn die betroffene Person in die Bekanntgabe ihrer Daten ins Ausland generell einwilligt. Eine Einwilligung für jeden *Einzelfall* führt zu unverhältnismässig hohem Aufwand und entspricht keinem klaren Schutzbedürfnis. **Daten einer verstorbenen Person** *(Art. 12 Abs. 1 lit. a)* Es ist zu konkretisieren, dass die verstorbene Person die Einsicht in die Daten zu Lebzeiten gegenüber dem Verantwortlichen nicht ausdrücklich untersagt hat. Ansonsten obliegt es dem Verantwortlichen den Willen des Erblassers umfänglich zu identifizieren, was sehr aufwendig und teils gar nicht möglich sein würde.

	Datenschutz-Folgenabschätzung *(Art. 16)* Nach dem Grundsatz der Verhältnismässigkeit und im Interesse effizienter Verfahren für alle Beteiligten sind Datenschutz-Folgenabschätzungen und entsprechende Meldungen an den Beauftragten nur bei erheblichen Risiken vorzuschreiben. **Meldepflicht bei Datenschutzverletzungen** *(Art. 17 Abs. 1)* Die Meldepflicht des Verantwortlichen gegenüber dem Beauftragten sollte nur bei *hohem* Risiko für Persönlichkeit oder Grundrechte bestehen. Entsprechend dem europäischen Recht ist eine konkrete Frist vorzugeben. **Dokumentation der Datenbearbeitung** *(Art. 19 lit. a)* Die detaillierte Dokumentation jeder Datenbearbeitung, z.B. mit ausführlichen Logs, führt zu einem unverhältnismässigen Aufwand. Das Schutzziel lässt sich auch mit milderen Massnahmen erreichen, beispielsweise mit einem Verzeichnis über die Verarbeitungsaktivitäten. Es gibt keinen Grund, über diese europäische Anforderung hinauszugehen. **II. Praxistauglichkeit** **Automatisierte Einzelentscheidung** *(Art. 15)* Es ist unklar, was eine automatisierte Einzelentscheidung ist. Da die daraus resultierenden Verpflichtungen erhebliche Auswirkungen auf künftige Geschäftsmodelle haben, ist eine eindeutige gesetzliche Definition mit einem klar abgegrenzten Anwendungsbereich erforderlich. **Strafbestimmungen** *(Art. 50 ff.)* Die Strafbarkeit fahrlässiger Verletzungen des Datenschutzgesetzes lehnen wir ab. In Kombination mit der mangelnden Bestimmtheit einiger Tatbestände führt dies für Mitarbeitende sowie Unternehmen zu nicht kalkulierbaren und unzumutbaren Risiken; dies zeigt sich insbesondere bei der sehr schwer einzuhaltenden detaillierten Dokumentationspflicht gemäss Art. 19 VE-DSG. Die strafrechtliche Verantwortlichkeit der handelnden natürlichen Person ist nicht sachgerecht. Vielmehr sind Verwaltungsbussen gegen das Unternehmen, wie sie beispielsweise bei Kartellrechtsverstössen üblich sind, das geeignete Instrument.

	Statt einer Kann-Bestimmung zur Entlassung der natürlichen Person aus der strafrechtlichen Verantwortlichkeit in bestimmten Fällen ist diese zwingend und für alle Fälle vorzusehen, in denen die Person für ein Unternehmen gehandelt hat. **Übergangsbestimmung** *(Art. 59)* Die angemessene Übergangsfrist von zwei Jahren muss für alle neuen und veränderten Pflichten des Verantwortlichen sowie des Auftragsbearbeiters gelten. Die Herausforderungen, die mit der Totalrevision auf die Unternehmen zukommen, sind stark voneinander abhängig, weshalb unterschiedliche Umsetzungsfristen zu vermeiden sind. **III. Herausforderung öffentlicher Verkehr** **Auskunftsrecht über Entscheidungen** *(Art. 20 Abs. 1 und 3)* Die kostenlose Bearbeitung von Auskunftsgesuchen durch die Unternehmen des öffentlichen Verkehrs steht in gewissen Fällen im Missverhältnis zum grossen Aufwand. In diesen Fällen muss der Auskunftsersuchende an den Kosten beteiligt werden können. Anders als bei der Mehrheit der Wirtschaft findet das Kerngeschäft der Transportunternehmen quasi im öffentlichen Raum statt. So ist die SBB regelmässig mit sehr aufwendigen Auskunftsgesuchen zur Videoüberwachung konfrontiert. Die Transportpolizei muss die entsprechende Videosicherung vornehmen, die Sequenz sichten und aufbereiten, sämtliche Personen im Hintergrund manuell anonymisieren und die Bilder in einem kompatiblen Format auf ein passendes Speichermedium übertragen. Zudem besteht das Risiko, dass beispielsweise Gegner von Videoüberwachungen das System durch gezielte Mehrfachanfragen faktisch lahmlegen. Zusätzlich ist das Auskunftsrecht der betroffenen Person nach Absatz 3 bei Entscheidungen des Verantwortlichen auf den relevanten Fall der automatisierten Einzelentscheidung zu beschränken.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SBB AG	DSG	3		f	Begriffe Die folgenden Ausdrücke bedeuten: (…) f. Profiling: jede *automatisierte* Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;
SBB AG	DSG	4	5		Grundsätze (…) [5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. *Er hat alle angemessenen Massnahmen zu treffen, um u*nrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, zu ~~*müssen*~~ korrigier~~*t*~~*en* oder *zu* ergänz~~*t werd*~~en. Andernfalls sind die Daten zu vernichten *oder zu sperren*.
SBB AG	DSG	6	1	a	Bekanntgabe ins Ausland in Ausnahmefällen [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: a. die betroffene Person ~~*im Einzelfall*~~ eingewilligt hat;
SBB AG	DSG	12	1	a	Daten einer verstorbenen Person [1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und: a. die verstorbene Person die Einsicht zu Lebzeiten *gegenüber dem Verantwortlichen* nicht ausdrücklich untersagt hat; (…)

SBB AG	DSG	16	1		Datenschutz-Folgenabschätzung [1] Führt die vorgesehene Datenbearbeitung ~~*voraussichtlich*~~ zu einem ~~*erhöht*~~ *hoh*en Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen.
SBB AG	DSG	16	3		(…) [3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen*, wenn ein erhebliches Risiko für die Persönlichkeit oder die Grundrechte festgestellt wurde*.
SBB AG	DSG	17	1		Meldung von Verletzungen des Datenschutzes [1] Der Verantwortliche meldet dem Beauftragten ~~*unverzüglich*~~ *möglichst innerhalb von 72 Stunden* eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem *hohen* Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.
SBB AG	DSG	19	1		Weitere Pflichten [1] Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie *führen ein Verzeichnis zur Dokumentation* ~~*dokumentieren*~~ ihre*r* Datenbearbeitung;
SBB AG	DSG	20	1		[1] Jede Person kann vom Verantwortlichen *grundsätzlich* kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. *In Ausnahmefällen kann der Verantwortliche von der Person eine angemessene Aufwandsentschädigung von bis zu 500 Franken verlangen, insbesondere wenn die Auskunftserteilung mit grossem Aufwand verbunden ist.*
SBB AG	DSG	20	3		(…) [3] ~~*Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere*~~ *Bei* eine*r* automatisierte*n* Einzelentscheidung~~,~~ erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.

SBB AG	DSG	50	4		(…) 4 ~~*Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.*~~
SBB AG	DSG	51	2		(...) 2 ~~*Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.*~~
SBB AG	DSG	53			Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen *wird* Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt ~~*werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungs-massnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären*~~.
SBB AG	DSG	59		a./b.	Übergangsbestimmungen *Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die ~~für~~ Verantwortlichen sowie der Auftragsbearbeiter ~~in der Lage sein:~~ die im Verhältnis zum Bundesgesetz über den Datenschutz vom 19. Juni 1992 mit Stand am 1. Januar 2014 neuen Pflichten erfüllen.* ~~*a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen;*~~ ~~*b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen*~~

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
SBB AG	Keine Bemerkungen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
SBB AG	Keine Bemerkungen

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
SBB AG	Keine Bemerkungen	

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
SBB AG	Keine Bemerkungen	

Jonas Amstutz
Office fédéral de la justice
Bundesrain 20
CH – 3003 Berne

Lausanne, le 24 mars 2017

Réponse de Swiss Biobanking Platform à la consultation avant-projet de la révision de la loi fédérale sur la protection des données

Madame, Monsieur,

Nous vous remercions de nous avoir invités à nous exprimer dans le cadre de la consultation sur l'avant-projet de la révision de la loi fédérale sur la protection des données (LPD).

La Swiss Biobanking Platform (SBP) est une initiative du Fonds National Suisse qui favorise la coordination nationale des biobanques dans le domaine humain et non-humain.
La mission de la plateforme est de fournir le soutien nécessaire aux hôpitaux et autres institutions universitaires suisses dans la construction et la gestion de leurs biobanques en proposant des services et prestations qui répondent aux besoins de la recherche biomédicale et aux défis de santé publique.

Remarques générales
La SBP accueille cette révision de façon très favorable. Nous considérons que ces modifications sont nécessaires et urgentes pour le développement d'un standard de protection des données élevé, répondre aux exigences en matière de libre circulation des données entre la Suisse et l'étranger, rendre le traitement de données plus transparent et renforcer le droit de chacun à disposer de ses propres données.

Cependant, selon SBP, deux points méritent une attention particulière:
1) Dans le contexte actuel, aucune loi sur les biobanques n'encadre l'utilisation d'échantillons biologiques et leurs données associées si ceux-ci ne font pas l'objet d'une réutilisation pour la recherche au sens de la LRH. Or, en pratique, il existe différents types de biobanques (par ex. diagnostique, thérapeutique) dont l'objectif principal n'est pas la recherche. Aussi, l'occasion de la révision de la LPD pourrait être saisie pour combler ce vide juridique en attendant l'adoption d'une loi fédérale sur les biobanques (Motion déposée par Rebecca Ruiz le 17 mars 2017). L'inclusion des échantillons biologiques et de leurs données associées au champ d'application de la

LPD permettrait ainsi de garantir un cadre légal et une protection minimale à ces données personnelles de santé.

Pour ce faire, nous vous rendons attentifs à la déclaration de Taipei sur les considérations éthiques relatives aux bases de données de santé et des biobanques adoptée par la World Medical Association (WMA) en Octobre 2016 et vous suggérons d'intégrer à cette révision les principes de gouvernance ainsi que les points relatifs à la protection des données.

2) A l'ère du « Big Data » et de la digitalisation, il nous semble important de souligner que le concept d'anonymisation des données devrait être appréhendé de manière avisée, en particulier en matière de données personnelles liées à la santé. En effet, avec les progrès des techniques utilisées en génétique, il n'est - aujourd'hui déjà - pas possible de garantir absolument l'anonymat des échantillons et des données. L'environnement des big data évolue rapidement et il est essentiel d'apporter un cadre juridique à la collecte et utilisation de ces données. Ce constat nécessite donc d'anticiper et prévoir dès à présent, dans le contexte de cette révision, les garde-fous nécessaires liés à ces évolutions en matière de traitement de données liées à la santé.

Commentaires particuliers

Le domaine d'application de la LPD est vaste. La SBP ne prend position ici que pour son domaine de compétence : la recherche. Aussi, les commentaires ci-dessous ne s'appliquent qu'à ce cadre précis.

1. Comme le champ d'application (Art. 2) n'exclut pas la recherche, la complémentarité avec la loi en vigueur sur la recherche sur l'être humain (LRH) n'est pas suffisamment explicite et certains points demandent à être clarifiés :

- Art. 3 Définitions, point c : Dans la définition des données personnelles sensibles, les données génétiques et les données liées à la santé sont considérées au même niveau de sensibilité alors que dans la LRH, les données génétiques sont considérées plus sensibles que les autres. En effet, le caractère identifiant et prédictif des données génétiques, ainsi que leur pérennité devraient impliquer une réflexion globale sur les risques augmentés qu'elles comportent et il conviendrait donc d'anticiper et prévoir dès à présent, dans le contexte de cette révision, les mesures nécessaires à la protection de ce type de données sensibles.

- Art. 4 Principes, al. 6 : Lorsque son consentement est requis pour justifier le traitement de données sensibles, la personne concernée ne consent valablement que si son consentement est au surplus exprès ce qui est plus contraignant que les exigences de la LRH (Art. 33, al. 2) qui permet l'utilisation à des fins de recherche sous une forme codée des données personnelles non génétiques liées à la santé si le patient a été informé et ne s'y est pas opposé (principe de la non opposition).

2. Art. 20, Droits d'accès, al. 4 : « *Des données personnelles sur la santé de la personne concernée peuvent lui être communiquées par l'intermédiaire d'un médecin qu'elle aura désigné.* »
Nous trouvons trop restrictif de limiter le retour de résultats au médecin désigné par le participant et proposons d'élargir à d'autres profils habitués dans leur pratique à traiter de questions sensibles (par ex. médecins traitant, généticien, psychologue).

3. Art. 24 Motifs justificatifs, point e1 et Art. 32 Traitements à des fins de recherche, de planification et de statistique, al. 1a :

- Les données personnelles peuvent être traitées à des fins de recherche si elles sont rendues anonymes dès que le but du traitement le permet. La notion d'anonymisation ne devrait être utilisée que pour des projets de recherche où le retour vers le patient n'est pas attendu, notamment en recherche fondamentale. Il serait donc bien de préciser de quel type de recherche il est question dans ces articles 24 et 32. En effet, dans le cadre de la recherche biomédicale, on encourage l'utilisation des données (ou matériel biologique) sous forme codée afin de garantir une ré-identification possible en cas de résultats fortuits significatifs pour la santé du patient.

- De plus, « *les organes fédéraux sont en droit de traiter des données personnelles à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, si les conditions suivantes sont réunies :*
  a. les données sont rendues anonymes dès que le but du traitement le permet;
  b. l'organe fédéral ne communique des données sensibles à des personnes privées que sous une forme ne permettant pas d'identifier les personnes concernées. »

Nous trouvons les conditions a et b contradictoires.

4. Art. 29 Communication de données personnelles, al. 4 : « *Ils sont en droit de communiquer, sur demande, le nom, le prénom, l'adresse et la date de naissance d'une personne même* ***si les conditions des al. 1 ou 2 ne sont pas remplies****.* »
Nous ne comprenons pas bien ce que cela implique pour le patient et trouvons ce paragraphe contradictoire si l'on considère **l'alinéa 2** : « *En dérogation à l'al. 1, les organes fédéraux peuvent exceptionnellement, dans un cas d'espèce,* ***communiquer des données personnelles si l'une des conditions suivantes est remplie****.* »

Nous vous prions de bien vouloir tenir compte de nos remarques et nous tenons volontiers à votre disposition pour toute question.

En vous remerciant par avance, nous vous prions, Madame, Monsieur, de bien vouloir agréer nos meilleures salutations.

C. Currat

Christine Currat
Directrice Exécutive

SwissBanking

Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
CH-3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

Basel, 4. April 2017
J.001/AER/LWI

Stellungnahme SBVg: Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Sehr geehrter Herr Amstutz

Wir beziehen uns auf die Einladung vom 21. Dezember 2016 zur Stellungnahme betreffend Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz.

Für die Konsultation in dieser für die Finanzbranche sehr wichtigen Angelegenheit bedanken wir uns bestens. Gerne nehmen wir die Gelegenheit zur Stellungnahme wahr und unterbreiten Ihnen wunschgemäss im beiliegenden Formular unsere Anliegen.

Wir danken Ihnen für die Kenntnisnahme unserer Stellungnahme und die Berücksichtigung unserer Überlegungen für die weiteren Arbeiten. Gerne stehen wir Ihnen für ergänzende Auskünfte zur Verfügung.

Freundliche Grüsse
Schweizerische Bankiervereinigung

Andrew Ertl Martin Hess

Beilage: Stellungnahme im Formular des EJPD

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schweizerische Bankiervereinigung

Abkürzung der Firma / Organisation : SBVg

Adresse : Aeschenplatz 7, Postfach 4182, 4002 Basel

Kontaktperson : Dr. Andrew Ertl

Telefon : 061 295 92 54

E-Mail : andrew.ertl@sba.ch

Datum : 4. April 2016

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SBVg	Wir anerkennen den Revisionsbedarf des aus dem Jahr 1992 stammenden Datenschutzgesetzes (DSG) und unterstützen den Bundesrat in seinem Anliegen, dessen Bestimmungen sowohl den veränderten technologischen und gesellschaftlichen Rahmenbedingungen anzupassen als auch auf die Rechtsentwicklungen auf europäischer Ebene abzustimmen. An mehreren Stellen scheint uns der Vorentwurf (VE-DSG) jedoch einseitig auf die vermeintlichen Interessen der betroffenen Personen abzustellen, was weder zweckmässig sein kann noch dem prinzipienbasierten Schweizer Rechtsverständnis entspricht und in der Folge – ohne Mehrwert zu schaffen – den Unternehmen unverhältnismässig hohe Umsetzungskosten aufbürdet. Zudem finden sich im VE-DSG auch Bestimmungen, die stark in die unternehmerischen Freiheiten eingreifen und in der Praxis nicht umsetzbar sind, was wiederum zu unerwünschten Rechtsunsicherheiten führt.
SBVg	Bestehende Konzepte und Begrifflichkeiten sind weggefallen, insbesondere die Rolle des Datenschutzbeauftragten und der Begriff der „Datensammlung“. Dies führt bei Unternehmen zu Unklarheiten in der Zuweisung von Aufgaben, Kompetenzen und Verantwortlichkeiten an eine oder mehrere Personen in der Umsetzung der Bestimmungen des DSG und zu Auslegungsschwierigkeiten bei der Zuordnung von Daten. In diesem Zusammenhang weisen wir auch darauf hin, dass in der französischen und deutschen Version unterschiedliche Begrifflichkeiten verwendet werden. Eine sorgfältige Abstimmung ist gerade bei einer solch weitreichenden Gesetzgebung zwingend.
SBVg	Um internationalen resp. europäischen Standards gerecht zu werden, bedarf es keiner Gesetzesreform dieses Umfanges. Die europäische Datenschutz-Grundverordnung (DSGVO) verlangt denn auch keine pauschale Übernahme ihrer Bestimmungen, vielmehr hält sie ausdrücklich fest, dass in Bezug auf den zu erneuernden Angemessenheitsbeschluss die Umsetzung des revidierten Übereinkommens zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (ERK 108) ein wesentlicher Faktor ist. Vor diesem Hintergrund muss sich der VE-DSG primär an der ERK 108 orientieren. Dagegen wäre eine Verschärfung gegenüber ERK 108 und DSGVO konzeptionell falsch, nicht notwendig und überdies kontraproduktiv, weil ein solcher „Swiss Finish“ einen einheitlichen internationalen „Datenraum“ verhindern und zulasten schweizerischer Unternehmen wettbewerbsverzerrend wirken würde.
SBVg	Der VE-DSG sieht für den Verantwortlichen und neu auch für den Auftragsbearbeiter zahlreiche verschärfte Prüf- und Meldepflichten vor. Das Gesamtpaket dieser Pflichten mag für spezifische Marketing-Dienstleister und Data-Miner angemessen sein, da sie im Rahmen eines eng begrenzten Geschäftsmodells typischerweise besonders sensible Datenbearbeitungen vornehmen. Für den Verantwortlichen und den

	Auftragsbearbeiter, welche ständig und in enormem Volumen Daten in Zusammenhang mit Ausführung von Kundenaufträgen und aufgrund aufsichtsrechtlicher Vorgaben an zahllose Empfänger weitergeben müssen, ist die pauschale Anwendung solcher strengen Regeln unbesehen der Sensibilität der betroffenen Daten nicht sachgerecht. Sie führen nicht zu besserem Datenschutz, sondern lediglich zu unnötigem Aufwand und zu einer Flut von Meldungen an den Beauftragten.
SBVg	Rechtsnatur, Konzept und Durchsetzung des Sanktionenregimes des VE-DSG geht über die ERK 108 sowie über die DSGVO hinaus. Die in Art. 50 ff. VE-DSG enthalten Strafbestimmungen für einzelne Individuen führen zusammen mit der erheblichen Unbestimmtheit der Straftatbestände zu einer nicht zu rechtfertigenden Bedrohung derjenigen Personen, die unternehmensintern die Einhaltung des Datenschutzes sicherstellen müssen. Das europäische Recht sieht Sanktionen lediglich auf Ebene der Unternehmen vor. Mit dem vorgeschlagenen Strafrechtspaket wären die gesamte Wirtschaft und insbesondere die einzelnen Personen, die mit Personendaten umzugehen haben, zu Unrecht mit unabsehbaren strafrechtlichen Risiken belastet. Dies hätte wohl erhebliche, heute noch nicht überblickbare Auswirkungen auf den Wirtschaftsstandort Schweiz. Es stellt sich sich die Frage, ob die mit Strafe bedrohten Sachverhalte überhaupt strafwürdig sind. In Bezug auf die fahrlässige Tatvariante ist dies aus unserer Sicht klar zu verneinen. Im Übrigen dürften die bestehenden Mechanismen im StGB (z.B. Art. 143 StGB, Art. 162 StGB, Art. 273 StGB) und in spezialgesetzlichen Regelungen (z.B. Art. 47 BankG, Art. 43 BEHG), welche einer Persönlichkeitsverletzung entgegengehalten werden können, für die Begründung der Strafbarkeit ausreichen. Aufgrund der Masse der Daten, die schon nur aufgrund gesetzlicher Pflichten bearbeitet werden müssen, lassen sich insbesondere bei grossen Unternehmen einzelne Pflichtverletzungen kaum verhindern. Würde hier jedes Mal der Strafrichter angerufen, wäre dies völlig unverhältnismässig. Die persönliche Strafbarkeit von Mitarbeitern scheint uns nicht angebracht. Dies ist angesichts des erweiterten Tatbestandes auch auf Fahrlässigkeit äusserst problematisch. Jeglicher Umgang mit Personendaten wäre somit stets potentiell strafrechtlich relevant. Dies würde derart in den Arbeitsalltag gewöhnlicher Mitarbeiter eingreifen, dass normale Arbeitsprozesse kaum mehr bewältigt werden könnten. Sämtliche an einer Datenbearbeitung beteiligten Mitarbeitenden würden pauschal kriminalisiert und dadurch in ihrer beruflichen sowie gesellschaftlichen Existenz bedroht. Dies würde gerade in Dienstleistungsbetrieben einen grossen Teil der Mitarbeitenden betreffen. Schliesslich stellt das Sanktionenregime des VE-DSG ein gravierendes Hindernis auf dem Weg zum angestrebten Angemessenheitsentscheid der EU-Kommission dar. Damit der vorgenannte Entscheid positiv ausfällt, müssen Sanktionen wegen Verstössen gegen die DSGVO auch in der Schweiz vollstreckt werden können. Damit hierfür der ordentliche Amts- bzw. Rechtshilfeweg beschritten werden kann, muss die Voraussetzung der sog. doppelten Strafbarkeit erfüllt werden können. Mit anderen Worten müssen die fraglichen Verstösse, in deren Zusammenhang Amts- bzw. Rechtshilfe ersucht wird – unter der Annahme, sie wären in der Schweiz verübt worden – auch nach schweizerischem Recht sanktionierbar sein. Aufgrund der Unvereinbarkeit der beiden Sanktionenregime wäre das jedoch klar nicht möglich.

	Economiesuisse hat einen Vorschlag für das Sanktionsmodell im DSG erarbeitet, in welchem nicht Sanktionen gegen Individuen, sondern Verwaltungsstrafen gegen Unternehmen im Vordergrund stehen. Dieser Vorschlag erscheint uns als sinnvolle Alternative zum jetzigen Sanktionenregime im VE-DSG, weshalb wir auf diesen verweisen und sinngemäss unterstützen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SBVg	DSG	1			Die Bearbeitung von Personendaten ist Bestandteil und Voraussetzung nicht nur der erfolgreichen Digitalisierung der schweizerischen Wirtschaft und Gesellschaft, sondern überhaupt jeder wirtschaftlichen Tätigkeit. Infolgedessen muss das neue DSG bei der Bearbeitung von Personendaten auch gesamtwirtschaftliche und gesellschaftliche Interessen berücksichtigen. Dies würde auch der Zielsetzung der DSGVO entsprechen und stünde im Einklang mit der Strategie des Bundesrates für eine digitale Schweiz. Es ist zudem falsch, von einem Schutz „der Grundrechte“ von natürlichen Personen zu sprechen. Das entspricht zwar mehr oder weniger der Regelung der DSGVO. Das europäische Recht kennt aber eine direkte Drittwirkung der Grundrechte, die dem schweizerischen Recht fremd ist. Es ist nicht Aufgabe privater Datenbearbeiter, die Grundrechte betroffener Personen zu schützen, soweit diese Grundrechte nicht in den einzelnen Anforderungen des DSG Ausdruck gefunden haben. Dazu kommt, dass völlig unklar ist, um welche Grundrechte es geht und welche Risiken dabei relevant wären. Anpassungsvorschlag: Dieses Gesetz bezweckt den Schutz der Persönlichkeit ~~und der Grundrechte~~ von natürlichen Personen, über die Daten bearbeitet werden, und die Förderung der Rahmenbedingungen der digitalen Wirtschaft.
SBVg	DSG	2	1		Der Anwendungsbereich des VE-DSG sollte klar auf diejenigen Personendaten beschränkt werden, die in einem Dateisystem abgespeichert sind oder sich in einem solchen befinden (vgl. dazu unten bei Art. 3 c^{bis} (neu) unseren Vorschlag in Bezug auf die Begriffsbestimmung „Dateisystem“). Anderenfalls wäre insbesondere die Bearbeitung von Auskunftsersuchen der betroffenen Person nicht handhabbar und einem solchen könnte nie präzise und vollständig nachgekommen werden. In Anlehnung an die DSGVO (Art. 2 Abs. 1 DSGVO) schlagen wir folgende Textänderung vor:

					Anpassungsvorschlag: Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen, die sich in einem Dateisystem befinden, durch:
SBVg	DSG	2	2	a	Heute werden „persönliche Unterlagen“ überwiegend in elektronischer Form verwaltet. Aufgrund der technischen Ausgestaltung solcher Speicherorte ist es ohne übermässigen Aufwand nicht möglich, den Zugriff durch Dritte (z.B. aus Wartungsgründen) auszuschliessen. Aus diesem Grund ist die Anknüpfung des Ausschlussgrundes am Merkmal der Bearbeitung nicht mehr sachgerecht. Richtigerweise muss er sich am Willen des Bearbeiters (Erstellers) orientieren. Legt ein Mitarbeiter eine persönliche Notiz in seinem „privaten/persönlichen“ Ordner im Netzwerk seines Arbeitgebers ab, muss diese von der Anwendung des DSG ausgeschlossen werden, auch wenn z.B. der technische Support die Möglichkeit hätte, darauf zuzugreifen. Anpassungsvorschlag: Personendaten, die durch eine natürliche Person ausschliesslich zum Zweck des persönlichen Gebrauchs bearbeitet werden;
SBVg	DSG	2	2	e (neu)	Die Abschaffung des Datenschutzes für juristische Personen im Einklang mit den europäischen Normen ist zu begrüssen. Dabei gilt es jedoch zu berücksichtigen, dass Unternehmen in der Regel durch natürliche Personen vertreten werden, die im Namen und für Rechnung des Unternehmens handeln. Bei Datenbearbeitungen durch Unternehmen werden daher oftmals zwangsläufig auch Daten von Arbeitnehmern des betreffenden Unternehmens bearbeitet (z.B. Erfassung von Namen von verantwortlichen Kundenberatern). Diese Arbeitnehmerdaten dem Datenschutz zu unterstellen, wäre sachlogisch falsch und ein Widerspruch zur Tatsache, dass Unternehmen keinen Datenschutz mehr geniessen sollen. Deshalb ist im Gesetz klar zu statuieren, dass Personendaten von Arbeitnehmern, die im Zusammenhang mit der Ausübung ihrer beruflichen Tätigkeit für den Verantwortlichen oder den Auftragsbearbeiter bearbeitet werden, dem VE-DSG nicht unterstellt sind. Dementsprechend ist auch Art. 328 lit. b OR und der dort beinhaltete Verweis auf das DSG anzupassen. Anpassungsvorschlag: Personendaten eines Arbeitnehmers, der für den Verantwortlichen oder den Auftragsbearbeiter tätig ist,

					sofern die bearbeiteten Personendaten des Arbeitnehmers im Zusammenhang mit der Ausübung seiner beruflichen Tätigkeit für den Verantwortlichen oder den Auftragsbearbeiter stehen;
SBVg	DSG	2	2	f (neu)	Sobald Gerichtsverfahren anhängig sind, stellen die anwendbaren Verfahrensregeln sicher, dass die Persönlichkeitsrechte der Parteien gewahrt werden. Die Ausweitung der Anwendbarkeit des DSG auf hängige Gerichtsverfahren für Parteien (nicht jedoch für Gerichte) ist unnötig und unverhältnismässig. Das wird zur Folge haben, dass während hängiger Verfahren das Auskunftsrecht zur (datenschutzrechtlich nicht vorgesehenen) Beweisbeschaffung zweckentfremdet wird: einerseits ist es kostenlos, andererseits können die (hohen) Hürden der ZPO (z.B. für Editionsbegehren) umgangen werden. Anpassungsvorschlag: hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren.
SBVg	DSG	2	3		Wir würden es begrüssen, wenn der Begriff „der Beauftragte“ zusammen mit den weiteren Begriffserklärungen in Art. 3 VE-DSG festgehalten würde. Vgl. Ausführungen zu Art. 3 lit. k (neu).
SBVg	DSG	3		a	Nach der heutigen Definition umfassen Personendaten diejenigen Informationen, die – in welcher Form auch immer – auf eine Person schliessen lassen. Im Rahmen des Bankgeschäfts sind somit sämtliche Belege, jeder Ausweis, jede Adressmutation etc. als Personendaten zu qualifizieren. Angesichts der im VE-DSG vorgesehenen erheblichen Ausweitung der Pflichten bei der Datenbearbeitung (beispielsweise Informationspflicht bei der Beschaffung, Auskunftsrecht der betroffenen Person oder Pflicht der Vernichtung von Personendaten) muss in Anlehnung an die DSGVO der Anwendungsbereich des VE-DSG klar eingeschränkt und die Bestimmung des Begriffs „Dateisystem“ in den VE-DSG aufgenommen werden (vgl. dazu unsere Vorschläge zu Art. 2 Abs. 1 sowie Art. 3 c^{bis} (neu) VE-DSG). Es stellt sich zudem die Frage, wann einzelne Daten durch Herstellung von Verbindungen, Profilierungen etc. zu Personendaten im Sinne des VE-DSG werden. Dies führt zwangsläufig zu Abgrenzungsschwierigkeiten und verursacht Rechtsunsicherheit. Wir verstehen anhand der Ausführungen im erläuternden Bericht nicht, welche konkrete Daten beim Profiling ausgenommen sind. Schliesslich weisen wir darauf hin, dass die zentralen Begriffe „Personendaten“ und „Daten“ im DSG

					nicht konsistent verwendet werden. Dies führt in der Anwendung der Bestimmungen des DSG zu Rechtsunsicherheit bzw. Auslegungsschwierigkeiten.
SBVg	DSG	3		c	„Besonders schützenswerte Daten“ werden auf genetische und biometrische Daten einer natürlichen Person ausgedehnt. Aufgrund der Begriffsverwendung „genetische/biometrische Daten“ in anderen Gesetzen stellt sich hier die Frage, wie diese Begriffe im Zusammenhang mit dem Datenschutz zu verstehen sind. Im Ergebnis sollten damit Daten gemeint sein, welche den Zweck der Identifizierung decken (vgl. auch Art. 4 Ziff. 14, 9 Abs. 1 und ErwG 51 DSGVO). Der Wortlaut des Gesetzes widerspricht zudem den Erläuterungen im Bericht. Diese sehen vor, dass nur diejenigen biometrischen Daten als besonders schützenswerte Personendaten qualifiziert werden sollen, die (mit besonderen technischen Mitteln) zum Zweck bearbeitet werden, eine natürliche Person eindeutig zu identifizieren. Im Übrigen entspricht dies auch der Auffassung der Konvention 108 und sollte sich analog im Gesetzeswortlaut des VE-DSG wiederspiegeln. Anpassungsvorschlag: 4. biometrische Daten, die zum Zweck der Personenidentifikation bearbeitet werden. ~~eine natürliche Person eindeutig identifizieren~~
SBVg	DSG	3		c[bis] (neu)	In Anlehnung an die europäische Datenschutzgesetzgebung sollte in der revidierten Version des DSG eine Definition des Begriffs „Dateisystem“ eingefügt werden (direkt nach der Begriffsbestimmung „besonders schützenswerte Personendaten“), die den Anwendungsbereich auf zwei Konstellationen von Personendaten limitiert: Daten von natürlichen Personen, die in einem elektronisch geführten Dateisystem gespeichert sind oder dort gespeichert werden sollen (vgl. Art. 2 Abs. 2 und Art. 3 Ziff. 6 RL-EU 2016/680; Art. 2 Abs. 1 und Art. 4 Ziff. 6 DSGVO). Anderenfalls werden die Bestimmungen des VE-DSG kaum vollständig umsetzbar sein, da weder die vorgesehenen Informationspflichten seitens des Verantwortlichen noch die Auskunftsrechte der betroffenen Person vollständig erfüllt werden können und erhebliche Rechtsunsicherheit ausgelöst wird. Infolge der heute vorherrschenden technologischen Gegebenheiten und Möglichkeiten wird kein Verantwortlicher gewährleisten können, dass z.B. Mitarbeiter des Unternehmens, in Bezug auf ihre Kunden, nicht eigene elektronische Notizen machen, die Personendaten des Kunden i.S.d. VE-DSG beinhalten. Physische Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind, sollten nicht in den

					Anwendungsbereich des VE-DSG fallen (vgl. Nr. 15 der in Bezug auf DSGVO in Erwägung stehenden Gründe). Ausnahmen dazu würden zum Beispiel Kontoeröffnungsdokumente oder vom Kunden im Rahmen der Geschäftsbeziehung unterzeichnete Formulare bilden, die zentral, z.B. unter der kundenspezifischen Kontonummer, aufbewahrt werden. Anpassungsvorschlag: *Dateisystem*: Strukturierte Sammlung von Daten, unabhängig davon, ob diese zentral, dezentral, gemäss definierten Kriterien oder ohne Berücksichtigung von definierten Gesichtspunkten geordnet geführt wird;
SBVg	DSG	3		d	Eine vollständige Löschung bzw. Vernichtung von Personendaten ist aufgrund von technischen Restriktionen nur mit erheblichem Aufwand umsetzbar. Eine Standardsoftware unterstützt nicht das vollständige Löschen von Kundendaten, sondern lediglich deren Inaktivierung zwecks Sicherstellung einer konformen Historisierung. Die Anforderung muss lauten, dass die Daten nicht mehr angezeigt oder weitergeleitet werden können. Anpassungsvorschlag: *Bearbeiten*: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder ~~Löschen oder Vernichten~~ Unzugänglichmachen von Daten.
SBVg	DSG	3		f	Die Definition von Profiling ist zu breit und geht massiv über die Vorgaben der DSGVO hinaus. Bereits eine „von Hand“ bearbeitete Mitarbeiterbeurteilung würde als „Profiling“ nach Art. 23 Abs. 2 lit. d. und damit per se als Persönlichkeitsverletzung gelten. Konsequenterweise müsste ein Bearbeiter vor jeder Bearbeitung einen Rechtfertigungsgrund aufweisen können, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden wäre. Dies stellt einen unnötigen und grundlosen partiellen Paradigmenwechsel im schweizerischen Datenschutzrecht dar. Warum eine im Geschäftsverkehr übliche Auswertung von Personendaten spezielle Schutzanforderungen erfordert, ist unseres Erachtens nicht schlüssig dargelegt worden. Solange Transparenz über die Bearbeitung besteht, sollten keine weitergehenden Voraussetzungen an die Auswertung der Personendaten gestellt werden. Möglicherweise besteht ein erhöhtes Schutzbedürfnis im Bereich der besonders schützenswerten Daten, weshalb wir vorschlagen, das Profiling auf diese Art der Daten zu beschränken. Zudem umfasst „Profiling“ gemäss VE-DSG auch das Bearbeiten von nicht-personenbezogenen Daten, was eine unzulässige Ausweitung des Geltungsbereichs des DSG darstellt und im Widerspruch zu Art. 2

					Abs. 1 VE-DSG steht. Schliesslich ist eine Analyse bzw. Auswertung noch keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte der betroffenen Personen auswirkt. Richtigerweise ist der Begriff „Auswertung“ durch „Bewertung“ zu ersetzen, denn erst diese stellt einen schützenswerten Eingriff in die Persönlichkeitsrechte der betroffenen Personen dar. „Bewertung“ umfasst eine Entscheidung, die sich auf eine Analyse bzw. Auswertung stützt. Die Anknüpfung an die Auswertung greift demnach zu weit. Anpassungsvorschlag: *Profiling*: ~~jede~~ automatisierte ~~Auswertung~~ Bewertung von ~~Daten oder~~ besonders schützenswerten Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität. Die Auswertung von subjektiven Beurteilungen einer betroffenen Person stellt kein Profiling dar;
SBVg	DSG	3		h	Die Umschreibung des „Verantwortlichen“ ist zu generell und umfassend, insbesondere muss separat definiert werden, wer unter „private Person“ zu verstehen ist (vgl. dazu unseren Vorschlag zu Art. 3 lit. l (neu)). Es ist zudem unklar, mit welchen Rechten und Pflichten der Verantwortliche bzw. die für das Unternehmen handelnde natürliche Person ausgestattet werden soll. Wir schlagen vor, dass die Umschreibung des „Verantwortlichen“ auf die Ebene des Unternehmens sowie auf die Ebene der für das Unternehmen handelnden Person erweitert wird.
SBVg	DSG	3		j (neu)	Im Hinblick auf die Verwendung des Begriffs „beteiligter Dritter“ im Rahmen des Art. 47 VE-DSG, der die Amtshilfe zwischen schweizerischen und ausländischen Behörden regelt, sollte der Begriff „beteiligter Dritter“ in Art. 3 formell definiert werden, um Missverständnissen mit einer gewissen Tragweite vorzubeugen. Wir schlagen vor, den Begriff „beteiligter Dritter“ in Anlehnung an die DSVGO (vgl. Art. 4 Ziff. 10) unter einem neuen Buchstaben in Art. 3 zu definieren und direkt nach der aktuellen Begriffsbestimmung „Auftragsbearbeiter“ einzufügen. Anpassungsvorschlag: *Beteiligter Dritter:* Bundesorgan oder private Person, ausser die betroffene Person, der Verantwortliche, der Auftragsbearbeiter und Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsbearbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

SBVg	DSG	3		k (neu)	Anpassungsvorschlag: *Beauftragte(r):* Eidgenössische(r) Datenschutz- und Öffentlichkeitsbeauftragte(r);
SBVg	DSG	3		l (neu)	Ebenfalls um Missverständnissen vorzubeugen, dass unter dem Begriff „private Person“ nur natürliche Personen und nicht auch andere Personen, die miteinander in einer privatrechtlichen Beziehung stehen, wie z.B. juristische Personen, zu verstehen sind, sollte der Begriff „private Person“ unter einem neuen Buchstaben definiert werden. Eine entsprechende Definition findet sich auch in der DSVGO (vgl. Art. 4 Ziff. 7 und 8). Anpassungsvorschlag: *Private Person:* Natürliche Person und juristische Personen des privaten Rechts;
SBVg	DSG	3		m (neu)	Wir empfehlen, die im Erläuterungsbericht verwendete Begrifflichkeit der „automatisierten Einzelentscheidung“ (vgl. Kapitel 8.1.3.3) in Konformität mit der DSGVO in Art. 3 VE-DSG zu definieren. Anpassungsvorschlag: *Automatisierte Einzelentscheidung*: Eine automatisierte Einzelentscheidung liegt vor, wenn ohne menschliches Dazutun eine Bewertung von Daten erfolgt, die zu einer konkreten Entscheidung gegenüber der betroffenen Person führt.
SBVg	DSG	4	3		Gemäss Erläuterungsbericht soll die Regelung des Grundsatzes von Treu und Glauben gemäss Art. 4 VE-DSG materiell keine Änderungen gegenüber der aktuellen Fassung gemäss Art. 4 DSG enthalten (Erläuterungsbericht, S. 45 f.). Entgegen dieser Aussage wird nun aber in Art. 4 Abs. 3 VE-DSG der Grundsatz der „Erkennbarkeit“ mit dem Zusatz „klarer“ Erkennbarkeit verschärft. Wir anerkennen den grundsätzlich nötigen Anpassungsbedarf an die DSGVO, sehen im zusätzlichen Adjektiv „klar“ jedoch keinen Mehrwert. Vielmehr wird die Regelung dadurch auslegungsbedürftiger und produziert damit gegenüber der bestehenden bewährten Fassung von Art. 4 Abs. 3 DSG unnötigerweise Rechtsunsicherheit. Grundsätzlich gehen wir davon aus, dass bei Banken die Beschaffung der Daten und der Zweck der Bearbeitung aus den Umständen erkennbar sind. Anpassungsvorschlag: Personendaten dürfen nur zu einem bestimmten und für die betroffene Person ~~klar~~ erkennbaren Zweck

					beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.
SBVg	DSG	4	4		Abs. 4 ist unseres Erachtens obsolet, da sich die Dauer der Aufbewahrungspflicht bereits aus Abs. 2 (Verhältnismässigkeitsprinzip) ergibt, weshalb wir die ersatzlose Streichung des Art. 4 Abs. 4 VE-DSG beantragen. Sollte das Bundesamt für Justiz wider Erwarten auf die ersatzlose Streichung von Art. 4 Abs. 4 VE-DSG verzichten, müsste eine Anpassung des Wortlauts vorgenommen werden, da in der Schweiz andere zwingende gesetzliche Vorschriften, welche die Dauer von Aufbewahrungspflichten oder Dokumentationspflichten regeln, wie z.B. Art. 958 lit. f OR oder Art. 7 GwG, dem entgegenstehen können. Ausserdem ist zu berücksichtigen, dass ein Verantwortlicher aufgrund von z.B. gerichtlichen, verwaltungsrechtlichen oder aufsichtsrechtlichen Verfügungen verpflichten werden kann, Daten nicht zu vernichten. Dies oftmals sogar für eine Dauer, die über den gesetzlich vorgeschriebenen Zeitraum der Aufbewahrungs- oder Dokumentationspflicht hinausgeht (siehe z.B. „Madoff-Verfahren“; „US-Programm“). Schliesslich darf auch nicht ausser Acht gelassen werden, dass der Vernichtung der Daten ein überwiegendes Interesse Dritter, inklusive des Verantwortlichen, entgegenstehen kann. Zu denken wäre in diesem Zusammenhang an gegen Dritte (z.B. Kunden einer Bank) oder gegen den Verantwortlichen gerichtete gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfahren, im Rahmen welcher der Dritte oder der Verantwortliche die Personendaten einer betroffenen Person zur Wahrung seiner jeweils eigenen Interessen benötigt. Anpassungsvorschlag: Sofern anderweitige gesetzliche oder aufsichtsrechtliche Vorschriften nichts anderes vorsehen oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter nicht entgegenstehen, dürfen Personendaten ~~dürfen~~ nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.
SBVg	DSG	4	5		Entgegen dem Erläuterungsbericht (S. 47) erfolgt nicht nur die Übernahme der bewährten Grundsätze gemäss bestehendem Art. 5 DSG. Vielmehr führt die gewählte Formulierung von Art. 4 Abs. 5 VE-DSG zu einer unnötigen Verschärfung des Pflichtenhefts. Statt der Pflicht zur Überprüfung der Richtigkeit der

					Daten würde z.B. die Pflicht genügen, geeignete Massnahmen zu ergreifen, um die Richtigkeit der Daten sicherzustellen. Teilweise entstehen aus den überschiessenden Pflichten auch unnötige Rechtsunsicherheiten und Abgrenzungsprobleme zu anderweitigen bestehenden gesetzlichen Regeln. Beispielsweise wird ein allgemeiner Löschungsanspruch statuiert, welcher im Einzelfall mit anderweitigen gesetzlichen Dokumentations- und Aufbewahrungspflichten kollidieren kann. Wir empfehlen, den bestehenden Art. 5 DSG als neue Formulierung von Art. 4 Abs. 5 VE-DSG zu übernehmen., wobei „vernichten“ durch „unzugänglich machen“ zu ersetzen wäre (vgl. oben zu Art. 3 lit. d VE-DSG) Anpassungsvorschlag: ~~Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten.~~ Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat angemessene Massnahmen zu treffen, damit die Daten berichtigt oder unzugänglich gemacht werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind, ausser es stehen gesetzliche oder aufsichtsrechtliche Aufbewahrungspflichten oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter entgegen. Jede betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden.
SBVg	DSG	4	6		Wie unter Abs. 3 wurde auch unter Abs. 6 eine unnötige Präzisierung eingefügt, indem die ausdrückliche Einwilligung nicht nur nach angemessener Information „freiwillig“, sondern neu zusätzlich „eindeutig“ sein soll. Diese Neuformulierung ist verunglückt, da sie entgegen der Absicht gemäss Erläuterungsbericht (S. 45 ff.) eine Verschärfung und damit verbundene Rechtsunsicherheit beinhaltet. Im Erläuterungsbericht (S. 47) wird zu Unrecht gefordert, dass die betroffene Person nicht gänzlich untätig bleiben darf, damit von einer „Einwilligung“ ausgegangen werden kann. Mit dieser Auslegung wird de facto eine Formvorschrift aufgestellt, welche das datenschutzrechtlich unproblematische und aus dem modernen Geschäftsleben nicht mehr wegzudenkende Abstellen auf Allgemeine Geschäftsbedingungen (AGB) im Massengeschäft und insbesondere beim elektronischen Auftritt künftig verunmöglichen würde. Richtigerweise ist auf den Zweck der Datenbearbeitung abzustellen (Art. 4 Abs. 3 DSG). Soweit dieser für die betroffene Person erkennbar ist, muss die Einwilligung formunabhängig erfolgen können. Wir erachten deshalb die bestehende Fassung von Art. 4 Abs. 5 DSG als klarer und in sich stimmiger

					formuliert. Demzufolge sollte diese Fassung auch in Art. 4 Abs. 6 VE-DSG übernommen werden. Anpassungsvorschlag: Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information ~~freiwillig und eindeutig~~ erfolgt. Die Einwilligung kann auch stillschweigend erteilt werden. Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen. Diese Einwilligung ist in standardisierter Form möglich.
SBVg	DSG	4	7 (neu)		In Anlehnung an Art. 13 Abs. 2 lit. c DSGVO sollte im VE-DSG geregelt werden, dass der Widerruf einer bereits erfolgten Einwilligung nicht die Rechtmässigkeit der aufgrund dieser Einwilligung bis zum Widerruf erfolgten Verarbeitung von Personendaten berührt wird. Anpassungsvorschlag: Der Widerruf einer Einwilligung berührt nicht die Rechtmässigkeit der aufgrund dieser Einwilligung bis zum Widerruf erfolgten Verarbeitung von Personendaten.
SBVg	DSG	5	1		Art. 5 Abs. 1 VE-DSG bringt zum Ausdruck, dass ein Auslandtransfer nicht grundsätzlich verboten, sondern grundsätzlich erlaubt ist. Nicht erlaubt ist ein Transfer von Personendaten in einen anderen Staat, wenn durch diesen der betroffenen Person schwerwiegende Persönlichkeitsverletzungen drohen. Angesichts von problematischen Entwicklungen in der Rechtsprechung bis hin zur Auffassung, dass Art. 5 Abs. 1 VE-DSG (heute Art. 6 Abs. 1 DSG) eine Verbotsnorm darstelle, wäre eine Klarstellung des Gesetzgebers dringend notwendig. Zumindest in der Botschaft sollte klargestellt werden, dass Art. 5 VE-DSG keine Verbotsnorm ist – dass also Auslandtransfers erlaubt sind, solange durch den Transfer nicht eine schwerwiegende Verletzung der Persönlichkeit der betroffenen Person droht. Dabei müssen die Interessen der betroffenen Person in Bezug auf den Schutz ihrer Persönlichkeit und die Interessen des Verantwortlichen am Auslandtransfer gegeneinander abgewogen werden.
SBVg	DSG	5	2		Um klarzustellen, dass sich der „angemessene Schutz“ nach der Liste des Bundesrates beurteilt, regen wir an, im Wortlaut von Abs. 2 einen Verweis auf den entsprechenden Art. 5 Abs. 7 aufzunehmen. Anpassungsvorschlag: Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat gemäss Artikel 5 Absatz 7 festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz

					gewährleistet.
SBVg	DSG	5	3		Da es sich um Alternativen handelt, schlagen wir vor, dies explizit so zu benennen. Anpassungsvorschlag: Liegt kein Entscheid des Bundesrates nach Abs. 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch (alternativ):
SBVg	DSG	5	3	b	Wir schlagen die Klarstellung vor, dass es sich bei diesen Garantien sowohl um spezifische als auch um standardisierte Garantien handeln kann. Um Arbeits- und Zeitaufwand sowohl auf Seiten eines Unternehmens als auch auf Seiten des Beauftragten in einem realistischem Mass in Grenzen zu halten, sollte das Verständnis sein, dass eine einmal vorgelegte vertragliche Garantie, gegenüber welcher seitens des Beauftragten keine Einwände erhoben wurden oder entsprechende Einwände durch den Verantwortlichen berücksichtigt wurden und die später für eine identische (oder vergleichbare) Kategorie von Personendaten und einen identischen (oder vergleichbaren) Zweck der Personendatenbearbeitungen verwendet werden soll, keiner weiteren vorgängigen Informationsverpflichtung unterliegt. Daher schlagen wir vor, in Art. 5 Abs. 3 lit. b. VE- DSG den Begriff „zweckgebunden“ einzufügen. Anpassungsvorschlag: spezifische oder standardisierte zweckgebundene Garantien, insbesondere durch Vertrag, über die der Beauftragte durch den Verantwortlichen vorgängig informiert wurde;
SBVg	DSG	5	3	c	Vgl. obige Ausführungen zu Art. 5 Abs. 3 lit. b VE-DSG. Anpassungsvorschlag: standardisierte zweckgebundene Garantien, insbesondere durch Vertrag, ~~1. welche der Beauftragte vorgängig genehmigt hat, oder~~ ~~2.~~ -welche der Beauftragte ausgestellt oder anerkannt und veröffentlicht hat;
SBVg	DSG	5	3	d	Die Pflicht, verbindliche unternehmensinterne Datenschutzvorschriften durch den Beauftragten vorgängig genehmigen zu lassen, erscheint uns nicht sachgerecht, da diese bereits durch die externen Revisionsstellen der Unternehmen zu prüfen sind. Daher beantragen wir die ersatzlose Streichung des Art. 5 Abs. 3 lit. d VE-DSG.

SBVg	DSG	5	4		Wir schlagen vor, dass der Beauftragte innerhalb von 30 Tagen, entsprechend dem Änderungsvorschlag in Art. 5 Abs. 4 VE-DSG, dem Verantwortlichen etwaige konkrete Einwände mitteilen muss. Bei Ausbleiben der Mitteilung von Einwänden müssen die Garantien als genehmigt gelten. Die Forderung, dass sich der Beauftragte sowohl hinsichtlich spezifischen als auch in Bezug auf standardisierte vertragliche Garantien verbindlich äussern muss, erfolgt aufgrund von Überlegungen zur Rechts- und Planungssicherheit. Gemäss dem vorliegende Wortlaut ist nicht auszuschliessen, dass seitens des Beauftragten verstanden werden kann, dass dieser einen Verantwortlichen über etwaige Einwände innerhalb von 30 Tagen lediglich informieren muss, mit konkreten Äusserungen und Anforderungen jedoch auch noch zu einem späteren Zeitpunkt auf den Verantwortlichen zukommen kann. Dieses Risiko ist einem Unternehmen nicht zuzumuten. Allenfalls könnte die Frist zur Äusserung von 30 Tagen auf zwei Monate erhöht werden. Anpassungsvorschlag: Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 lit. b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien seine Einwände mitteilen ~~informieren~~.
SBVg	DSG	5	5		Infolge der Anpassungsvorschläge von Art. 5 Abs. 3 und Abs. 4 VE-DSG ist Abs. 5 ersatzlos zu streichen.
SBVg	DSG	5	6		Die pauschale Informationspflicht bei Verwendung von Standardklauseln bedeutet eine hohe administrative Belastung für sämtliche Unternehmen und bietet weder der betroffenen Person noch dem Beauftragten einen Mehrwert. Letzterer wird mit Informationen überhäuft werden und nicht in der Lage sein, diese zu bearbeiten. Dementsprechend ist diese Pflicht dem EU-Recht fremd und stellt ein Swiss Finish dar. Sie ist ersatzlos zu streichen.
SBVg	DSG	6	1	a	Der Terminus „Einzelfall“ impliziert eine allzu strenge Einschränkung und führt in der Praxis zu Unklarheiten in der Anwendung. Nach allgemeinen Grundregeln genügt es, wenn die betroffene Person mit Bezug auf bestimmte wiederkehrende Sachverhalte generell gültig zustimmen kann, mithin nicht nur für einen aktuellen Einzelfall, sondern auch mit Wirkung für analoge künftige Fälle. Wir empfehlen deshalb die Streichung dieses Begriffs. Anpassungsvorschlag:

					die betroffene Person ~~im Einzelfall~~ eingewilligt hat;
SBVg	DSG	6	1	b	Art. 6 Abs. 1 lit. b VE-DSG sollte aus Gründen der Rechtssicherheit und Äquivalenz mit der Regelung der DSGVO in Übereinstimmung gebracht werden. Eine Bekanntgabe im Sinne eines Ausnahmefalls muss auch dann zulässig sein, wenn die betroffene Person nicht Vertragspartei ist, aber der fragliche Vertrag in ihrem Interesse oder zu ihren Gunsten abgeschlossen wurde. Bei internationalen Transaktionen des Handels und der Verwahrung von Wertschriften tritt die Bank nach bewährter Usanz in eigenem Namen und bloss im Interesse der betroffenen Kunden auf. Andere Lösungen wären in Massengeschäften dieser Art gegenüber ausländischen Vertragspartnern der Bank nicht durchsetzbar. Solche bewährte Strukturen liegen somit im klaren Interesse der betroffenen Kunden. Anpassungsvorschlag: die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt oder einer Person, zu deren Gunsten oder in deren Interesse der Vertrag abgeschlossen wird;
SBVg	DSG	6	1	c	Im Rahmen von gerichtlichen oder verwaltungsrechtlichen Verfahren werden in der Regel Informationsverbote verfügt, die eine Meldung an den Beauftragten nicht zulassen würden. Eine gleichwohl zu erfolgende Meldung würde für den Verantwortlichen eine Verletzung des Ermittlungsgeheimnisses darstellen, was nicht Sinn des VE-DSG sein kann. Insofern schlagen wir vor, den Text des Art. 6 Abs. 2 lit. c Ziff. 1 und 2 in zwei separate Buchstaben (c und c^{bis}) aufzuteilen und den in Art. 6 Abs. 2 VE-DSG vorhandenen Verweis auf Art. 6 Abs. 1 lit. c VE-DSG zu beschränken. Anpassungsvorschlag: ~~die Bekanntgabe im Einzelfall unerlässlich ist für:~~ ~~1. die Wahrung eines überwiegenden öffentlichen Interesses, oder~~ ~~2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde;~~ c. die Bekanntgabe im Einzelfall unerlässlich ist für die Wahrung eines überwiegenden öffentlichen Interesses;

SBVg	DSG	6	1	c^{bis} (neu)	Vgl. obige Ausführungen zu Art. 6 Abs. 1 lit. c VE-DSG. Anpassungsvorschlag: die Bekanntgabe im Einzelfall unerlässlich ist für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen;
SBVg	DSG	6	1	d	Vgl. obige Ausführungen zu Art. 6. Abs. 1 lit. a VE-DSG. Anpassungsvorschlag: die Bekanntgabe ~~im Einzelfall~~ notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen;
SBVg	DSG	6	2		Sollte es sich bei den Vertragspartnern um natürliche Personen handeln, ist davon auszugehen, dass diese vom Inhalt des Vertrags Kenntnis und in die Bekanntgaben der Personen gemäss den Bestimmungen des Art. 6 Abs. 1 lit. a VE-DSG eingewilligt haben. Insofern schlagen wir vor, den in Art. 6 Abs. 2 VE-DSG vorhandenen Verweis auf Art. 6 Abs. 1 lit. b VE-DSG zu streichen. Anpassungsvorschlag: Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben ~~b,~~ c und d bekannt gibt.
SBVg	DSG	7	2		Art. 7 Abs. 2 VE-DSG führt Pflichten auf, welche gemäss Gesamtgefüge des VE-DSG ohnehin bereits bestehen. Diese Regelung ist demzufolge ebenso wenig notwendig wie zusätzliche Präzisierungen in der Verordnung. Letztere könnten sogar kontraproduktiv sein, da jedes Projekt eigene spezifische Datenschutzthemen generiert. Ein allgemeiner starrer Anforderungskatalog kann diesen projekt-spezifischen Herausforderungen nicht gerecht werden. Vielmehr würde der Katalog Herausforderungen bestimmter Projekte gar nicht aufführen oder umgekehrt die Verantwortlichen zwingen, bestimmte Themen generell in jedem Projekt detailliert zu klären, obwohl solche Themen je nach Projekt gar keine Rolle spielen. Allgemeine Präzisierungen würden somit einerseits per definitionem unvollständig bleiben und andererseits zu unnötigem Zusatzaufwand führen. Solche Detailregulierungen wiedersprechen sodann auch dem bewährten prinzipienbasierten Ansatz des DSG, an welchem der VE-DSG erklärtermassen festhalten will. Abs. 2 von Art. 7 VE-DSG ist demzufolge ersatzlos zu streichen.

SBVg	DSG	7	3		In der heutigen arbeitsteiligen Welt ist das Verlangen nach einer „vorgängigen schriftlichen Zustimmung“ kaum umsetzbar und würde zu einem Verbot der Unterakkordanz führen. Dies kann nicht im Sinne des Gesetzgebers sein. Wir empfehlen deshalb die Streichung der vorgängigen schriftlichen Zustimmung. Im Erläuterungsbericht sollte klar festgehalten werden, dass eine generelle Einwilligung zum Beizug von Sub-Auftragsdatenbearbeitern ausreicht, sofern der Verantwortliche im konkreten Fall (d.h. wenn ein konkreter Sub-Auftragsdatenbearbeiter beigezogen wird) informiert wird und ein Vetorecht ausüben kann. Anpassungsvorschlag: Der Auftragsbearbeiter darf die Bearbeitung nur mit ~~vorgängiger schriftlicher~~ Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. Die Bewilligung kann in genereller Art erteilt werden. Sie ist zu dokumentieren.
SBVg	DSG	8	1		Der Beauftragte sollte lediglich die Kompetenz erhalten, vorgelegte Richtlinien zu genehmigen. Dies würde weitgehend einer Selbstregulierung entsprechen und den Vorteil haben, dass die Richtlinien von Betroffenen verfasst werden, die mit der nötigen Expertise die möglichen Besonderheiten einer Branche am sachgerechtesten erfassen können. Damit würde der Beauftragte einerseits entlastet und anderseits verhilft dieser Mechanismus zu sachgerechten Lösungen. Über das Genehmigungserfordernis hätte letztlich aber immer noch der Beauftragte das letzte Wort. Anpassungsvorschlag: Der Beauftragte genehmigt ihm vorgelegte Empfehlungen der guten Praxis, welche ~~die~~ Datenschutzvorschriften konkretisieren~~. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen.~~
SBVg	DSG	9	1		Art. 9 Abs. 1 VE-DSG ist dahingehend zu ergänzen, dass auch der Auftragsdatenbearbeiter Datenschutzvorschriften einhält, welche auf dem Wege von Empfehlungen der guten Praxis konkretisiert werden. Anpassungsvorschlag: Befolgen ~~t~~ der Verantwortliche und Auftragsdatenbearbeiter die Empfehlungen der guten Praxis, ~~hält~~ halten sie ~~er~~ diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren.

SBVg	DSG	12			Die Regelung von Art. 12 VE-DSG ist schwer verständlich und erscheint im VE-DSG als Fremdkörper. • Soweit es sich bei Personendaten auch um Geschäftsdaten handelt, was die Regel ist, bestehen gemäss diversen anderen einschlägigen Gesetzen weitreichende legitime Dokumentations- und Archivierungspflichten, welche dem Kerngehalt von Art. 12 VE-DSG zuwiderlaufen. • Effektiv gehen beim Tod einer Person dessen Rechte qua erbrechtlicher Universalsukzession ohne weiteres auf die Erben über (Art. 560 Abs. 1 ZGB). Gestützt auf diesen erbrechtlichen Übergang sämtlicher Rechte von Gesetzes wegen sind die Erben bereits ausreichend legitimiert, geeignete Massnahmen vorzukehren. Umgekehrt können die Erben per definitionem auch nicht mehr Rechte haben, als der Erblasser sie hatte. In diesem Zusammenhang ist auch eine unklare Abgrenzung von Art. 12 VE-DSG zu der im Rahmen der pendenten Erbrechtsreform geplanten Regelung des Auskunftsrechts von Erben nach neuem Art. 601a ZGB zu bemängeln. Schliesslich ist Art. 12 VE-DSG sogar kontraproduktiv, weil er eine Regelung aufstellt, welche zumindest nicht deckungsgleich mit etabliertem Erbrecht ist. • Gleiches gilt für Regelungen von Amts- und Berufsgeheimnissen in bereits bestehenden gesetzlichen Bestimmungen (für Banken z.B. Art. 47 BankG). Die pauschale Regelung, dass unter Art. 12 Abs. 3 VE-DSG Amts- und Berufsgeheimnisse generell nicht geltend gemacht werden können, kann so jedenfalls nicht stimmen. Aufgrund dieser Argumente fordern wir die ersatzlose Streichung von Art. 12 VE-DSG.
SBVg	DSG	13	1		Sinnvollerweise wird die Informationspflicht ausdrücklich auf besonders schützenswerte Daten und überdies auf Datenbearbeitungen ausserhalb des (objektivierten) Erkennbarkeitshorizonts i.S.v. Art. 4 DSG der betroffenen Person eingeschränkt. Dies folgt aus dem naheliegenden Grundsatz, dass alle anderen Daten entsprechend den Grundsätzen von Art. 4 VE-DSG für die betroffene Person erkennbar sind und demzufolge keiner (zusätzlichen) Information bedürfen. Klarzustellen ist, dass die Information sich jedenfalls auf den Zeitpunkt der Datenbeschaffung bezieht und sich auch die Richtigkeit und Vollständigkeit der Daten an diesem Zeitpunkt misst. Für spätere Änderungen kann keine Informationspflicht bestehen. Anpassungsvorschlag: Der Verantwortliche informiert die betroffene Person zum Zeitpunkt der Datenbeschaffung über die Beschaffung von besonders schützenswerten Personendaten; diese Informationspflicht gilt auch, wenn

					die Daten bei Dritten beschafft werden.
SBVg	DSG	13	2	a	Wir schlagen vor, den Begriff „Identität“ des Verantwortlichen durch „Name“ des Verantwortlichen zu ersetzen. Die einfache Namensnennung ist auch in der DSGVO vorgesehen. Das Schweizer Datenschutzgesetz sollte diesbezüglich keine höheren Anforderungen stellen. Anpassungsvorschlag: ~~die Identität~~ den Namen und die Kontaktdaten des Verantwortlichen;
SBVg	DSG	13	2	b	Es sollte keine Verpflichtung bestehen, sämtliche bearbeiteten Personendaten oder die entsprechenden Kategorien abschliessend in der Information aufführen zu müssen, so wie es gemäss dem vorliegenden Wortlaut des VE-DSG den Anschein erweckt. Wir schlagen daher vor, die Formulierung durch den Zusatz „voraussichtlich“ weniger absolut zu gestalten. Anpassungsvorschlag: die voraussichtlich bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten;
SBVg	DSG	13	2	d (neu)	Die in Absatz 3 normierte Pflicht fällt in den Anwendungsbereich von Absatz 2 und sollte deshalb auch dort integriert werden. Zudem hat Art. 13 VE-DSG aus Klarheitsgründen konsequent dieselbe Terminologie zu verwenden. Es muss z.B. konsequent von „Dritten“ gesprochen werden und nicht von „Empfängern“. Anpassungsvorschlag: gegebenenfalls die Dritten oder die Kategorien der Dritten, denen Personendaten bekanntgegeben werden.
SBVg	DSG	13	3		Aufgrund der Einfügung von Art. 13 Abs. 2 lit. d (neu) VE-DSG ist Art. 13 Abs. 3 ersatzlos zu streichen.
SBVg	DSG	13	4		Die Vorschrift geht über die entsprechenden Bestimmungen der DSGVO hinaus und ist als Swiss Finish abzulehnen. Des Weiteren würde sie zu einem erheblich Mehraufwand führen. Wir beantragen deshalb die ersatzlose Streichung des Absatzes.
SBVg	DSG	13	5		Die Regel fordert maximale Transparenz zum Preis eines unverhältnismässig hohen Aufwandes. Bei der Datenbeschaffung durch Dritte sind die relevanten Eckpfeiler wie insbesondere „erstmalige Speicherung“ dem Verantwortlichen regelmässig gar nicht bekannt. Der dafür eingesetzte Dritte kennt diese Modalitäten naturgemäss viel besser. Wird der Verantwortliche direkt verpflichtet, müsste er deshalb aus

					Gründen seiner Sorgfaltspflicht immer zuerst den Dritten anfragen, bevor er gestützt auf dessen Angaben die betroffenen Personen informieren könnte. Dieser Absatz ist deshalb ersatzlos zu streichen. Eventualantrag: Sollte wider Erwarten auf die ersatzlose Streichung von Art. 13 Abs. 5 VE-DSG verzichtet werden, schlagen wir eine Anpassung des Wortlauts an die entsprechende Bestimmung der DSGVO vor. Anpassungsvorschlag: Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person innerhalb von drei Monaten nach der Datenbeschaffung ~~spätestens bei der Speicherung der Daten~~ informiert werden; werden die Daten beschafft, um mit der betroffenen Person zu kommunizieren, so muss die betroffene Person darüber bei dem ersten Kontakt informiert werden. ~~werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.~~
SBVg	DSG	14	2	a	Wir empfehlen, den Terminus „Speicherung" mit dem Begriff „Beschaffung" zu ersetzen. Überdies sollte das Erfordernis der ausdrücklichen Erwähnung im Gesetz durch „rechtliche Pflichten" ersetzt werden. Banken stehen in der Pflicht, Hintergrundinformationen zu Kunden zu sammeln (diese Pflichten werden von der FINMA in ihren Erlassen konkretisiert, sind aber nicht explizit in einem Gesetz festgehalten). Ausserdem entfällt die Informationspflicht gemäss DSGVO, wenn die Daten dem Berufsgeheimnis unterliegen. Anpassungsvorschlag: ~~die Speicherung,~~ die Beschaffung oder die Bekanntgabe der Personendaten ~~Daten ausdrücklich im Gesetz vorgesehen ist~~ auf gesetzlichen oder aufsichtsrechtlichen Pflichten beruht; oder
SBVg	DSG	14	2	c (neu)	Die DSGVO sieht keine Informationspflicht vor, wenn die Daten einem Berufsgeheimnis unterliegen. Wir empfehlen deshalb, eine zusätzliche Bestimmung aufzunehmen, damit das Schweizer Amts- und Berufsgeheimnis gewahrt ist. So werden beispielsweise Banken von der FINMA angehalten, Hintergrundinformationen zu Vertragspartner, Kontrollinhaber und wirtschaftlich Berechtigten zu sammeln. Diese Information dürfen jedoch nur eingeschränkt an die betroffenen Personen weitergeleitet werden. Anpassungsvorschlag: die Daten dem [Amts- oder] Berufsgeheimnis unterliegen.

SBVg	DSG	14	3		Diese Bestimmung ist unklar formuliert und sollte deshalb präzisiert werden. Anpassungsvorschlag: Der Verantwortliche kann die ~~Übermittlung der~~ Information~~en~~ einschränken, aufschieben oder darauf verzichten, wenn:
SBVg	DSG	14	3	c (neu)	Wir empfehlen, eine zusätzliche Bestimmung aufzunehmen, welche einen Informationsverzicht durch den Verantwortlichen vorsieht, wenn die Personendaten durch die betroffene Person veröffentlicht wurden oder diese frei zugänglich sind. Anpassungsvorschlag: die Personendaten von der betroffenen Person veröffentlicht wurden oder diese allgemein zugänglich sind.
SBVg	DSG	14	4	a	Die Bestimmung geht unnötigerweise über die Regelung der europäischen DSGVO hinaus. Sollten die Interessen der betroffenen Personen durch die Bekanntgabe an einen Dritten tatsächlich beeinträchtigt sein, so ist dies bereits im Rahmen der allgemeinen Interessenabwägung im Sinne von Art. 24 VE-DSG berücksichtigt. Wir empfehlen deshalb die Streichung des letzten Teilsatzes. Unternehmen haben ein legitimes Interesse, die Vorbereitung von Zivilprozessen, in denen das Unternehmen Kläger oder Beklagter ist, geheim zu halten und dabei auch Personendaten ihrer Mitarbeiter, Berater oder Kunden zu bearbeiten. Eine vorgängige Information der betroffenen Personen würde den eigentlichen Zweck der Bearbeitung vereiteln. Entsprechendes gilt für interne Untersuchungen und Whistleblowing-Verfahren: Damit der Zweck einer internen Untersuchung bzw. eines Whistleblowing-Verfahrens nicht vereitelt wird, können die betroffenen Mitarbeiter nicht vorgängig über die Datenbearbeitung informiert werden. Nicht zuletzt können Unternehmen auch ihren Mitwirkungspflichten im Rahmen von inländischen oder ausländischen Verwaltungs- oder Strafverfahren (einschliesslich Kartellverfahren) nicht, nicht richtig oder nicht rechtzeitig nachkommen, wenn alle betroffenen Personen vorgängig über eine Datenbearbeitung (z.B. Erhebung und Lieferung von Beweisen, die Personendaten enthalten) informiert werden müssten. Eine solche Information wäre den Unternehmen aufgrund bestehender Geheimhaltungs- oder Kooperationspflichten in den entsprechenden Verfahren gar nicht erlaubt. Sie würde den Zweck der behördlichen Untersuchung in Frage stellen und es dem Unternehmen in vielen Fällen sogar

					verunmöglichen, Rechte durzusetzen, Klagen abzuwehren oder sich in Strafverfahren adäquat zu verteidigen. Zum Beispiel ist es gemäss dem sog. Yates Memorandum absolut notwendig, dass Unternehmen bereits zu Beginn einer Untersuchung die Namen sämtlicher für den Verstoss verantwortlicher Mitarbeiter im Unternehmen nennt. Das Yates Memorandum bzw. die entsprechend dem Memorandum revidierten Grundsätze des U.S. Department of Justice sind Anweisungen an die Staatsanwälte, dass parallel zu Ermittlungen gegen ein Unternehmen von Anfang an auch gegen verantwortliche Mitarbeiter innerhalb des Unternehmens ermittelt werden soll. Zudem ist darin festgelegt, dass Unternehmen nur dann mit einer einvernehmlichen Regelung einschliesslich Kooperationskredit rechnen dürfen, wenn sie von Anfang an alle relevanten Tatsachen zu mutmasslich am Fehlverhalten beteiligten oder dafür verantwortlichen Mitarbeiter offen legen – einschliesslich der Namen der Mitarbeiter (Alles-oder-Nichts-Prinzip). Entsprechend ist Art. 14 Abs. 4 lit. a VE-DSG wie oben vorgeschlagen anzupassen. Die in Art. 14 Abs. 4 lit. a Ziff. 2 (neu) VE-DSG zusätzlich eingefügte Ausnahmen müsste konsequenterweise auch als möglicher Grund für die Einschränkung des Auskunftsrechts (so der Verweis in Art. 21 Abs. 1 VE-DSG) und als Rechtfertigungsgrund für Verletzungen von Bearbeitungsgrundsätzen (vgl. Kommentar zu Art. 24 VE-DSG) gelten. Anpassungsvorschlag: 1. wenn es sich beim Verantwortlichen um eine private Person handelt, oder falls überwiegende Interessen des Verantwortlichen dies erfordern ~~und er die Personendaten nicht Dritten bekannt gibt~~; 2. falls die Übermittlung der Information den Zweck der Bearbeitung, insbesondere die Feststellung, Ausübung, Durchsetzung oder Verteidigung von Rechtsansprüchen, in Frage stellen würde.
SBVg	DSG	14	5		Art. 14 Abs. 5 VE-DSG ist ersatzlos zu streichen. Diese Pflicht hat faktisch zur Folge, dass Unternehmen permanent überprüfen müssen, ob eine Information nachzuholen ist. Das ist in grossen, komplexen Organisationen nicht zu bewerkstelligen. Es ist der betroffenen Person zumutbar, dass sie ein Informationsgesuch gegebenenfalls wiederholt.
SBVg	DSG	15	1		Es fehlt an den Rechtfertigungsgründen des Abschlusses oder der Erfüllung eines Vertrags bzw. der ausdrücklichen Einwilligung (vgl. Art. 22 Abs. 2 lit. a und c DSGVO). Die Informationspflicht in Abs. 1 ist zu konkretisieren, insbesondere der Zeitpunkt der Mitteilung, der Inhalt und Umfang der Informationen (z.B. Geldbezug via Bankautomat) sowie die Begriffe „rechtliche Wirkung“ und „erhebliche

					Auswirkungen“.
SBVg	DSG	15	2		Das neu vorgeschlagene Recht einer betroffenen Person, sich zu einer automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern („Anhörungspflicht“), stufen wir als wettbewerbs- und auch innovationsbehindernd ein. Darüber hinaus ist dieses Recht aber auch schlicht unnötig, insbesondere angesichts der ebenfalls neu eingeführten Pflicht, die betroffene Person darüber zu informieren, wenn eine automatisierte Einzelentscheidung gefällt wurde (Abs. 1). Unabhängig davon quasi „auf Vorrat“ zu informieren, produziert demnach keine zusätzliche Transparenz, sondern generiert lediglich unnötigen zusätzlichen Administrativaufwand. Weder ERK 108 noch DSGVO sehen ein entsprechendes Äusserungsrecht vor. Die Regelung ist demzufolge ein kontraproduktiver Swiss Finish, den es zur Erreichung von Äquivalenz zu verhindern gilt. Zudem gehört die Information darüber, wie bestimmte Entscheide zustande kommen, zum Geschäftsgeheimnis eines Unternehmens, und ist demnach klar unverhältnismässig. So ist zum Beispiel im Finanzbereich die Einschätzung von Ausfallrisiken bei der Kreditvergabe ein wichtiges, differenzierendes Know-How eines Finanzdienstleisters. Die Auskunft über die für diese Einschätzung genutzten Daten und deren Gewichtung führt zu einer Replizierbarkeit dieser Einschätzung und damit zur Aufgabe dieses Geschäftsgeheimnisses. Offenlegungspflichten solcher Art würden im Ergebnis jede Innovationskraft der Wirtschaft abtöten, da der dafür eingesetzte Aufwand nicht angemessen geschützt werden könnte. Aufgrund all dieser Argumente fordern wir die ersatzlose Streichung des Äusserungsrechts nach Art. 15 Abs. 2 VE-DSG.
SBVg	DSG	15	3		Ferner sollte die Informationspflicht betreffend eine automatisierte Einzelentscheidungen entfallen, wenn eine solche gestützt auf eine Vereinbarung, die zwischen der betroffenen Person und dem Verantwortlichen abgeschlossen wurde, getroffen wurde. Dies kann z.B. bei einem Vertrag betreffend die automatisierte Verwaltung des Vermögens der betroffenen Person gegeben sein (z.B. RoboAdvice – hier möchte der Kunde gerade eine ausschliesslich automatisierte Einzelentscheidung). In diesem Fall sind der betroffenen Person die zugrundeliegenden Parameter bekannt bzw. sie hat diese mit dem Verantwortlichen vereinbart. Die Schlechterstellung einer automatisierten Einzelentscheidung im privaten Bereich aufgrund einer vertraglichen Vereinbarung gegenüber einer gesetzlich vorgesehenen automatischen Einzelentscheidung ist nicht gerechtfertigt.

					Anpassungsvorschlag: Die Informations- ~~und Anhörungspflicht~~ gilt nicht, wenn ein Gesetz oder ein Vertrag zwischen Verantwortlichem und betroffener Person eine automatisierte Einzelentscheidung vorsieht.
SBVg	DSG	16			Die Regelung der Datenschutz-Folgenabschätzung (DSFA) im VE-DSG erachten wir grundsätzlich als überflüssig. Die Forderung gemäss Art. 8bis der revidierten ERK 108, bei geplanten Datenbearbeitungen die Risiken einzuschätzen, wird durch Art. 11 VE-DSG (Datensicherheit) bereits vollumfänglich erfüllt. Überdies bestehen bereits zahlreiche Spezialregeln, die bestimmte Datenflüsse einer Überwachung unterstellen. Im Bankenbereich wird z.B. gemäss Art. 42c FINMAG die Informationsübermittlung an ausländische Finanzmarktaufsichtsbehörden und weiteren mit der Aufsicht betraute ausländischen Stellen durch die FINMA überwacht (vgl. auch neues FINMA-RS 2017/6 „Direktübermittlung"). „Doppelte" Überwachungen sind aus Effizienzgründen und zur Vermeidung von Widersprüchen zu vermeiden. Wie dieses Beispiel zeigt würde eine zusätzliche Überwachung durch den Beauftragten dem Zweck der Regelung von Art. 42c FINMAG und des einschlägigen FINMA-RS 2017/6 offensichtlich zuwiderlaufen, da beide bereits bestehende Regelungen klare und rechtssichere Regeln für eine rasche Lösung der Thematik – unter Anwendung von kurzen Fristen – zur Verfügung stellen. Wir erachten die Regelung des Art. 16 VE-DSG im vorliegenden Kontext deshalb für verzichtbar, zumal die DSFA stark interpretationsbedürftig bleibt und zu einem grossen, nicht absehbaren Aufwand führt, ohne dass ein Datenschutzmissbrauch letztlich verhindert werden könnte. Wir fordern daher die Streichung des Art. 16 VE-DSG. Sollte wider Erwarten an einer gesetzlichen Regelung der DSFA festgehalten werden, sind nachfolgende Punkte zwingend zu berücksichtigen.
SBVg	DSG	16	1		Die Schwelle zur Durchführung einer DSFA wurde zu tief angesetzt und mit vagen Kriterien umschrieben. Ein „voraussichtlich erhöhtes Risiko" wird es bei jeder Datenbearbeitung geben; insbesondere bei einem grösseren Unternehmen, die Personendaten grenzübergreifend bearbeitet. Zudem ist unklar, gegenüber was das Risiko „erhöht" sein muss. Aus dem Erläuterungsbericht geht sinngemäss hervor, dass jede Übermittlung von Personendaten in die USA, jedes Profiling sowie jede Bearbeitung besonders schützenswerter Personendaten eine DSFA verlangen würde. Der Natur der Sache nach muss sich die Regelung auf hohe Risiken beschränken, was im Übrigen auch den Anforderungen von Art. 36 Abs. 1 DSGVO entspricht. Im aktuellen Entwurf würde die Regel ohne

					Notwendigkeit enormen Aufwand verursachen, welcher überdies einen für die Äquivalenz mit der DSGVO unnötigen Swiss Finish darstellen würde. Im Interesse der Rechtssicherheit müssen Datenbearbeitungen mit hohem Risiko auf Verordnungsstufe durch eine Aufzählung der Fälle abschliessend definiert werden. Schliesslich muss klar festgehalten werden, dass eine Wiederholung (Update) einer DSFA nicht nötig ist, sofern und soweit sich die Logik der fraglichen Datenbearbeitung im Wesentlichen nicht ändert. Ferner muss eine DSFA ausbleiben können, wenn ein Rechtfertigungsgrund gegeben ist oder die betroffenen Personen in die fragliche Datenbearbeitung rechtsgültig eingewilligt haben. Sobald eine Einwilligung vorliegt, besteht keine Notwendigkeit einer DSFA, da die Rechte der betroffenen Person auf diese Weise bereits berücksichtigt sind. Angesichts der Tatsache, dass nur der Verantwortliche über Zweck, Mittel sowie Umfang der Datenbearbeitung entscheidet, ist es nicht sachgerecht, dass auch der Auftragsdatenbearbeiter der Pflicht zur Durchführung einer DSFA unterliegt. Letzterer wird regelmässig nicht über die für eine DSFA notwendigen Angaben verfügen. Anpassungsvorschlag: Führt die vorgesehene Datenbearbeitung ~~voraussichtlich~~ zu einem hohen ~~erhöhten~~ Risiko für die Persönlichkeit oder ~~die Grundrechte~~ der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen.
SBVg	DSG	16	1bis (neu)		Um die Einschätzung und Entscheidung eines Verantwortlichen bezüglich die Frage, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, zu erleichtern, sollte der Bundesrat in Anlehnung an die DSGVO verpflichtet sein, Fallkonstellationen zu definieren, für welche eine Datenschutz-Folgenabschätzung durchzuführen ist. Wir schlagen deshalb einen neuen Absatz 1bis vor. Anpassungsvorschlag: Der Bundesrat definiert Fälle mit hohem Risiko.
SBVg	DSG	16	2		Vgl. Ausführungen zu Art. 16 Abs. 1 VE-DSG. Anpassungsvorschlag: Die Datenschutz-Folgeabschätzung umschreibt die geplante Bearbeitung, die Bewertung von Risiken für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person sowie die Massnahmen, die vorgesehen

					sind, um das Risiko einer Verletzung der Persönlichkeit ~~oder der Grundrechte~~ der betroffenen Person zu verringern.
SBVg	DSG	16	3		Die vorgesehene Meldepflicht an den Beauftragten geht viel zu weit. Jede DSFA melden zu müssen, stellt einen massiven Eingriff in die Geheimsphäre der Unternehmen dar. Diesen würde dadurch ein Anreiz gesetzt, im Zweifel keine DSFA durchzuführen. Zudem besteht die Gefahr, dass der Beauftragte aufgrund der grossen Anzahl von Meldungen nicht in der Lage sein wird, den ihm obliegenden gesetzlichen Verpflichtungen nachzukommen. Wir empfehlen, die Meldepflicht auf hohe Risiken zu beschränken, wobei die Erheblichkeit – entsprechend den Bestimmungen der DSGVO – aufgrund des gemäss der DSFA enthaltenen Endresultats zu beurteilen ist. Eine Meldepflicht sollte auf diejenigen Fälle beschränkt sein, die selbst nach Implementierung von geeigneten Massnahmen weiterhin hohe Risiken beinhalten. Anpassungsvorschlag: Der Verantwortliche ~~oder der Auftragsbearbeiter~~ benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen, wenn trotz der Massnahmen ein hohes Risiko für die Persönlichkeit der betroffenen Person besteht.
SBVg	DSG	16	4		Art. 16 Abs. 4 VE-DSG sieht vor, dass der Beauftragte seine Einwände innert drei Monaten geltend machen kann. Während dieser Zeit steht die fragliche Datenbearbeitung still. Zusätzlich kann der Beauftragte diese Frist selber um jeweils weitere drei Monate verlängern, immer wenn er weitere Angaben für „erforderlich“ hält. Die DSGVO ist in dieser Hinsicht viel praxisnäher: sie sieht eine acht-wöchige Frist vor; diese kann nur in besonderen Ausnahmefällen um sechs Wochen verlängert werden (vgl. Art. 36 Abs. 2 DSGVO). Wir empfehlen, die Lösung der DSGVO entsprechend zu übernehmen. Für eine abweichende Regel gibt es keine Veranlassung. Zudem ist zu präzisieren, wie die Mitteilung allfälliger Einwände durch den Beauftragten zu erfolgen hat. Anpassungsvorschlag: Hat der Beauftragte Einwände gegen die vorgesehene Massnahme, so teilt er dies dem Verantwortlichen ~~oder dem Auftragsbearbeiter~~ innerhalb von zwei Monaten nach Erhalt der Benachrichtigung ~~aller erforderlichen Informationen~~ mit. Der Beauftragte hat dem Verantwortlichen schriftlich mitzuteilen, welche Massnahmen zu ergreifen sind.

SBVg	DSG	17			Diese Pflicht wird ohne gezielte Eingrenzung in qualitativer und quantitativer Weise uferlos. Entsprechend würden die Verantwortlichen, um dem Vorwurf einer strafbaren Handlung zu entgehen (vgl. Art. 50 Abs. 2 lit. e), jeden noch so geringfügigen Verstoss melden. Der Beauftragte wäre ausser Stande, innerhalb dieser Papierflut allfällige wirklich wichtige Meldungen zeitgerecht zu erkennen und geeignete Massnahmen einzuleiten. In solchen Fällen sähe er sich selbst mit dem Vorwurf konfrontiert, trotz erhaltener Meldung nicht gehandelt zu haben. Die Regelung krankt überdies am Ansatz, dass sich der Verantwortliche mit Erfüllung der Meldepflicht de facto gleich selbst anzeigen muss. Damit wird das strafrechtliche Grundprinzip „nemo tenetur“ verletzt. Befolgt er die Meldepflicht nicht, wird er gleichwohl durch Nichteinhaltung derselben strafbar (Art. 50 Abs. 2 lit. e). Umso schlimmer ist diese Regelung, wenn man davon ausgeht, dass seriöse Datenbearbeiter der Meldepflicht wohl nachkommen werden und gestützt darauf „als Dank“ für ihre Versäumnisse sanktioniert werden. Demgegenüber werden die wirklich „schwarzen Schafe“ die Meldepflicht nicht ausüben und - in vielen Fällen zu Recht - darauf vertrauen, dass der Skandal nicht erkannt wird.
SBVg	DSG	17	1		In Art. 17 Abs. 1 VE-DSG sollte, wie im erläuternden Bericht bereits präzisiert, explizit erwähnt werden, dass die unverzügliche Meldung einer unbefugten Datenbearbeitung erst nach Kenntnisnahme durch den Verantwortlichen zu erfolgen hat. Um den administrativen Aufwand sowohl für den Verantwortlichen als auch den Beauftragten möglichst gering zu halten, empfehlen wir zudem, die in Art. 17 Abs. 1 normierte Meldepflicht analog zur DSGVO auf diejenigen Verletzungen des Datenschutzes einzuschränken, die ein hohes Risiko für die Persönlichkeit der betroffenen Person in sich bergen. Schliesslich führt Art. 17 VE-DSG zu einer Unternehmenskultur mit totaler Überwachung: ein für den Datenschutz verantwortlicher Mitarbeiter wäre unter Strafdrohung verpflichtet, seine für einen Datenschutzverstoss verantwortlichen Kollegen beim Beauftragten zu melden. Aufgrund der Anzeigepflicht des Beauftragten würden die fehlbaren Mitarbeiter durch einen ordentlichen Strafrichter verurteilt. Im Übrigen steht dieser Mechanismus im krassen Widerspruch zu rechtsstaatlichen Grundsätzen wie z.B. dem nemo tenetur-Prinzip. Gemäss Wortlaut von VE-DSG muss die Meldung "unverzüglich" erfolgen. Obschon hier nicht klar ist, ob sich der Gesetzgeber eine, gemessen an den 72 Stunden in der DSGVO, längere oder kürzere Frist vorstellt oder ob sich diese an irgendwelchen äusseren Umständen bemisst, suggeriert eine

					"unverzügliche" Meldung, dass das betroffene Unternehmen in der Praxis die Meldung übereilt absetzten muss, ohne dass der betroffenen Abteilung die Zeit bleibt, den eigentlichen Fehler, der zu einer Verletzung geführt hat, vorab ausreichend zu untersuchen, zu analysieren und zu beheben. In Bezug auf die Begrifflichkeit des „Verlusts von Daten“ verweisen wir auf Kapitel 8.1.3.5 des erläuternden Berichts, welches explizit festhaltet, dass darunter auch der unterwünschte Zugriff auf Daten zu verstehen ist. Anpassungsvorschlag: Der Verantwortliche meldet dem Beauftragten ~~unverzüglich~~ ohne unnötigen Verzug nach Kenntnisnahme ~~eine unbefugte Datenbearbeitung oder~~ den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem hohen Risiko für die Persönlichkeit ~~und die Grundrechte~~ der betroffenen Person. Die gemeldete Verletzung wird nicht sanktioniert.
SBVg	DSG	17	2		Es ist nicht klar, wann und mit welchem Inhalt die betroffene Person genau zu informieren ist; nach Art. 34 DSGVO ist die betroffene Person nur zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person hat. Dies sollte im VE-DSG entsprechend angepasst werden. Anpassungsvorschlag: Der Verantwortliche informiert ausserdem die betroffene Person, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person in sich birgt ~~es zum Schutz der betroffenen Person erforderlich ist~~ oder der Beauftragte es verlangt.
SBVg	DSG	17	4		Absatz 4 ist nicht kongruent mit Absatz 1. Anpassungsvorschlag: Der Auftragsbearbeiter informiert den Verantwortlichen ~~unverzüglich~~ ohne unnötigen Verzug nach Kenntnisnahme über eine Verletzung gemäss Absatz 1. ~~über eine unbefugte Datenbearbeitung.~~
SBVg	DSG	18	1		Die schweizerische Regulierung weitet in diesem Punkt den Adressatenkreis auf den Auftragsbearbeiter aus. Wir beantragen, die Vorschrift an die Regelung der DSGVO anzupassen. Anpassungsvorschlag:

					Der Verantwortliche ~~und der Auftragsbearbeiter sind~~ ist verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit ~~oder der Grundrechte~~ verringern und solchen Verletzungen vorbeugen.
SBVg	DSG	18	2		Bei Art. 18 Abs. 2 VE-DSG geht es im Kern um „Privacy by default“ als Präzisierung des Verhältnismässigkeitsgrundsatzes im Sinne von Art. 4 Abs. 2 VE-DSG. Danach soll diejenige Datenbearbeitung voreingestellt sein, welche am schonendsten ist und nur das Minimum der erforderlichen Personendaten bearbeitet. Der gewählte Wortlaut bringt dieses Anliegen jedoch nur ungenügend zum Ausdruck. Richtigerweise sollte diese Bestimmung nicht an der Art bzw. Umfang der Personendaten, sondern am standardmässig vorgesehenen Zweck anknüpfen. Anpassungsvorschlag: Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen oder äquivalenter Methoden sicherzustellen, dass standardmässig ~~nur diejenigen~~ Personendaten nur derart bearbeitet werden, ~~die~~ wie es für den jeweiligen Verwendungszweck erforderlich ~~sind~~ ist.
SBVg	DSG	19		a	Diese Regelung geht über die vergleichbare Bestimmung der DSGVO hinaus (vgl. Art. 30 DSGVO). Letztere verlangt nämlich nur ein Verzeichnis. Richtigerweise sollte Art. 19 lit. a VE-DSG mit „ein Verzeichnis für regelmässige Datenbearbeitungen“ angepasst werden. Andernfalls müsste jede E-Mail, jede Chatnachricht etc. dokumentiert werden und damit wäre der Aufwand für die Dokumentation ungleich höher als das Verfassen einer E-Mail selbst. Alternativ könnte am bewährten Begriff der Datensammlung gemäss Art. 3 lit. g DSG festgehalten werden. Dieser würde eine bereits existierende und verlässliche Übersicht über die massgeblichen Datenbearbeitungen bieten (vgl. dazu oben unseren Vorschlag zu Art. 3 lit. c^{bis} (neu): Definition des Begriffs „Dateisystem“). Anpassungsvorschlag: Sie erstellen ein Verzeichnis für regelmässige Datenbearbeitungen, die ihrer Zuständigkeit unterliegen. ~~dokumentieren ihre Datenbearbeitung.~~
SBVg	DSG	19		b	Diese Pflicht geht sehr weit, ohne dass ein klarer datenschutzrechtlicher Mehrwert erkennbar ist. Selbst die DSGVO kennt solche Pflichten nicht. Weder der Verantwortliche noch dessen Auftragsdatenbearbeiter können selbst umfassend beurteilen, welche Daten für welche Empfänger

					überhaupt (noch) von Interesse sind. Nur mit Bezug auf solche Daten würde sich aber eine Information überhaupt rechtfertigen. Pauschale „Massen"-Informationen generieren nur unnötigen Aufwand beim Absender und Unklarheiten bei den zahlreichen Empfängern. Zudem bestehen dahingehende Ansprüche der betroffenen Personen bereits nach Art. 25 (vgl. insb. Abs. 1 lit. c). Wir beantragen deshalb, den Absatz ersatzlos zu streichen.
SBVg	DSG	20			Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen und überdies auf hängige Verfahren (vgl. Art. 2 Abs. 3) erachten wir als unverhältnismässig. Dies gilt umso mehr, als gemäss geltender Schweizer Rechtsprechung kein Auskunftsersuchen je rechtsmissbräuchlich sein kann, weil selbst ein untergeordnetes Datenschutzinteresse ausreicht, um einen Auskunftsanspruch zu bejahen. Die Anknüpfung am bisher bewährten System der Datensammlung wäre sachgerechter und würde den betroffenen Personen ausreichenden Schutz bieten (vgl. dazu oben unseren Vorschlag zu Art. 3 lit. c^{bis} (neu): Definition des Begriffs „Dateisystem").
SBVg	DSG	20	1		Dem zunehmenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke ist ein Riegel zu schieben. Daher ist der Ansatz falsch, das Auskunftsrecht generell kostenlos auszugestalten. Damit wird ein Grundprinzip verletzt, welches ansonsten in der Rechtsordnung generell gilt. Dementsprechend ordnet auch die DSGVO keine allgemeine Kostenlosigkeit an. Wir beantragen, die pauschale Kostenlosigkeit zu streichen und stattdessen einen angemessenen Unkostenbeitrag vorzusehen. Anpassungsvorschlag: Jede Person kann vom Verantwortlichen ~~kostenlos~~ Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.
SBVg	DSG	20	2	a	Vgl. die Ausführungen zu Art. 13 Abs. 2 lit. a VE-DSG. Anpassungsvorschlag: ~~die Identität~~ der Name und die Kontaktdaten des Verantwortlichen;
SBVg	DSG	20	2	b	Wir empfehlen eine dahingehende Präzisierung, als dass die Information nur die Kategorien der bearbeiteten Personendaten beinhalten sollte. Dies entspricht Art. 15 lit. b DSGVO. Anpassungsvorschlag: die Kategorien der bearbeiteten Personendaten;

SBVg	DSG	20	2	f	Wir erachten es als ausreichend, wenn die Herkunft der Personendaten dann angegeben werden muss, wenn die Daten nicht bei der betroffenen Person selbst erhoben wurden. Dies entspricht Art. 15 Abs. 1 lit. g DSGVO. Anpassungsvorschlag: die verfügbaren Informationen über die Herkunft der Personendaten, falls diese nicht bei der betroffenen Person erhoben werden;
SBVg	DSG	20	2	g	Empfänger der Daten schliesst auch Auftragsdatenbearbeiter ein. Es ist nicht praktikabel und kann operativ nicht sichergestellt werden, sämtliche Auftragsdatenbearbeiter inkl. Identität und Kontaktdaten zu nennen (vgl. auch DSGVO, wonach in Art. 15 Abs. 1 lit. b nur die Angabe von Kategorien von Empfängern verlangt wird). Anpassungsvorschlag: gegebenenfalls die Informationen nach Artikel 13 Absatz 2 lit. d (neu) und Absatz 3. ~~und 4~~.
SBVg	DSG	20	3		Der geforderte Umfang des Auskunftsrechts ist mit Blick auf die anderweitig im VE-DSG bereits bestehenden weitreichenden Informationspflichten weder sinnvoll noch nötig und produziert zusätzlichen Administrativaufwand ohne Mehrwert. Er würde ausserdem zwangsläufig zu einer Offenlegung von Geschäftsgeheimnissen z.B. in Form von internen Entscheid- und Ablaufverfahren führen. Die Regelung würde auch zu Unrecht eine Vermischung des allgemeinen Auskunftsrechts mit individuellen Auskünften zu Einzelentscheidungen produzieren. Eine gestützt auf Art. 20 erteilte allgemeine Auskunft hat in allgemeiner, übersichtlicher und leicht verständlichen Form den Anforderungen an die Auskunftspflicht zu genügen. Solche allgemeinen Auskünfte dürfen deshalb nicht mit einer Auflistung sämtlicher in der Vergangenheit durchgeführten individuellen Entscheidungen wie z.B. automatisierten Einzelentscheidungen ergänzt werden. Die vorgeschlagene Regelung geht sodann klar über den von den EU-Anforderungen gesetzten Rahmen hinaus (vgl. Art. 15 Abs. 1 lit. h DSGVO). Dies stellt einen kontraproduktiven Swiss Finish dar, welcher dem Regulierungsziel der Äquivalenz entgegensteht. Zusammenfassend ist die Regelung von Art. 20 Abs. 3 VE-DSG in Art. 20 zu streichen.
SBVg	DSG	20	5		Das in Art. 20 Abs. 5 VE-DSG vorgesehene subsidiäre Auskunftsrecht der betroffenen Person gegenüber dem Auftragsbearbeiter kann nicht aufrechterhalten werden, da ein solches jedem

					Verständnis in Bezug auf die gegenseitigen Rechte und Pflichten, die nur durch eine rechtliche Beziehung begründet werden können, widerspricht. Zwischen der betroffenen Person und dem Auftragsbearbeiter im Sinne des VE-DSG, der die Personendaten in der Regel gerade nicht für eigene Zwecke, sondern „nur" im Auftrag des Verantwortlichen bearbeitet – und somit nicht Inhaber der Daten ist – wird nie eine rechtliche Beziehung bestehen, die ein Auskunftsrecht der betroffenen Person begründen kann. Somit kann der Auftragsbearbeiter (z.B. ein Outsourcing-Dienstleister) gegenüber einer betroffenen Person auch nicht auskunftspflichtig werden. Im Falle einer Anfrage seitens der betroffenen Person, ob dieser Daten in Bezug auf seine Person bearbeitet, kann der Auftragsbearbeiter rechtlich gesehen nur eine negative Antwort geben. Wahrscheinlich aus gerade diesen Gründen ist in der EU-Datenschutzgesetzgebung (vgl. Art. 15 DSGVO) ein Auskunftsrecht der betroffenen Person nur gegenüber dem Verantwortlichen und nicht zusätzlich (oder subsidiär) gegenüber dem Auftragsbearbeiter vorgesehen. Letzteres darf auch nicht in die Schweizer Datengesetzgebung einfliessen. Anpassungsvorschlag: Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. ~~Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat.~~
SBVg	DSG	20	6		Es sollte im Gesetzestext explizit erwähnt werden, dass es sich beim Auskunftsrecht um ein subjektives höchstpersönliches Recht handelt. Anpassungsvorschlag: Niemand kann im Voraus auf das Auskunftsrecht verzichten. Das Auskunftsrecht ist ein subjektives und höchstpersönliches Recht.
SBVg	DSG	21	1		Die Ausnahmetatbestände von Art. 21 VE-DSG sind zu eng formuliert und überdies inkonsistent. So ist beispielsweise nicht einzusehen, weshalb die Informationspflicht bei Unmöglichkeit und Unzumutbarkeit nur entfallen soll, soweit der Verantwortliche die betreffenden Daten nicht Dritten bekannt gibt (Art. 14 Abs. 4 lit. a). Gleichwohl ist die Informationspflicht aber dann nicht nachzuholen, wenn dies nicht unmöglich oder unzumutbar ist (Art. 14 Abs. 5). Richtigerweise muss die Informationspflicht immer entfallen, wenn die Information nicht möglich oder unzumutbar ist, wie es auch die DSGVO vorsieht (Art. 12 Abs. 5 lit. b). Dies gilt umso mehr, als das Auskunftsrecht neu bei jeder

					Datenbearbeitung greift. Nicht nachvollziehbar ist auch, weshalb die Informationspflicht nach gesetzlicher Vorschrift nur bei indirekter Beschaffung durch Dritte entfallen soll (Art. 14 Abs. 2 lit. a). Umso mehr muss die Informationspflicht bei direkter Beschaffung entfallen. Dem Auskunftsverpflichteten muss sodann nach allgemeinen Rechtsgrundsätzen generell das Recht zustehen, das Auskunftsrecht unter Berufung überwiegender eigener Interessen einzuschränken oder sogar zu verweigern. Um dieser Regel griffige Konturen zu verleihen, sind - ohne Anspruch auf Vollständigkeit - typische Fallgruppen direkt im Gesetz aufzuführen. Anpassungsvorschlag: Die Auskunftspflicht entfällt, wenn die Auskunft nicht möglich oder unzumutbar ist. Zudem kann der Verantwortliche das Auskunftsrecht ~~unter den Voraussetzungen von Artikel 14 Absätze 3 und 4~~ unter Berufung auf überwiegende eigene Interessen verweigern, einschränken oder aufschieben. Als überwiegende eigene Interessen gelten insbesondere: a. Daten, welche die betroffene Person bereits erhalten hat, z.B. in Form von Verträgen, Abrechnung und Korrespondenzen; b. aufgrund einer gesetzlichen oder aufsichtsrechtlichen Pflicht bearbeitete Daten, z.B. zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption; c. Daten, welche vom Auskunftspflichtigen als Geschäftsgeheimnisse qualifiziert werden; d. rein intern bearbeitete Daten;
SBVg	DSG	21	1bis (neu)		In Angleichung an die Bestimmungen der DSGVO regen wir die Einführung eines Mechanismus zur Verhinderung des Missbrauchs des Auskunftsrechtes an. In diesem Zusammenhang wäre denkbar, eine in der Praxis bewährte Vorgehensweise aus dem Bereich der Strafverfolgung anzuwenden (vgl. Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI); SR 361): danach könnte der Verantwortliche bei begründetem Verdacht auf Missbrauch die herauszugebenden Personendaten einem Dritten (z.B. dem Beauftragten) übergeben. Dieser würde anstelle des Gesuchstellers die Einhaltung bzw. Verletzung des Datenschutzes prüfen und sein Prüfergebnis in Form einer anfechtbaren Verfügung vorlegen (vgl. eine analoge Regelung in Art. 8 Abs. 2 BPI). Im Übrigen sollte bei besonders aufwendigen Verfahren bzw. bei offenkundig unbegründeten oder

					exzessiven Anträgen, analog zur DSGVO, nach vorgängiger Abmahnung der betroffenen Person kein maximales Kostendach gelten. Vielmehr müssen die über den angemessenen Unkostenbeitrag hinaus effektiv angefallenen Kosten geltend gemacht werden dürfen. Dies ist mit rechtsstaatlichen Grundsätzen durchaus vereinbar, muss es doch auch darum gehen, den Auskunftspflichtigen vor uferlosem Aufwand infolge von klarem Rechtsmissbrauch zu schützen. Alternativ wäre analog DSGVO dem Bundesrat die Kompetenz einzuräumen, die Ausnahmen der Kostenlosigkeit auf Verordnungsstufe festlegen zu können. Anpassungsvorschlag: Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung - übermässigen Anträgen einer betroffenen Person kann der Verantwortliche entweder: a. ein angemessenes Entgelt verlangen, bei dem die Aufwandkosten für die Auskunft berücksichtigt werden, oder b. sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder übermässigen Charakter des Antrags zu erbringen. Lehnt der Verantwortliche ein Ersuchen nach diesem Absatz ab, kann die betroffene Person verlangen, dass der Beauftragte entscheidet, ob das Ersuchen datenschutzrechtlich motiviert ist.
SBVg	DSG	23	2	d	Die Relevanz von Profiling sollte wie in der DSGVO auf automatisierte Einzelentscheidungen beschränkt werden. Zudem ist das elektronische Profiling gesamtheitlich in Art. 15 VE-DSG zu regeln. Wir beantragen die ersatzlose Streichung dieses Swiss Finish.
SBVg	DSG	24	1		Die Rechtfertigung durch „Gesetz“ ist weiter zu definieren; andernfalls besteht ein Ungleichgewicht zwischen datenschutzrechtlichen und sonstigen rechtlichen Pflichten. Anpassungsvorschlag: Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch ~~Gesetz~~ gesetzliche oder aufsichtsrechtliche Vorschriften gerechtfertigt ist.
SBVg	DSG	24	2		Der Begriff „möglicherweise“ ist mangels Aussagekraft und Mehrwert unnötig, demzufolge in

					Gesetzestexten auch gänzlich unüblich und deshalb ersatzlos zu streichen. Anpassungsvorschlag: Ein überwiegendes Interesse der bearbeitenden Person ist ~~möglicherweise~~ gegeben, wenn diese~~r~~: […]
SBVg	DSG	24	2	a	Zur Herstellung eines in sich stimmigen Gesamtkonzepts ist hier dieselbe Ergänzung anzubringen, wie sie auch unter Art. 6 Abs. 1 lit. b notwendig ist. Anpassungsvorschlag: in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags oder einer Person, zu deren Gunsten oder in deren Interesse der Vertrag abgeschlossen wird, Personendaten über ihren Vertragspartner bearbeitet
SBVg	DSG	24	2	c Ziff. 1	Die Einschränkung gemäss Art. 24 Abs. 2 lit. c Ziff. 1 VE-DSG ist nicht sachgerecht und deshalb ersatzlos zu streichen. Sie verkennt, dass z.B. Massnahmen der sozialen Hilfe (Art. 3 lit. c Ziff. 6 VE-DSG) von zentraler Bedeutung für die Beurteilung der Kreditwürdigkeit sein können. Ein Verzicht darauf würde zu Fehlbewertungen führen, was nicht im Interesse der betroffenen Person sein kann.
SBVg	DSG	24	2	g (neu)	Schliesslich ist mit Art. 24 Abs. 2 lit. g (neu) VE-DSG ein Rechtfertigungsgrund einzuführen, welcher den Einsatz neuer Technologien (insbesondere Profiling) zur Steigerung der Sicherheit bzw. der Prävention von Straftaten gegen das Vermögen der betroffenen Person ermöglichen würde. Anpassungsvorschlag: die Daten zur Erhöhung der Sicherheit und Vermeidung von erheblichen Nachteilen für die betroffene Person bearbeitet werden, wofür sie auch Profiling durchführen kann.
SBVg	DSG	24	2	h (neu)	Art. 24 Abs. 2 lit. h (neu) VE-DSG entspricht dem Ausnahmetatbestand des Art. 14 Abs. 4 lit. a Ziff. 1 (neu) VE-DSG, der für die Information nach Art. 13 VE-DSG und das Auskunftsrecht gemäss Art. 20 VE-DSG gelten soll. Konsequenterweise muss dieser Ausnahmetatbestand auch als legitimes Interesse des Verantwortlichen gelten, das eine von den Datenschutzgrundsätzen (Art. 4 VE-DSG bzw. Art. 23 Abs. 2 lit. a VE-DSG) abweichende Bearbeitungen rechtfertigen kann. Anpassungsvorschlag: Personendaten zur Feststellung, Ausübung, Durchsetzung oder Verteidigung von Rechtsansprüchen bearbeitet.

SBVg	DSG	25	1	c	Wie bereits oben im Zusammenhang mit Art. 4 Abs. 4 und Abs. 5 VE-DSG (Grundsätze) erwähnt, können zwingende gesetzliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter der Vernichtung oder Löschung von Personendaten entgegenstehen (vgl. oben stehende Ausführungen zu Art. 4 Abs. 4 VE-DSG). Anpassungsvorschlag: Personendaten berichtigt werden; ~~, gelöscht oder vernichtet werden.~~
SBVg	DSG	25	1	d (neu)	Vgl. die Ausführungen zu Art. 25 Abs. 1 lit. c. Anpassungsvorschlag: Personendaten gelöscht oder vernichtet werden, sofern zwingende gesetzliche oder aufsichtsrechtliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter dem nicht entgegenstehen.
SBVg	DSG	25	3		Vgl. die Ausführungen zu Art. 25 Abs. 1 lit. c. Anpassungsvorschlag: Die klagende Partei kann zudem verlangen, dass das Unzugänglichmachen, sofern zwingende gesetzliche oder aufsichtsrechtliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter dem nicht entgegen stehen, die Berichtigung, ~~die Vernichtung,~~ das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.
SBVg	DSG	38	1		Eine Amtszeitbeschränkung ist eine in der Schweiz unübliche Praxis mit fragwürdigem Nutzen. Wir beantragen die ersatzlose Streichung dieser Bestimmung.
SBVg	DSG	39	1		Es muss sichergestellt werden, dass unter Mitglied der Verwaltung nicht die Verwaltung als Institution, sondern das oberste Exekutivorgan einer Gesellschaft verstanden wird. Anpassungsvorschlag: Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, ~~der Verwaltung~~ des Verwaltungsrats, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig werden.

SBVg	DSG	41	1		Die Einschränkung des geltenden DSG, wonach der EDÖB nur dann eine Untersuchung von sich aus durchführen kann, wenn eine grössere Zahl von Personen betroffen ist, muss in Art. 41 Abs. 1 VE-DSG wiederaufgenommen werden. Das Verfahren vor dem Beauftragten ist ein öffentlich-rechtliches. Es ist daher weder geeignet, noch dazu vorgesehen, um Ansprüche aus der Persönlichkeitsverletzung geltend zu machen. Dafür muss der zivilrechtliche Weg beschritten werden. Folglich ist es auch nicht sachgerecht, dass jede Datenschutzverletzung untersucht wird. Dies würde sowohl beim Beauftragten als auch beim Untersuchten unnötig wertvolle Ressourcen binden. Im Sinne der Verhältnismässigkeit sollte daher eine Untersuchung nur in schweren Fällen stattfinden. Anpassungsvorschlag: Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen**,** dass eine Datenbearbeitung ~~gegen die Datenschutzvorschriften verstossen~~ die Persönlichkeit einer grösseren Anzahl von Personen verletzen könnte.
SBVg	DSG	41	3		Im Unterschied zur DSGVO räumt der VE-DSG dem Beauftragen umfangreiche Ermittlungs- und Eingriffsbefugnisse ein. Dieser Swiss Finish ist abzulehnen. Diese Zwangsmassnahmen führen ausserdem zu Kompetenzkonflikten, wenn gleichzeitig eine Strafuntersuchung stattfindet. Aus Sicht der Verhältnismässigkeit sollte daher nur derjenige über Zwangsmittel verfügen, der das Strafverfahren führt. Im Übrigen unterscheidet sich die Untersuchung gemäss DSG genau darin von jener gemäss KG. Im Kartellrecht ist es die Verwaltungsbehörde, welche das "Strafverfahren" führt und die Sanktionen ausspricht. Im reinen Verwaltungsverfahren besteht aber für spezialgesetzliche Untersuchungsbefugnisse kein Raum. Es ist ferner nicht einzusehen, weshalb für das Verfahren beim Beauftragten nicht einfach wie im Verwaltungsrecht üblich, das VwVG anwendbar sein soll, wie das in Art. 44 ohnehin vorgesehen ist. Zudem ist fraglich, ob die Bestimmung im Einklang mit strafrechtlichen, untersuchungsrechtlichen und staatsrechtlichen Grundsätzen steht. Insbesondere ist unklar, wie vorzugehen ist, wenn ein gesetzliches/aufsichtsrechtliches Mitwirkungsverweigerungsrecht und/oder Recht auf Aussageverweigerung besteht. Bei der Inspizierung von Räumlichkeiten müssten dieselben Voraussetzungen eingehalten werden, wie dies heute bei Hausdurchsuchungen der Fall ist. Anpassungsvorschlag:

					Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte trotz angesetzter angemessener Frist die notwendigen ~~vergeblich versucht,~~ Auskünfte und Unterlagen nicht erhalten ~~einzuholen~~, so kann der Beauftragte im Rahmen einer Untersuchung, nach Erlass einer entsprechenden anfechtbaren Verfügung: a. ~~ohne Vorankündigung~~ Räumlichkeiten inspizieren;
SBVg	DSG	41	4		Diese Regelung ist zu präzisieren, zumal nicht klar ist, welche Überprüfungsbefugnisse der Beauftragte ausserhalb einer Untersuchung haben wird.
SBVg	DSG	41	5		Wir regen an, in Art. 41 Abs. 5 VE-DSG auch den Interessen der angezeigten Person Rechnung zu tragen. Insbesondere soll die angezeigte Person vom Beauftragten über das weitere Vorgehen und das Ergebnis einer allfälligen Untersuchung informiert werden. Anpassungsvorschlag: Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung. Der Beauftragte hat dabei die Interessen der angezeigten Person zu berücksichtigen. Zudem hat der Beauftragte auch die angezeigte Person über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung zu informieren.
SBVg	DSG	42			Die geltende Regelung (Art. 28 Abs. 4 DSG), wonach der Beauftragte beim Bundesverwaltungsgericht eine entsprechende Massnahme beantragen muss, hat sich bewährt und sollte nicht ohne Not geändert werden. Auch hier besteht kein Erfordernis über die allgemeinen Regeln des VwVG hinauszugehen. Zudem bleibt hier auch zu erwähnen, dass die betroffenen Personen auch auf zivilprozessualem Weg die Möglichkeit haben, entsprechende Massnahmen einzuleiten (vgl. Art. 28 ff. ZGB). Wir beantragen, die vorgesehene Formulierung zu streichen, und durch den Wortlaut der geltenden Regelung zu ersetzen. Anpassungsvorschlag: Wird eine solche Empfehlung des Beauftragten nicht befolgt oder abgelehnt, so kann er die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen. Er ist berechtigt, gegen diesen Entscheid Beschwerde zu führen.
SBVg	DSG	43			Der Beauftragte sollte diese Massnahmen nur ergreifen können, wenn er zuvor den Verantwortlichen beraten hat, es aber dennoch zu einer Verletzung kommt (im Sinne einer vorgängigen Abmahnung);

					i.V.m. Art. 44 VE-DSG haben die betroffenen Parteien Anspruch auf rechtliches Gehör (VwVG 29 ff.), welches hier zu gewähren sind. Wie bereits oben im Zusammenhang mit Art. 4 Abs. 4 und Abs. 5 VE-DSG (Grundsätze) und Art. 25 Abs. 3 VE-DSG (Rechtsansprüche) erwähnt, können zudem zwingende gesetzliche Vorschriften (z.B. Art. 958 f OR oder Art. 7 GwG) oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter der Vernichtung oder Löschung von Personendaten entgegenstehen (vgl. oben stehende Ausführungen zu Art. 4 und Art. 25 VE-DSG). Anpassungsvorschlag: Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden, sofern zwingende gesetzliche oder aufsichtsrechtliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter dem Unzugänglichmachen nicht entgegenstehen.
SBVg	DSG	44	3		Der Entzug der aufschiebenden Wirkung hat für die betroffenen Unternehmen weitreichende Folgen, möglicherweise auch erhebliche Wettbewerbsnachteile im Verhältnis zu direkten Konkurrenten. Wir beantragen deshalb die ersatzlose Streichung dieses Absatzes.
SBVg	DSG	45			Die Pflicht des Beauftragten, Strafverfolgungsbehörden zu informieren, sollte nicht über die Bestimmungen der DSGVO hinausgehen, nach jener besteht ein Recht zur Anzeige, nicht jedoch eine Pflicht. Anpassungsvorschlag: Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so kann ~~teilt~~ er dies den Strafverfolgungsbehörden mitteilen.
SBVg	DSG	47	1		Zum Terminus „beteiligten Dritter“ vgl. die Ausführungen zu Art. 3 lit. m VE-DSG. Diesbezüglich muss direkt in Art. 47 Abs. 1 VE-DSG - wie im erläuternden Bericht richtigerweise erwähnt - präzisiert werden, dass bei der Zurverfügungstellung von Personendaten in Bezug auf den Verantwortlichen, den Auftragsbearbeiter, einen (anderen) beteiligten Dritten oder den Empfänger, die Voraussetzungen des Art. 5 VE-DSG (Bekanntgabe ins Ausland) erfüllt werden müssen. Dies insbesondere, da es sich bei diesen Personen um natürliche Personen handeln kann, die als eigenständige Rechtssubjekte selbst den

					Bestimmungen des Datenschutzes unterliegen, und die Übermittlung ihrer Personendaten ins Ausland den Bestimmungen des Art. 5 VE-DSG (Bekanntgabe ins Ausland) unterliegt. Anpassungsvorschlag: Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen, sofern die Voraussetzungen des Art. 5 erfüllt sind:
SBVg	DSG	47	1	a	Der Zusatz „andere“ bei „beteiligen Dritten sollte gestrichen werden, da er gemäss oben stehenden Ausführungen unnötig ist. In Bezug auf den Vorschlag, den Begriff „Identität“ durch „Name“ zu ersetzen, verweisen wir auf unsere Ausführungen zu Art. 13 VE-DSG. Anpassungsvorschlag: den Namen ~~die Identität~~ des Verantwortlichen und des Auftragsbearbeiters oder von ~~anderer~~ ~~beteiligter~~ beteiligten Dritter;
SBVg	DSG	50 ff.			Hinsichtlich der im VE-DSG vorgeschlagenen Strafbestimmungen verweisen wir auf den Alternativvorschlag von economiesuisse, welchen wir sinngemäss unterstützen.
SBVg	DSG	54			Da dies bereits in der Strafprozessordnung geregelt ist, wird diese Bestimmung obsolet und ist ersatzlos zu streichen.
SBVg	DSG	55			Da dies bereits in Art. 109 des Strafgesetzbuches geregelt ist, wird diese Bestimmung obsolet und ist ersatzlos zu streichen.
SBVg	DSG	59			Die Übergangsbestimmungen beschränken sich auf die Regelungen von Art. 16, 18 und 19. In Tat und Wahrheit lässt sich der mit zahlreichen veränderten bzw. neuen Pflichten ausgestattete VE-DSG nur im Zuge einer umfassenden IT-gestützten Umstellung der gesamten internen Datenbearbeitungsprozesse bewerkstelligen. Dies geht weit über Art. 16, 18 und 19 VE-DSG hinaus und umfasst sämtliche geänderten oder neuen Pflichten und andern zur Strukturierung der rechtskonformen Datenbearbeitung notwendigen Regeln. Mit Blick auf die Komplexität des neuen VE-DSG erachten wir eine Umsetzungsfrist von mindestens 3 Jahren als absolut zwingend. Anpassungsvorschlag:

					Die Übergangsfrist für das ~~Zwei Jahre nach~~ Inkrafttreten dieses Gesetzes beträgt 3 Jahre. ~~a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen;~~ ~~b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.~~
SBVg	GwG	34	2		Vgl. die Anmerkungen zum unten vorgeschlagenen Art. 34bis GwG. Anpassungsvorschlag: Sie dürfen Daten aus diesen Datensammlungen nur an die FINMA, die Eidgenössische Spielbankenkommission, Selbstregulierungsorganisationen, die Meldestelle und Strafverfolgungsbehörden weitergeben. Vorbehalten bleibt die Weitergabe an Zweigniederlassungen des Finanzintermediärs und an vom Finanzintermediär mehrheitlich kontrollierte Tochtergesellschaften gemäss Artikel 34bis.
SBVg	GwG	34bis (neu)			Die FINMA konkretisiert das per 2016 in Kraft getretene revidierte Geldwäschereigesetz sowie die entsprechende GwV-FINMA dahingehend, dass ein Finanzintermediär, der Zweigniederlassungen im Ausland besitzt oder eine Finanzgruppe mit ausländischen Gesellschaften leitet, seine mit Geldwäscherei und Terrorismusfinanzierung verbundenen Rechts- und Reputationsrisiken global erfassen, begrenzen und überwachen muss (Art. 6 Abs. 1 GwV-FINMA). Gemäss Art. 6 Abs. 2 lit. a und b GwV-FINMA setzt die Pflicht zur gruppenweiten Erfassung, Begrenzung und Überwachung von Risiken im Bedarfsfall den Zugang der zuständigen Überwachungsorgane der Gruppe zu Informationen über einzelne Geschäftsbeziehungen voraus. Die Bestimmungen des Geldwäschereigesetzes sind daher dahingehend zu ergänzen, als dass der Informationsaustausch innerhalb der Finanzgruppe im In- und Ausland zulässig ist, falls und soweit dieser zur Erfüllung der Pflichten aus GwG erforderlich ist. Dies entspricht auch der in der Präambel (19) der DSGVO festgehaltenen Bestimmung, dass die Mitgliedstaaten Erlasse beschliessen können, welche die in der DSGVO festgehaltenen Pflichten und Rechte beschränken, soweit dies zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung erforderlich und verhältnismässig ist. Anpassungsvorschlag: Weitergabe an Zweiniederlassungen und mehrheitlich kontrollierte Tochtergesellschaften eines

					Finanzintermediärs Sofern zur Erfüllung der in diesem Gesetz festgelegten Pflichten erforderlich, darf der Finanzintermediär, Informationen an Zweigniederlassungen und an von ihm mehrheitlich kontrollierte Tochtergesellschaften im In- und Ausland weitergeben. Davon eingeschlossen sind sämtliche für die globale Überwachung der Rechts- und Reputationsrisiken wesentlichen Informationen, inklusive Informationen über einzelne Geschäftsbeziehungen und Informationen aus Datensammlungen gemäss Art. 34.
SBVg	OR	328		b	Vgl. Ausführungen zu Art. 2 Abs. 2 lit. e (neu) VE-DSG. Anpassungsvorschlag: Der Arbeitgeber darf Daten, die die Persönlichkeit des ~~über den~~ Arbeitnehmers betreffen nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Im Übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz, es sei denn der Arbeitgeber bearbeitet Personendaten des Arbeitnehmers, die im Zusammenhang mit der Ausübung seiner beruflichen Tätigkeit für das Unternehmen stehen.

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
SBVg	8.1.1.2	Wir regen an, oben stehende Ausführungen zu Art. 2 in den Erläuterungsbericht aufzunehmen und zwar am Ende des Abschnitts, der mit „Aufhebung des Schutzes für Daten juristischer Personen“ betitelt ist.
SBVg	8.1.2	Viele Schweizer Unternehmen werden neben den Bestimmungen des DSG auch jene der DSGVO einhalten müssen. Dies führt zu zusätzlichem Administrationsaufwand und ruft zahlreiche Rechtsunsicherheiten hervor, da die DSGVO keine klaren Regeln in Bezug auf ihre Geltung für Unternehmen ausserhalb des Territoriums der EU enthält. Auch besteht das Risiko, sich nach der schweizerischen Rechtsordnung strafbar zu machen (Art. 271 StGB). Das Konzept des One-Stop-Shop kommt ausserhalb der EU nicht zur Anwendung (Art. 56 DSGVO). Auch scheint ein Schweizer Unternehmen als Rechtfertigungsgrund für eine Datenbearbeitung nicht anführen zu dürfen, dass hierfür eine Verpflichtung nach Schweizer Recht besteht (s. Art. 6 Abs. 1 Bst. c DSGVO i.V. m. Art. 6 Abs. 3 DSGVO). Es besteht daher dringender Abstimmungsbedarf zwischen der Schweiz und der EU, um die beiden Datenschutzgesetzgebungen miteinander in Einklang zu bringen. Es muss dabei gelten, dass die Aufsicht auf dem jeweiligen Hoheitsgebiet alleine Sache der jeweils nationalen Behörde nach lokalem Recht ist und dass für die anwendbaren Melde-, Genehmigungs- und Informationspflichten der Schweizer Unternehmen einzig der Beauftragte zuständig ist. Der Austausch zwischen den Datenschutzbehörden der EU und der Schweiz erfolgt über die hierfür vorgesehene Amtshilfe. Bei den anstehenden Arbeiten – die Motion 16.3752 „Gegen Doppelspurigkeiten im Datenschutz“ von Nationalrätin D. Fiala wurde an den Bundesrat überwiesen – ist jedoch dem etablierten prinzipienbasierten Ansatz Rechnung zu tragen.
SBVg	8.1.2.3	Die Erläuterungen sollten klarstellen, dass unter „Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen“ auch die „Abwehr“ bzw. „Verteidigung“ gegen Rechtsansprüche zu verstehen ist.
SBVg	8.1.4.1	Die geforderte Information über das Vorliegen einer automatisierten Einzelentscheidung muss im Rahmen der allgemeinen Auskunftspflicht nicht eine detaillierte Auflistung aller in der Vergangenheit ausgeführten automatisierten Einzelentscheidungen beinhalten.
SBVg	8.1.4.1	Wir regen an zu präzisieren, dass die Information gemäss Art. 20 Abs. 2 lit. b VE-DSG die Kategorien der bearbeiteten Personendaten, die über die betroffene Person bearbeitet werden, umfasst, nicht aber eine Kopie jeglicher über diese bearbeiteten Personendaten.

Amstutz Jonas BJ

Von: Stephan Obwegeser <stephan.obwegeser@schober.ch>
Gesendet: Dienstag, 4. April 2017 10:59
An: Amstutz Jonas BJ
Betreff: Vernehmlassung DSG - Stellungnahme Schober
Anlagen: Vernehmlassung_VE DSG_Schober_20170403_SO.docx

Sehr geehrter Herr Amstutz

Anbei erhalten Sie termingerecht die Stellungnahme der Schober Information Group (Schweiz) AG zum Vorentwurf des Bundesgesetzes über die Totalrevision des Datenschutzgesetzes.

Bei Rückfragen stehe ich Ihnen gerne zur Verfügung!

Beste Grüsse,

Stephan Obwegeser
CEO | Geschäftsführer
Schober Information Group (Schweiz) AG
Bramenstrasse 5
CH-8184 Bachenbülach
Telefon +41 44 864 22 80
Telefax +41 44 864 23 25
Mobile +41 78 613 33 55
E-Mail stephan.obwegeser@schober.ch
www.schober.ch
www.adressenonline.ch - www.adressesonline.ch - www.indirizzionline.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schober Information Group (Schweiz) AG

Abkürzung der Firma / Organisation : Schober

Adresse : Bramenstrasse 5, 8184 Bachenbülach

Kontaktperson : Stephan Obwegeser

Telefon : 044 864 22 11

E-Mail : stephan.obwegeser@schober.ch

Datum : 3. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Schober	Schober begrüsst die Revision des Datenschutzgesetzes. Nicht nur beim Geschäftsmodell von Schober, sondern generell in der immer digitalisierteren Wirtschaft hat das Datenschutzrecht eine immer grössere Bedeutung. Bei digitalen Geschäftsmodellen ist einerseits das Vertrauen des Kunden in die korrekte und transparente Datenbearbeitung von besonderer Wichtigkeit. Gleichzeitig dürfen jedoch innovative und nutzenstiftende Geschäftsmodelle nicht unverhältnismässig und unnötig eingeschränkt werden. Die weiterhin schnell voranschreitende Digitalisierung lässt sich nicht aufhalten – deshalb ist für alle Anspruchsgruppen wichtig, dass Rechtssicherheit betreffend die Anforderungen an die Datenbearbeitung besteht. Dies insbesondere auch dann, wenn die Verletzung dieser Anforderungen mit Sanktionen bedroht ist. Bei digitalen Geschäftsmodellen sind grenzüberschreitende Datenbearbeitungen relativ häufig – auch bei Schober. Zudem besteht betreffend die Erbringung von Dienstleistungen im digitalen Raum regelmässig eine sog. Ubiquität, d.h. entsprechende Dienstleistungen müssen, selbst wenn sie gegenüber Kunden mit Sitz in der Schweiz angeboten werden, nicht zwingend von der Schweiz aus erbracht werden. Schober und auch andere Unternehmen mit vergleichbarem Geschäftsmodell befinden sich damit in einem Wettbewerb mit ausländischen Anbietern. Es ist für Schober wichtig, dass aufgrund der vorgesehenen Datenschutzrevision keine Wettbewerbsnachteile gegenüber ausländischen Konkurrenten entstehen. Das Geschäftsmodell von Schober ist bekanntlich besonders datenabhängig. Schober hilft seinen Kunden, zu denen zahlreiche schweizerische KMUs aber auch grosse Verlage, Grossverteiler, Banken und Versicherungen gehören, dabei, potentielle Kunden sowie bestehende Kunden und Konsumenten personalisiert und zielgerichtet anzusprechen. Die Dienstleistungen von Schober sind damit für deren Kunden betriebswirtschaftlich von grosser Bedeutung. Dank der personalisierten und zielgerichteten Ansprache kann das Marketingbudget effizienter und mit mehr Wirkung eingesetzt werden. Dies ist für die betreffenden Unternehmen beim immer härter werdenden Wettbewerb überlebensnotwendig. Personalisiertes und zielgerichtetes Marketing ist für jedes Unternehmen die Basis für den wirtschaftlichen Erfolg! Die personalisierte Werbung ist jedoch nicht nur für die werbetreibenden Unternehmen ein Erfolgsfaktor und damit nutzenbringend. Personalisierte Werbung bringt auch den Konsumenten einen Mehrwert. Die Konsumenten erhalten nur die Informationen, welche sie interessieren, d.h. für sie relevant sind. Es besteht ein berechtigtes, gesamtwirtschaftliches Interesse an den Dienstleistungen von Schober. Die Dienstleistungen von Schober können jedoch durch Informationspflichten, Regelungen zum Profiling sowie Sorgfaltspflichten, je nach Ausgestaltung, erschwert oder gar verunmöglicht werden. Dies würde sich wiederum negativ auf die Kunden von Schober und damit auf die Gesamtwirtschaft auswirken. Für die betroffenen Personen ist darüber hinaus nichts gewonnen, wenn werbetreibende Unternehmen ihre Marketingdienstleistungen bei Anbietern im Ausland mit niedrigeren datenschutzrechtlichen Anforderungen beziehen.

	Vor diesem Hintergrund lehnt Schober jeden Swiss Finish ab. Die Revision des Datenschutzgesetzes soll sich auf die Einhaltung der Vorgaben der Europarats-Konvention (E-SEV 108) und die Angemessenheit im Hinblick auf die EU beschränken. Den „Swiss Finish“ bei einzelnen Regelungen (z.B. beim Profiling und bei der Sanktionierung von Verstössen) lehnen wir strikte ab. Zur Bestehung der Angemessenheitsprüfung muss die EU-DSGVO nicht eins zu eins übernommen werden. In der aktuellen Fassung müssen wir den vorgelegten Vorentwurf des neuen DSG ablehnen. Insbesondere das vorgesehene Sanktionssystem, mit dem eine weitgehende Kriminalisierung von natürlichen Personen in den datenbearbeitenden Unternehmen erfolgt, ist inakzeptabel.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Schober	DSG	1			Als weiterer Zweck ist die „Förderung des freien Verkehrs von Personendaten“ in die Zweckbestimmung aufzunehmen.
Schober	DSG	3		a	**Wir begrüssen, dass keine Änderung am Begriff der „Personendaten“ vorgenommen wird.** Die Ausführungen zu Art. 3 lit. a VE-DSG im erläuternden Bericht könnten allerdings zu Diskussionen führen. Es wird dort aus Erwägungsgründen zur EU-DSGVO zitiert, welche in der EU für Unklarheiten sorgten. Die Zitate sind zu streichen. Vielmehr ist auf die bisherige Praxis und Rechtsprechung in der Schweiz zu verweisen. Entscheidend ist aus Sicht von Schober, dass die sog. relative Methode betreffend die Bestimmbarkeit einer natürlichen Person in den Materialien, d.h. der Botschaft, explizit anerkannt wird.
Schober	DSG	3		f	**Wir lehnen die vorgeschlagene Definition des „Profiling“ ausdrücklich ab. Es handelt sich um einen Swiss Finish. Er geht ohne Not über die Regelung in der EU-DSGVO (Art. 4 Ziff. 4) hinaus.** Die E-SEV 108 verlangt die vorgeschlagene Regelung ebenfalls nicht. Für das Geschäftsmodell und die Dienstleistungen von Schober ist es besonders wichtig, dass das Profiling im Gesetzeswortlaut, aber vor allem auch in den Materialien viel konkreter umschrieben wird. Aus Sicht des Persönlichkeitsschutzes besteht nicht bei jeder Auswertung und Analyse ein erhöhtes Schutzbedürfnis. Dies war unter dem geltenden Recht bei der Praxis zum Persönlichkeitsprofil bereits anerkannt und sollte nun auch beim Profiling klar so verankert werden. Dies auch wenn zwischen dem Profiling als dynamische Tätigkeit und dem Persönlichkeitsprofil quasi als Ergebnis eines

					Profiling ein Unterschied besteht. Das Profiling ist auf automatisierte Bearbeitungen zu beschränken. Bei manuellen Auswertungen und Analysen reichen die Datenbearbeitungsgrundsätze aus. Zu streichen ist zuletzt die Unterscheidung zwischen Personendaten und Daten, d.h. nicht personenbezogenen Daten. Diese Unterscheidung bringt keinen Mehrwert, sondern führt lediglich zu Verwirrung.
Schober	DSG	4	3		**Das Erfordernis der „klaren" Erkennbarkeit ist zu streichen**. Im erläuternden Bericht wird zu Recht darauf hingewiesen, dass keine inhaltliche Änderung beabsichtigt wird. Dann ist auch keine sprachliche Änderung notwendig. Diese führt zudem zu Unklarheiten und damit zu Rechtsunsicherheit. Darüber hinaus ist in den Materialien explizit festzuhalten, dass die Daten nicht nur für einen einzigen Zweck bearbeitet werden dürfen. Der Wortlaut hat hier für Unklarheiten gesorgt. Wie nach geltendem Recht ist es erlaubt, die Daten für mehrere Zwecke zu bearbeiten, sofern diese genügend transparent gemacht wurden.
Schober	DSG	4	5		Gemäss Seite 47 des erläuternden Berichts sind keine materiellen Änderungen beabsichtigt. Es gibt keinen Grund dafür, den Wortlaut zu ändern. Dies führt lediglich zu Missverständnissen und Unklarheiten.
Schober	DSG	4	6		**Auch betreffend die Begriffsbestimmung der „Einwilligung" ist nicht ersichtlich, weshalb eine terminologische Annäherung notwendig sein soll, wenn sich inhaltlich an der Einwilligung nichts ändert**. Vorliegend ist auf eine Änderung zu verzichten. Wird die vorgeschlagene Terminologie beibehalten, ist in den Materialien explizit klarzustellen, dass sich inhaltlich an der Interpretation des Begriffes „Einwilligung" und an den Anforderungen an diese gegenüber dem geltenden DSG nichts ändert.

					Unklar bzw. unbestimmt und widersprüchlich sind sodann die Ausführungen im erläuternden Bericht zur ausdrücklichen Einwilligung. Dies wiegt vorliegend beim Geschäftsmodell von Schober insofern schwer, als z.B. das Profiling ohne ausdrückliche Einwilligung grundsätzlich eine Persönlichkeitsrechtsverletzung darstellt. Der Umstand, dass sowohl „Profiling" als auch „ausdrückliche Einwilligung" nicht zweifelsfrei bestimmt sind, führt zu einer Rechtsunsicherheit. In den Materialien ist zuletzt klarzustellen, dass die Einwilligung – auch die ausdrückliche – wie bisher durch Zustimmung zu einem Dokument erteilt werden kann, in welchem auch weitere Informationen enthalten sind (z.B. AGB oder Datenschutzerklärungen).
Schober	DSG	5+6			**Bei den Regelungen zur Bekanntgabe von Daten ins Ausland handelt es sich um einen Swiss Finish.** Auf diesen ist zu verzichten. Zur Einhaltung der E-SEV 108 ist unseres Erachtens keine inhaltliche Änderung der Datentransfer-Regelung im bestehenden DSG notwendig. Auch die EU-DSGVO bzw. die Sicherstellung der Angemessenheit zum betreffenden Datenschutzstandard verlangt keine solch komplizierte Umsetzung. Unnötig – und auch durch die EU-DSGVO nicht gefordert – ist die generelle Informationspflicht bei der Nutzung von standardisierten Garantien (Art. 5 Abs. 6 VE-DSG). Es geht hierbei um die Nutzung von Garantien, welche durch den EDÖB anerkannt bzw. genehmigt wurden. Zuletzt ist in Art. 6 Abs. 1 lit. a VE-DSG der Zusatz „im Einzelfall" zu streichen. Bei wiederkehrenden Sachverhalten und unveränderter Erkennbarkeit und Erwartung muss eine einmalige Zustimmung ausreichen.
Schober	DSG	7			**Auch bei der vorgeschlagenen Regelung zur Auftragsbearbeitung handelt es sich um einen Swiss Finish**. Die bestehende Regelung würde für die Einhaltung der E-SEV 108 ausreichen. Für die Angemessenheit würde die bestehende Regelung ebenfalls ausreichen.

					Die Anforderungen an den Beizug von Subunternehmern führen im wirtschaftlichen Alltag zu unnötigen Beeinträchtigungen. Die betroffenen Personen gewinnen durch die vorgeschlagenen Regelungen im Vergleich zum bestehenden DSG nichts. Für die betroffenen Personen ist entscheidend, dass der Verantwortliche für alle Auftragsdatenbearbeitungen letztverantwortlich bleibt. Zuletzt ist die unbeschränkte Delegation zur Festlegung weiterer Pflichten an den Bundesrat zu streichen. Die Anforderungen an die Auftragsdatenbearbeitung sind bereits nach geltendem Recht ausreichend. Es ist nicht ersichtlich, weshalb der Bundesrat eine gesetzesvertretende Kompetenz erhalten soll.
Schober	DSG	8	1		**Schober unterstützt die Einführung von Empfehlungen der guten Praxis**. Wir sind jedoch der Auffassung, dass der EDÖB kein Letztgenehmigungsrecht erhalten darf. Das Genehmigungsrecht ist einer neutralen Instanz zuzuweisen. Dies auch aus rechtsstaatlichen Gesichtspunkten – Stichwort Gewaltenteilung. Der Anstoss für solche Empfehlungen muss zudem zwingend aus der Praxis und den Verbänden kommen. Der EDÖB sollte daher in keinem Fall die Kompetenz erhalten, selber solche Empfehlungen vorzuschlagen.
Schober	DSG	8	2		**Schober ist der Ansicht, dass gegen Empfehlungen der guten Praxis, d.h. den Erlass oder die Nicht-Genehmigung solcher Empfehlungen, ein Rechtsmittelweg offenstehen muss**. Dieser Rechtsmittelweg ist im Gesetz zu regeln, wobei insbesondere auch klarzustellen ist, wer zur Ergreifung eines Rechtsmittels legitimiert sein soll.
Schober	DSG	12			**Es handelt sich um einen Swiss Finish**. Die Regelung ist zu streichen. Sie wäre gesetzessystematisch ohnehin ins Zivilgesetzbuch einzubauen.
Schober	DSG	13			Unseres Erachtens ist fraglich, ob die vorgeschlagene aktive Informationspflicht gegenüber der Transparenzpflicht im geltenden DSG für die betroffenen

					Personen zu einem Mehrwert führt. **Bei der Ausgestaltung der Informationspflicht und vor allem bei den Anforderungen an deren Umsetzung ist im Auge zu behalten, dass diese Pflicht die Transparenz der Datenbearbeitungen fördern soll.** Zudem ist zu berücksichtigen, dass das Datenschutzrecht einen risiko-basierten Ansatz verfolgen soll. Es ist daher nicht ganz ersichtlich, weshalb bei jeder Datenbearbeitung – selbst bei solchen mit sehr geringem oder gar keinem datenschutzrechtlichen Risiko – eine generelle und aktive Informationspflicht vorausgesetzt wird. Klarzustellen ist in den Materialien, wie die Informationspflicht umzusetzen ist. In den Materialien ist diesbezüglich explizit darauf hinzuweisen, dass die Information auch in Form von standardisierten Datenschutzerklärungen auf der Webseite erfüllt werden kann. Es muss hierbei, wie nach geltendem Recht, genügen – und dies ist in den Materialien ebenfalls klarzustellen –, dass z.B. bei einem Bestellformular oder einer Bestellkarte auf diese Datenschutzerklärungen auf der Webseite verwiesen werden kann. Des Weiteren ist klarzustellen, dass die Informationspflicht sich auf Angaben bezieht, die im Zeitpunkt der Datenbeschaffung bestehen bzw. bekannt sind. Eine spätere Neuinformation ist, wie unter geltendem Recht, nicht notwendig bzw. müsste sich aus einer anderen Bestimmung des DSG (z.B. dem Transparenzgebot) ergeben.
Schober	DSG	13	2		Die Informationspflicht ist auf diejenigen Angaben zu beschränken, welche für die Transparenz notwendig sind. Die Auflistung muss abschliessend sein. Offene Rechtsbegriffe oder Umschreibungen der Pflicht sind zu vermeiden. Dies auch deshalb, weil die Verletzung der Informationspflicht mit Sanktionen bedroht ist.
Schober	DSG	13	4		**Es handelt sich hierbei um einen unnötigen Swiss Finish, der zu streichen ist**. Sie bringt für den Betroffenen keinerlei Mehrwert.
Schober	DSG	13	5		Die Ausdehnung der Pflicht auf die indirekte Datenbeschaffung wird in der Praxis

					jegliche Beschaffung von Daten bei Dritten verunmöglichen. Dies insbesondere für Unternehmen mit einem vergleichbaren Geschäftsmodell wie Schober. Damit Unternehmen potenzielle Neukunden ansprechen können, sind indirekte Datenbeschaffungen unumgänglich. Wird dies verunmöglicht, erleiden die Unternehmen – im Vergleich zu ausländischen Wettbewerbern – einen Nachteil. **Die Bestimmung ist zu streichen.** Sofern daran festgehalten wird, muss es analog zur EU-DSGVO und dem E-SEV 108 auch in der Schweiz zulässig sein, die Information zu späteren Zeitpunkten zu erteilen. Aus dem Vorentwurf und dem erläuternden Bericht geht zudem nicht hervor, wie die Informationspflicht bei der indirekten Beschaffung umzusetzen ist. Es muss auch hier möglich sein, die Detailinformationen in einer standardisierten Datenschutzerklärung auf der Webseite aufzuführen.
Schober	DSG	14			**Der Katalog der Ausnahmen ist enger gefasst, als es nach dem E-SEV 108 erforderlich wäre (Swiss Finish)**. Der Ausnahmekatalog soll mindestens die Ausnahmen gemäss E-SEV 108 enthalten.
Schober	DSG	15			Der Anwendungsbereich der vorgeschlagenen Regelung geht zu weit. Es ist klarzustellen, **dass auch rechtliche Auswirkungen eine gewisse Schwere erreichen müssen.** Zudem sind die Ausnahmen in Art. 22 EU-DSGVO (z.B. wenn die automatisierte Einzelfallentscheidung für die Abwicklung eines von der betroffenen Person gewünschten Vertrages notwendig ist) in Art. 15 VE-DSG aufzunehmen. Die E-SEV 108 würde solche Ausnahmen zulassen.
Schober	DSG	16			**Die vorgeschlagene Regelung zur Datenschutz-Folgenabschätzung stellt ebenfalls einen Swiss Finish dar, auf den zu verzichten ist.** Selbst eine einzelne Datenbekanntgabe ins Ausland könnte theoretisch die Pflicht

					zur Folgenabschätzung und Notifikation an den EDÖB auslösen. Die damit verbundene Belastung der Unternehmen und auch des EDÖB ist unnötig und unverhältnismässig. Die Regelung muss so ausgestaltet werden, dass nur Datenbearbeitungsprozesse, welche regelmässig durchgeführt werden, eine Datenschutz-Folgenabschätzung auslösen können. Art. 35 EU-DSGVO erwähnt z.B. die systematische Bearbeitung besonders schützenswerter Daten oder das umfangreiche Profiling. Entsprechend der EU-Regelung **sind nur regelmässige Datenbearbeitungen mit „hohem Risiko" (oder besser „besonders hohem Risiko") zu erfassen**. **Die vorgeschlagene Regelung geht in weiteren Punkten über die EU-DSGVO hinaus (Swiss Finish)**: Art. 35 DSGVO verpflichtet im Gegensatz zu Art. 16 VE-DSG den Auftragsbearbeiter nicht. Die E-SEV 108 sieht ebenfalls nicht vor, dass der Auftragsbearbeiter eine Datenschutz-Folgenabschätzung durchführen muss. Die vorgeschlagene Ausdehnung auf den Auftragsbearbeiter ist zu streichen. **Bei der Notifikationspflicht an den EDÖB handelt es sich ebenfalls um einen unnötigen Swiss Finish**. Art. 36 EU-DSGVO verlangt die Notifikation nicht bei jeder Datenschutz-Folgenabschätzung. Die Ausgestaltung der Notifikationspflicht in Art. 36 EU-DSGVO ist für die Schweiz zu übernehmen. Zudem ist die Reaktionsfrist des EDÖB zu verkürzen.
Schober	DSG	17	1		**Nach der vorgeschlagenen Regelung besteht gegenüber dem EDÖB grundsätzlich für jede „unbefugte Datenbearbeitung" eine Meldepflicht**. Dabei handelt es sich um ein **schweizerisches Überschiessen (Swiss Finish)**. Entsprechend der Vorgabe im E-SEV 108 (Art. 7 Abs. 2**) ist die Meldepflicht auf Verletzungen zu beschränken, welche die Rechte der Betroffenen „schwerwiegend" („seriously") gefährden könnten.**
Schober	DSG	17	2		**Die Meldepflicht gegenüber Dritten ist ein Swiss Finish und daher zu streichen**. Eine derart weitgehende und aufwändige administrative

					Zusatzbelastung ist in der EU-DSGVO (Art. 19) nicht vorgesehen.
Schober	DSG	18			**Die Anforderungen an die Datenbearbeiter durch diese beiden Pflichten sind unklar.** Zusammen mit der Strafbedrohung wirkt sich diese Rechtsunsicherheit erheblich negativ aus. Die Grundsatzfragen müssen im Gesetz geregelt werden. Im Zweifelsfalle, d.h. ist es nicht möglich, die Pflichten klarer zu umschreiben, ist auf eine Sanktionierung zu verzichten. Eine indirekte Sanktionierung kann immer noch dadurch erfolgen, dass der EDÖB nach erfolgter Untersuchung Empfehlungen abgibt oder die Implementierung gewisser Massnahmen verfügt.
Schober	DSG	19		a	**Der Umfang der Dokumentationspflicht ist unklar**. Es ist konkreter festzulegen, welche Angaben über eine Datenbearbeitung dokumentiert werden müssen. Zudem ist klarzustellen, dass es sich dabei nicht um die Dokumentation einer einzelnen Datenbearbeitung handeln kann. Ansonsten würde die Dokumentationspflicht, insbesondere für kleinere Unternehmen zu einem unnötigen Aufwand führen. Zudem sind wie in der EU-DSGVO Ausnahmen von der Dokumentationspflicht vorzusehen.
Schober	DSG	19		b	**Eine solche Mitteilungspflicht ist im E-SEV 108 nicht vorgesehen (Swiss Finish). Sie ist deshalb ersatzlos zu streichen.** Sofern an ihr festgehalten werden sollte, ist die Pflicht auf Konstellationen zu beschränken**, in denen die betroffene Person ein schützenswertes Interesse hat**. Die vorgeschlagene Regelung geht zudem **wiederum unverständlicherweise über die Vorgaben der EU-DSGVO (Art. 19) hinaus, indem Verletzungen des Datenschutzes auch den Empfängern offen gelegt werden müssen (Swiss Finish)**.
Schober	DSG	20	1		**E-SEV 108 verlangt nicht, dass die Ausübung des Auskunftsrechts kostenlos sein muss.** Es wird nur verlangt, dass die Auskunftserteilung ohne

					übermässige Kosten erfolgen muss („without excesive expense"; Art. 8 Abs. 1 lit. b). Eine angemessene Aufwandsentschädigung ist damit weiterhin zulässig.
Schober	DSG	20	3		**Es handelt sich wiederum um einen Swiss Finish, der zum Schutz der betroffenen Personen nicht erforderlich ist.** **Das Auskunftsrecht bei automatisierten Einzelfallentscheidungen ist viel zu weit gefasst und nach der vorgeschlagenen Regelung geradezu uferlos.** Entsprechend der Regelung in der EU-DSGVO (Art. 15 Abs. 1 lit. h) ist das Auskunftsrecht auf diejenigen Fälle zu beschränken, in welchen auch eine Informations- und Anhörungspflicht nach Art. 15 VE-DSG besteht, also auf Entscheidungen, die automatisiert erfolgen und entsprechende Auswirkungen haben.
Schober	DSG	23			**Das generelle Erfordernis der ausdrücklichen Einwilligung für das Profiling stellt eine der problematischsten Schweizer Verschärfungen dar und ist zwingend zu streichen (Swiss Finish)**. Wie bereits erwähnt, ist aufgrund der vorgeschlagenen Begriffsbestimmung unklar, wann ein Profiling vorliegt. Wenn zudem für dieses Profiling eine ausdrückliche Einwilligung notwendig ist, wirkt sich diese begriffliche Unklarheit auf Schober, aber auch viele andere Unternehmen, erschwerend aus. Es ist hierbei zu beachten, dass personalisiertes Marketing im Interesse der betroffenen Personen ist. Zudem schadet eine unnötige Erschwerung der Gesamtwirtschaft. Insbesondere KMUs sind auf gute und effiziente Marketingmöglichkeiten angewiesen, um sich auf dem Markt sichtbar zu machen. **Wird diese Vorschrift Gesetz, verunmöglicht sie faktisch einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung / Marketing und stellt eine Bedrohung für den Standort Schweiz dar**. Profiling und damit personalisierte Werbung wäre dann nur noch den

					grossen (insbesondere internationalen) Unternehmen vorbehalten.
Schober	DSG	23	3		Die Beibehaltung der geltenden Regelung von allgemein zugänglich gemachten Daten ist zu begrüssen. Dabei ist jedoch die Erwägung im erläuternden Bericht, wonach die Regelung nur zum Tragen komme, wenn die Bearbeitung dieser Daten auch rechtmässig erfolgt (S. 69), unzutreffend und daher in der Botschaft klar zu stellen.
Schober	DSG	25			**Der letzte Satz in Absatz 2 ist ersatzlos zu streichen**. Es handelt sich um einen Swiss Finish. Weder die E-SEV 108 noch die DSGVO sehen vor, dass neben dem Bestreitungsvermerk auch eine Beschränkung der Datenbearbeitung verlangt werden kann.
Schober	DSG	44	3		**Gegen vorsorgliche Massnahmeverfügungen des EDÖB sind Rechtsmittel mit aufschiebender Wirkung zur Verfügung zu stellen.** Die Massnahmen können bei den Unternehmen zu erheblichen Schäden führen.
Schober	DSG	50 ff.			**Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt**. Dieses vorgesehene Sanktionssystem steht der Digitalen Strategie der Schweiz diametral entgegen. Es führt zu einem ganz erheblichen Standortnachteil der Schweiz. Die vorgeschlagene Sanktionsregelung führt dazu, dass die für Datenbearbeitungen verantwortlichen Personen in den Unternehmen direkt mit Strafrisiken bedroht sind. Die subsidiäre Haftung des Unternehmens dürfte gerade bei kleineren Unternehmen, wo die verantwortliche Person relativ leicht eruiert werden kann, nicht zur Anwendung gelangen. Die Strafrisiken für die verantwortlichen Personen würden dazu führen, dass kein Mitarbeiter bereit wäre, die Funktion eines internen Datenschutzbeauftragten zu übernehmen. Dies ist aus Sicht der Datenschutz-Compliance negativ. Zudem würde die Strafbarkeit der Mitarbeiter dazu führen, dass diese – allenfalls vorschnell – Verstösse und

					vermeintliche Verstösse dem EDÖB melden, um sich selber zu entlasten. Die vorgeschlagene Sanktionslösung führt darüber hinaus bei schweizerischen Unternehmen zu Wettbewerbsnachteilen. Die Vollstreckung allfälliger Sanktionen gegenüber ausländischen Unternehmen wäre stark erschwert, weshalb sich diese allenfalls gar nicht an die Regeln halten würden. Des Weiteren verstösst die vorgeschlagene Regelung gegen gewichtige (rechtsstaatliche) strafprozessuale Prinzipien. Betroffen ist primär das Bestimmtheitsgebot. Tangiert ist aufgrund der verschiedenen Informations-, Melde- und Mitwirkungspflichten im VE-DSG jedoch auch der Grundsatz „nemo tenetur“, d.h. das Selbstbelastungsgebot. Die Pflicht, Datenschutzverstösse zu melden, welche ihrerseits strafbedroht ist, führt faktisch zu einer Selbstanzeigepflicht. **Betreffend die Ausgestaltung eines alternativen Sanktionssystems verweisen wir auf den entsprechenden Vorschlag der economiesuisse**. Im Vordergrund stehen Verwaltungsstrafen gegen das Unternehmen und nicht die natürlichen Personen. Anknüpfungspunkt für die Strafbarkeit der Unternehmen wären Organisationsmängel im Unternehmen, d.h. eine mangelhafte Datenschutz-Compliance. Lediglich subsidiär soll eine Strafbarkeit von Mitarbeitern möglich sein, wenn diese absichtlich bzw. mit Vorsatz gegen interne oder gesetzliche Datenschutzregeln verstossen haben. Aus rechtsstaatlichen Überlegungen darf nicht der EDÖB über die Verwaltungssanktionen entscheiden. Die untersuchende bzw. anklagende Behörde soll nicht gleichzeitig die urteilende Behörde sein. Um dieses Problem zu lösen, ist eine neue Entscheidinstanz zu gründen. Das Verhältnis zwischen dieser neuen Behörde und dem EDÖB wäre im DSG zu regeln. Betreffend die Anpassung des Strafkataloges in Art. 50 und 51 VE-DSG wird auf die detaillierten Aufführungen in der Stellungnahme von economiesuisse verwiesen. Schober unterstützt die entsprechenden Vorschläge.

Schober	DSG	52			**Der vorgeschlagene Ausbau der geltenden Regelung (Art. 35 DSG) ist abzulehnen. Die vorgeschlagene Regelung ist weder durch die EU-DSGVO noch den E-SEV 108 erforderlich.** Sofern die Regelung extensiv interpretiert wird, würde die Konzeption des Schweizerischen Datenschutzrechts auf den Kopf gestellt – zumindest betreffend die Bekanntgabe von Daten an Dritte. Bis anhin durften „normale“ Personendaten grundsätzlich ohne einen Rechtfertigungsgrund an Dritte weitergegeben werden – sofern auch die anderen Datenbearbeitungsgrundsätze eingehalten wurden. Nur für besonders schützenswerte Personendaten und Persönlichkeitsprofile wurde vermutet, dass die Bekanntgabe an Dritte ohne Zustimmung der betroffenen Person eine Persönlichkeitsrechtsverletzung darstellt. Art. 52 VE-DSG würde diesen Mechanismus auf den Kopf stellen. Obwohl eigentlich der materielle Teil des Datenschutzgesetzes für die Bekanntgabe von normalen Personendaten an Dritte keinen Rechtfertigungsgrund verlangt, würde eine solche Pflicht zumindest bei der Bekanntgabe von „geheimen“ Personendaten über den Umweg der strafbewehrten Schweigepflicht eingeführt werden. **Hinzu kommt, dass der Begriff der „geheimen Personendaten“ unklar ist.**

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Schober	3 lit. a	Die Ausführungen zum Begriff der Personendaten sind widersprüchlich und sorgen für Rechtsunsicherheit. Einerseits ist keine Änderung an der geltenden Begriffsbestimmung beabsichtigt, andererseits wird jedoch unnötig aus den Erwägungsgründen der EU-DSGVO zitiert, nota bene aus Erwägungsgründen, welche bereits in der EU für Unklarheiten sorgten. Es reicht aus, wenn in den Materialien auf die geltende Praxis und Rechtsprechung verwiesen wird. Zudem soll klargestellt werden, dass für die Bestimmbarkeit die sog. relative Methode relevant ist.

Schober	3 lit. f	Der **Begriff des Profiling** ist nach der vorgeschlagenen Regelung **untauglich und realitätsfremd**. Hier sind Konkretisierungen und Beispiele angezeigt, damit Klarheit herrscht, welche konkreten Tätigkeiten als Profiling zu betrachten sind.
Schober	4 Abs. 6	**Es wird zwar ausgeführt, dass es sich nur um eine terminologische Annäherung an die EU-DSGVO handelt, doch werden die strengen Anforderungen an die Einwilligung in der EU-DSGVO gerade aus dem Wortlaut abgeleitet.** In den Materialien ist klarzustellen, dass gegenüber den Anforderungen an die Einwilligung nach geltendem DSG keine Änderung beabsichtigt wird. Insbesondere werden die strengen Anforderungen aus der EU-DSGVO ausdrücklich nicht übernommen. Es muss auch nach zukünftigem DSG möglich sein, die Einwilligung im Rahmen von AGB einzuholen und zwar nicht separat oder getrennt von anderen Informationen. Auch Stillschweigen muss unter gewissen Umständen als Einwilligung gelten.
Schober	8	Die Materialien müssen klarstellen, dass die Initiative für solche Empfehlungen von den Branchenverbänden ausgehen muss. Der EDÖB soll nicht zum Erlass von Empfehlungen berechtigt sein. Gegen die Genehmigung oder Nicht-Genehmigung von Empfehlungen (durch den EDÖB) muss es sodann Rechtsmittel geben. In den Materialien sind die wichtigsten Voraussetzungen betreffend diese Rechtsmittel zu erläutern (z.B. Legitimation, etc.).
Schober	13	In den Materialien sind die Einzelheiten, insbesondere auch betreffend die Umsetzung der Informationspflicht, genauer festzulegen. Es ist klarzustellen, dass die Information in allgemeiner Form in einer Datenschutzerklärung auf der Webseite erfolgen kann. Dies ist auch durch die E-SEV 108 vorgesehen. In den Materialien ist zudem explizit klarzustellen, dass die Informationspflicht sich auf den Zeitpunkt der Datenbeschaffung beschränkt. Eine Nachinformation ist nicht notwendig. Dies entspricht auch dem vorgeschlagenen Gesetzeswortlaut („spätestens bei der Datenbeschaffung“). Sofern die Informationspflicht bei der indirekten Beschaffung beibehalten wird, ist in den Materialien klarzustellen, wie diese Information erfolgen muss. Damit hier keine unnötigen Umsetzungsschwierigkeiten entstehen und auch im Sinne des risiko-basierten Ansatzes muss es auch hier möglich sein, die Information mittels Datenschutzerklärung auf der Webseite sicherzustellen. Zudem muss den Unternehmen für die Information bei der indirekten Datenbeschaffung mehr Zeit eingeräumt werden. Entgegen dem vorgeschlagenen Wortlaut in der VE-DSG erlauben sowohl die E-SEV-108 als auch die EU-DSGVO bei der Information eine zeitliche Verzögerung.

Schober	15	Hier muss klargestellt werden, dass auch „rechtliche Auswirkungen“ eine gewisse Schwere aufweisen müssen.
Schober	18	Die Ausführungen zu diesen beiden Pflichten sind unklar. In den Materialien ist zu betonen, dass bei der Frage der Umsetzung dieser Pflichten der risikobasierte Ansatz entscheidend ist. Die Datenbearbeiter müssen einen gewissen Spielraum haben und die Anstrengungen auf Datenbearbeitungen mit höherem Risiko fokussieren.
Schober	23 Abs. 3	Die Erwägung im erläuternden Bericht, wonach die Regelung nur zum Tragen komme, wenn die Bearbeitung dieser Daten auch rechtmässig erfolgt (S. 69), ist unzutreffend und in der Botschaft klar zu stellen.
Schober	24 Abs. 2	In den Materialien ist explizit darauf hinzuweisen ist, dass die Bearbeitung von Personendaten zum Zwecke der Direktwerbung ein überwiegendes Interesse darstellen kann.
Schober	50 ff	**Das vorgeschlagene Sanktionssystem wird strikt abgelehnt**. Das vorgeschlagene Sanktionssystem ist in höchstem Masse innovationshemmend und führt zu einem ganz erheblichen Standortnachteil der Schweiz. Gute Mitarbeiter werden nicht mehr bereit sein, Verantwortung in den Unternehmen mitzutragen. Schober schliesst sich der Forderung von economiesuisse nach einem alternativen, datenschutzgerechten Sanktionssystem an.
Schober	Seite 88	**Es ist eine angemessene Übergangsfrist von mindestens zwei Jahren für die Umsetzung aller neuen Pflichten vorzusehen.** Eine Umsetzungsfrist von zwei Jahren entspricht auch der EU-DSGVO. Darüber hinaus ist in den Materialien klarzustellen, dass die neuen Bestimmungen keine Rückwirkung haben. Personendaten, welche vor dem Inkrafttreten der neuen Bestimmungen rechtmässig beschafft wurden, gelten weiterhin als rechtmässig beschafft. War z.B. nach geltendem Recht für eine bestimmte Datenbeschaffung und – bearbeitung keine ausdrückliche Information oder gar eine Zustimmung notwendig, dürfen diese Daten auch zukünftig ohne Nachinformation oder Nacheinwilligung bearbeitet werden, sofern sich an der Bearbeitung dieser Personendaten (z.B. am Bearbeitungszweck) nichts ändert.

scienceINDUSTRIES
SWITZERLAND

Eidgenössiches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

scienceindustries
Wirtschaftsverband Chemie Pharma Biotech

Nordstrasse 15 · Postfach · 8021 Zürich
info@scienceindustries.ch
T +41 44 368 17 11
F +41 44 368 17 70

Zürich, 30. März 2017

Vorentwurf zum Bundesgesetz über den Datenschutz
Stellungnahme von scienceindustries

Sehr geehrte Damen und Herren

Wir beziehen uns auf den erläuternden Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG) sowie die Änderungen weiterer Erlasse zum Datenschutz und danken Ihnen für die Gelegenheit, dazu Stellung nehmen zu können.

scienceindustries ist der Schweizer Wirtschaftsverband Chemie Pharma Biotech. Sie vertritt die wirtschaftspolitischen Interessen von mehr als 250 in der Schweiz tätigen in- und ausländischen Unternehmen aus genannten und verwandten Branchen. Unsere Mitgliedunternehmen, darunter nicht weniger als sechs SMI- und zahlreiche andere kotierte Firmen, beschäftigen in der Schweiz rund 70‘000 Mitarbeitende und leisten einen sehr wesentlichen Beitrag zum Wohlstand unseres Landes: rund 45% aller Schweizer Exporte stammen von ihnen und 40% der gesamten privatwirtschaftlichen Investitionen in Forschung und Entwicklung in der Schweiz werden von unseren Mitgliedfirmen getätigt. Die überwiegende Mehrheit unserer Mitgliedunternehmen sind global tätig, erzielen dabei im Schnitt rund 98% ihrer Umsätze im Ausland und beschäftigen dort zusätzlich über 320‘000 Mitarbeitende. Die vielfältigen Aktivitäten unserer Industrie führen zwangsläufig zu mannigfachen Datenbearbeitungen sowie zu einem regen Datenaustausch im In- wie Ausland resp. auch grenzüberschreitend. Die Thematik ist entsprechend von eminenter Bedeutung für alle unsere Mitgliedfirmen: eine pragmatische Regelung ist dabei genauso anzustreben, wie auch gleichzeitig eine international kompatible Lösung, die einen reibungslosen Datenaustausch in andere Länder garantiert.

Klärend sei an dieser Stelle festgehalten, dass die vorliegende Stellungnahme aus Rücksicht auf die unmittelbare Betroffenheit der Unternehmen sowie die vorhandene Expertise nur auf den Vorentwurf zum Bundesgesetz über den Datenschutz (das DSG) und hierbei ausschliesslich auf jene Regelungen eingeht, welche die Privatwirtschaft direkt betreffen. Zu den übrigen sich in Revision befindlichen Rechtserlassen resp. Bestimmungen werden wir uns nicht äussern.

Äquivalenz als Massstab

Die Mitgliedfirmen von scienceindustries betreiben ein internationales Geschäft und finden sich dabei in einem sehr kompetitiven Umfeld wieder. Entsprechend wichtig ist es, dass die Rahmenbedingungen am Standort, wo die Firmen einen wesentlichen Teil ihrer Wertschöpfung erzielen, ein erfolgreiches Wirtschaften ermöglichen. Das Datenschutzrecht beschlägt zahlreiche Aktivitäten der Firmen und entfaltet somit direkte Auswirkungen auf die Rahmenbedingungen des Wirtschaftsstandortes, wobei das Schweizer Datenschutzkonzept sich bislang über weite Strecken bewährt hat. Im Bewusstsein um die Wichtigkeit des Themas sprechen sich unsere Mitgliedfirmen für einen angemessenen Datenschutz aus und setzen die entsprechenden Vorgaben in ihren Unternehmen um, was bereits heute einen beachtlichen Aufwand verursacht. Entsprechend gilt es Augenmass zu halten und inskünftig keine Regelungen einzuführen, die bei den Firmen zu weiteren grossen Aufwendungen führen, ohne dass gleichzeitig ein berechtigter Nutzen für die schutzbezogenen Personen resultiert. Auch bietet die Totalrevision die Gelegenheit, gewisse Regelungen im bestehenden Datenschutzgesetz, die sich nicht bewährt haben, zu überdenken und anzupassen.

Nach Ansicht von scienceindustries hat sich die Revision des DSG weitgehend auf das Notwendige zu beschränken und sich dabei an der Kompatibilität mit grundlegenden internationalen Vorgaben (insbes. das Übereinkommen SEV 108 sowie die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten) zu orientieren. Die grundsätzliche Äquivalenz des Schweizer Datenschutzniveaus mit diesen Vorgaben ist vor allem mit Blick auf die Fortführung des heute schon bestehenden Angemessenheitsbeschlusses durch die Kommission der Europäischen Union (EU) gerade für den grenzüberschreitenden Datenaustausch von zentraler Bedeutung. Ein revidiertes DSG muss diesen Anforderungen genügen, soll indes aus unserer Sicht nicht darüber hinausgehen und gleichzeitig bestehende Freiräume ausschöpfen.

Zentrale Anliegen der Lifescience-Industrie

- **Der Grundsatz der lex specialis ist umfassend zu verstehen: bereichsspezifische Datenschutzbestimmungen auf Gesetzes- sowie auf Verordnungsstufe müssen auch inskünftig dem DSG stets vorgehen, was insbes. für die Humanforschung von Bedeutung ist.**
- **Die Begriffe genetische wie biometrische Daten sind zu präzisieren sowie der gewählte Ansatz zum Profiling zu überarbeiten.**
- **Die Informations- und Auskunftspflichten müssen überarbeitet werden.**
- **Das Konzept des unabhängigen internen Datenschutzbeauftragten ist beizubehalten und damit verbunden sind Erleichterungen für die Verantwortlichen vorzusehen.**
- **Es sind Verwaltungssanktionen mit unmittelbarer Haftung der fehlbaren Unternehmen vorzusehen.**
- **Das Sanktionssystem ist in wesentlichen Teilen zu verbessern: insbes. ist auf Freiheitsstrafen zu verzichten und die fahrlässige Begehung straffrei zu halten.**

Grundsatz der lex specialis

Dem erläuternden Bericht zur DSG-Revision ist auf Seite 39 zu entnehmen, dass die lex specialis Regel uneingeschränkte Geltung haben soll und damit bereichsspezifische Datenschutznormen dem DSG auch weiterhin vorgehen sollen. Die uneingeschränkte Geltung dieses Grundsatzes ist angesichts der zahlreichen bereichsspezifischen Regelungen im Datenschutz von besonders grosser Bedeutung, weshalb scienceindustries die **ausnahmslose Geltung des Grundsatzes der lex specialis ausdrücklich begrüsst**. Gerade für die Lifescience-Industrie und hier im besonderen Ausmass für jene Unternehmen, die im Bereich der Humanforschung tätig sind, ist es von höchster Bedeutung, dass die bestehenden, spezifischen Datenschutzbestimmungen des Humanforschungsrechts sowie weiterer, unsere Industrie betreffende Rechtsbereiche uneingeschränkte Geltung behalten und ausnahmslos dem DSG vorgehen. Dabei ist zu beachten, dass eine Vielzahl entsprechender Regelungen nicht auf Gesetzesstufe, sondern in Verordnungen geregelt ist. Der **Grundsatz der lex specialis muss also umfassend verstanden** sein und sich nicht nur auf bereichsspezifische Bestimmungen **in anderen Gesetzen als dem DSG beziehen, sondern auch für entsprechendes Verordnungsrecht gelten**.

In diesem Zusammenhang führen die Erläuterungen unter Seite 70 des erläuternden Berichts doch zu einiger Verunsicherung, wenn die Bestimmung von Art. 24 Abs. 2 lit. e Ziff. 1 VE DSG (Rechtfertigungsgrund der Forschung, Planung und Statistik) inskünftig verschärft ausgelegt und deshalb nur noch erschwert angerufen werden kann, dies insbes. auch im Kontext der Datenaufbewahrung (Art. 4 Abs. 4 VE DSG). Diese Aussage gilt es vor dem Hintergrund der lex specialis Regel klar zu relativieren und festzuhalten, dass von dieser einschränkenden Auffassung abweichende, bereichsspezifische Datenschutzbestimmungen auf Gesetzes- wie Verordnungsstufe auch inskünftig dem DSG klar vorgehen werden. Für den Bereich der Humanforschung bedeutet dies konkret, dass auch weiterhin nicht nur die spezifischen Datenschutzbestimmungen des Humanforschungsgesetzes (HFG) sondern auch all dessen Verordnungen (wie z.B. die Humanforschungsverordnung [HVF] und die Verordnung über klinische Versuche [KlinV]) weiterhin uneingeschränkte Gültigkeit haben und auch gegenüber dem revidierten DSG stets vorgehen müssen. Eine entsprechende **explizite Klarstellung muss u.E. mindestens Eingang in die Botschaft an das Parlament** finden, ansonsten in dieser eminent wichtigen Frage eine zu grosse Rechtsunsicherheit geschaffen wird. Wird dieser Weg aus staatsrechtlichen Überlegungen als ungenügend erachtet, so muss eine Lösung gefunden werden, der den umfassenden Vorrang bereichsspezifischer Datenschutzbestimmungen ausnahmslos sicherstellt.

Werden also Daten in Übereinstimmung mit den gesamten spezifischen Vorgaben bearbeitet, so können keine Datenschutzverletzungen resultieren. Gerade am Beispiel des Humanforschungsrechts zeigt sich die sachliche Rechtfertigung zu einem solchen Ansatz, wurden dessen datenschutzspezifischen Bestimmungen insgesamt nach internationalen Grundsätzen ausgestaltet und dabei auf die berechtigten Interessen sowie das Schutzbedürfnis der Patienten gebührend Rücksicht genommen. Der Humanforschungsplatz Schweiz ist darauf angewiesen, dass diese Bestimmungen, die durchaus von gewissen Vorgaben des DSG abweichen, weiterhin uneingeschränkte Geltung haben, ansonsten die Schweiz Gefahr läuft, inskünftig noch weniger Humanforschung betreiben zu können, als sie dies heute aufgrund der administrativen Hürden und der vergleichsweise hohen Kosten schon tut. Selbstverständlich **gelten diese Ausführungen stellvertretend auch für alle anderen bereichsspezifischen Datenschutzbestimmungen**, die in anderen Gesetzen und den dazugehörigen Verordnungen geregelt sind.

Geltungsbereich und Begrifflichkeiten

Während scienceindustries die Streichung des Schutzes **juristischer Personen** begrüsst, so ortet sie einigen Anpassungsbedarf beim Geltungsbereich und den Begrifflichkeiten. Es fällt auf, dass einige Formulierungen im VE DSG nicht konsequent verwendet werden, was es mit Blick auf eine konsistente Rechtsanwendung zu verbessern gilt. Sodann soll nach unserem Verständnis des VE DSG das Datenschutzgesetz inskünftig auch im Rahmen **bereits hängiger Zivilprozesse und laufender Strafverfahren** uneingeschränkt zur Anwendung kommen, was faktisch zu einer Ausweitung des Auskunftsrechts führt. Davon ist abzusehen, denn eine solche Ausweitung des Geltungsbereichs des DSG birgt ein grosses Missbrauchspotential, weil sich damit die zivilprozessualen Editionsregeln umgehen liessen. Auch möchten wir zu einer konsequenteren Verwendung des Begriffes „**Personendaten**" anstelle des Miteinbezugs des Ausdrucks „Daten" anregen, da dies u.E. die Definitionen einzelner Konzepte unnötig ausweitet. Ebenso sind die Pflichten zwischen dem Verantwortlichen und dem Auftragsdatenbearbeiter unklar verteilt resp. ist nicht ersichtlich, nach welcher Logik diese vergeben wurden, was es auch zu verbessern gilt. Desweitern ist für uns nicht nachvollziehbar, warum inskünftig auf die Definition des Begriffs des „**Gesetzes im formellen Sinn**" verzichtet werden soll, wenn dieser im Gesetz weiterhin Verwendung findet; u.E. sollte an der bisherigen Definition festgehalten werden.

Anzupassen sind sodann Art. 3 lit. c Ziff. 3 und 4 VE DSG, welche die **genetischen** sowie die **biometrischen Daten** als besonders schützenswerte Daten festschreiben. Beide Definitionen sind zu präzisieren, indem es heissen muss: *genetische resp. biometrische Daten, die den Zweck haben, eine natürliche Person eindeutig zu identifizieren*. Die im Vorentwurf verwendete Begrifflichkeit ist zu weit gefasst und bedarf zwingend der Präzisierung, ansonsten jegliche genetischen und biometrischen Daten als besonders schützenswert gelten, dies verbunden mit den entsprechenden Erschwernissen im Umgang mit diesen Daten. Sowohl bei genetischen wie auch den biometrischen Daten muss berücksichtigt werden, dass etliche Personendaten nicht mit der Absicht zur eindeutigen Identifikation einer Person erhoben werden und dann in Ermangelung des Bearbeitungszwecks nicht unter den Anwendungsbereich des DSG fallen sollen. Zudem ist zu beachten, dass es keine allgemein zugänglichen Datenbanken über Geninformationen gibt, mittels welcher Personen allein aufgrund einer DNA-Sequenz identifiziert werden könnten. Vielmehr sind solche Datenbanken besonders geschützt, wobei für jene mit Klartext-Identifikationselementen sehr grosse Sicherheitsmassstäbe gelten, was gut und richtig ist. Umgekehrt bedeutet dies aber auch, dass in der Realität im Regelfall eine Person nicht alleine durch eine DNA-Sequenz identifiziert ist.

Ebenso ist der Begriff oder anders ausgedrückt das Konzept des **Profilings**, wie er/es in Art. 3 lit. f VE DSG vorgeschlagen wird, zu verwerfen, da auch diese Definition viel zu weit gefasst ist und im Unterschied zur Datenschutzgrundverordnung der EU (DSGVO) auch manuelle Auswertungen miterfasst sind, wie bspw. eine Mitarbeiterbewertung. Bereits der Begriff des Persönlichkeitsprofils, wie er im aktuell gültigen DSG definiert ist, hat sich in der Praxis nicht bewährt und die Gelegenheit der Totalrevision sollte dahingehend genutzt werden, Abstand von diesem Konzept zu nehmen. Der Datenschutz bezieht sich auf Daten resp. alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Damit ist das Schutzobjekt des DSG umfassend bestimmt und zudem wird präzisiert, welche dieser Angaben als besonders schützenswert gelten. Es macht deshalb keinen Sinn, eine zusätzliche Schutzkategorie hinzuzufügen, die letztlich auf einen Arbeitsprozess - die Auswertung von Daten - abzielt. Denn sollten so gewonnene Arbeitsergebnisse für sich genommen den Begriff der Personendaten wieder erfüllen, so fallen sie ohnehin unter den Anwendungsbereich des DSG. Die Auswertung als Vorgang kann indes u.E. per se materiell den Datenbegriff gar nicht erfüllen. Auch ist der im VE DSG gewählte Ansatz aus Sicht des Schutzgedankens

nicht angezeigt, denn das Profiling wird für das Datensubjekt erst dann relevant, wenn ein Profil verwendet wird und nicht bereits mit dessen Erstellung. Dies gilt es unbedingt im Auge zu behalten.

Insofern würde scienceindustries es begrüssen, wenn sich das DSG in dieser Hinsicht stärker am Ansatz der DSGVO orientiert. In Anlehnung an diese sollte das Profiling nicht mehr als eine zusätzliche Schutzkategorie umschrieben werden. Vielmehr sollte sich dessen Begriffsumschreibung darin erschöpfen, dass unter diesem ein **Verarbeitungsvorgang**, bei welchem es **mittels technischer Hilfsmittel** zu einer **automatisierten, systematischen Verarbeitung von Personendaten** kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen hervorzusagen. Gleichzeitig wäre dann im Gesetz festzuschreiben, welches die spezifischen Pflichten der Verantwortlichen im Zusammenhang mit dem so definierten Profiling sind, wobei keinesfalls über das Schutzniveau der DSGVO hinausgegangen werden darf. Zu denken wäre an wenige Informations- und Auskunftspflichten sowie allenfalls ein Widerspruchsrecht beim Profiling zu Zwecken der Direktwerbung. Klar **Abstand zu nehmen** ist indes vom Konzept, dass **Profiling per se bereits als Persönlichkeitsverletzung** gilt und damit im Ergebnis für jedes Profiling eine ausdrückliche Einwilligung der betroffenen Person vorliegen muss (Art. 23 Abs. 2 lit. d VE DSG). Wenn ein Profiling erfolgt und im Ergebnis Personendaten daraus resultieren, dann stehen diese wiederum unter dem Schutz des DSG, weshalb sich eine zusätzliche Erwähnung des Profilings ohne ausdrückliche Einwilligung als Persönlichkeitsverletzung u.E. als unnötig erweist. Angesichts des damit verbundenen erheblichen Aufwands und der entstehenden Rechtsunsicherheiten auf Seiten der Unternehmen ist dieser Vorschlag abzulehnen.

Wollte man nicht Abstand vom vorgeschlagenen Konzept nehmen, dann wäre immerhin die Definition des Profilings auf mittels technischer Hilfsmittel automatisierte, systematische Entscheidungen zur Analyse und Bewertung von auf eine bestimmte Person bezogene persönliche Merkmale zu reduzieren und zur Verneinung einer Persönlichkeitsverletzung müsste die konkludente Einwilligung genügen.

Grundsätze

Der VE-DSG verschärft den Grundsatz der Erkennbarkeit des Zwecks unnötigerweise mit dem Zusatz der **«klaren» Erkennbarkeit**. Diese Anpassung an die Terminologie des DSGVO ist verfehlt, da die Schweizer Regelung einem unterschiedlichen Grundkonzept folgt (Erkennbarkeit im Rahmen einer klaren Zweckbindung). Die Verschärfung ist auslegungsbedürftig und produziert unnötige Rechtsunsicherheit, weshalb der Zusatz zu streichen ist.

Bezugnehmend auf Art. 4 Abs. 6 VE DSG, wonach eine gültige **Einwilligung eindeutig** zu erfolgen hat, nehmen wir zur Kenntnis, dass mit der Neuformulierung wohl eine terminologische Annäherung an das Übereinkommen SEV 108 und die DSGVO beabsichtigt wurde. Unserer Ansicht nach ist jedoch die Abgrenzung zur im zweiten Satz erwähnten ausdrücklichen Einwilligung im Rahmen des Profilings nicht ersichtlich und wirft lediglich Fragen der Unterscheidung dieser beiden Begriffe auf. Der Zusatz „eindeutig“ sollte daher ersatzlos gestrichen werden.

Auch wenn die **Nachführungspflicht** bereits heute im DSG vorgesehen ist, so ist dennoch festzuhalten, dass diese weit geht und bei den Firmen zu hohen Aufwendungen führt. Es wird zu beachten sein, hier auf Verordnungsstufe die Vorgaben minimal zu halten.

Datentransfer ins Ausland

scienceindustries begrüsst grundsätzlich die gegenüber dem aktuellen Gesetz beibehaltene Regelung zur Datenübertragung ins Ausland, **kritisiert indes die erweiterten Notifikations- und Genehmigungspflichten**. Zustimmend zur Kenntnis nehmen wir die vorgesehene Regelung, Daten ohne Vorliegen eines Angemessenheitsbeschlusses auf Basis von Standardklauseln exportieren zu können, stellen hierzu jedoch die Informationspflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragen (EDÖB) aufgrund des aus unserer Sicht ungünstigen Verhältnisses von Aufwand und Nutzen in Frage. Vielmehr regen wir eine Abkehr im Sinne eines weitgehenden Verzichts auf diese Pflicht – ganz im Sinne der DSGVO (Art. 46) – an.

Der Vorentwurf sieht zudem vor, dass „**verbindliche unternehmensinterne Datenschutzvorschriften**“ (sog. Binding Corporate Rules - BCR) neu einer Genehmigung durch den EDÖB unterstellt sind, was uns inkonsequent erscheint, da BCRs in der Regel dann zum Tragen kommen, wenn nicht mit Standardklauseln operiert werden soll und daher als Subgruppe von spezifischen Garantien nach Art. 5 Abs. 3 lit. b VE DSG aufgefasst werden können, diese jedoch lediglich einer Informationspflicht gegenüber dem EDÖB unterstehen. Desweitern stufen wir die genannte Frist zur Genehmigung von BCRs als nicht praktikabel ein, indem aufgrund der möglichen mehrmonatigen Unklarheit die Unternehmen in ihrer Entscheidungsfreiheit, nichtstandardisierte Datenexportverträge einzugehen, eingeschränkt wären. Die Frist ist deshalb auf das heutige Mass von maximal 30 Tagen zu kürzen und von einer unbeschränkt möglichen Verlängerung abzusehen. Wünschenswert wäre aus Sicht der Rechtssicherheit zudem, dass einmal bewilligte Garantien oder BCRs bis auf weiteres Gültigkeitsstaus erhalten und nicht ohne triftige Gründe widerrufen werden können sowie eine **Beibehaltung des heutigen Art. 6 Abs. 2 lit. g DSG** (Bekanntgabe von Personendaten innerhalb derselben Unternehmung), da diese Regelung zu einer erheblichen Erleichterung des Datenaustauschs innerhalb eines Unternehmens führt.

Hervorheben und kritisch würdigen möchten wir die neue Bestimmung in Art. 6 Abs. 2 VE DSG, wonach **Datenexporte auch in jenen Fällen dem EDÖB gemeldet** werden müssen, die durch Vertragsabschluss, Vertragserfüllung oder ein ausländisches Rechtsverfahren statthaft sind. Eine solche erweiterte Notifikationspflicht würde einerseits zu einer Überflutung an Meldungen an den EDÖB führen, welche dieser kaum innerhalb nützlicher Frist bearbeiten könnte. Andererseits gilt es den damit unerwünscht herbeigeführten Effekt zu beachten, dass Unternehmen gezwungenermassen gegenüber dem EDÖB Geschäftsgeheimnisse offenzulegen hätten, was unserer Ansicht nach zu weit geht. Dies hätte zur Konsequenz, dass etwa Unterlagen aus ausländischen Gerichtsverfahren oder Untersuchungen über das Öffentlichkeitsgesetz publik gemacht werden müssten, was jedoch vielmehr der Unternehmenstätigkeit schaden als den Datenschutz verstärken würde. Aus diesen Überlegungen sprechen wir uns für eine ersatzlose Streichung der genannten Bestimmung aus.

Informations-, Auskunfts- und weitere Pflichten

Informationspflicht

Auch wenn die Informations- und Auskunftspflichten zum Kern des VE DSG gehören und aus Sicht des Datensubjekts von grosser Wichtigkeit sind, so führen sie in der nun vorgeschlagenen Form zu einer verwirrenden Überinformation der betroffenen Personen, die der gewünschten Transparenz letztlich gar zuwiderläuft. Die erweiterten Informationspflichten auf alle Personendaten bringen Mehraufwand und führen auf Grund des öffentlich-rechtlichen Charakters der Bestimmungen sowie den daraus fliessenden Sanktionsfolgen zu Problemen in der Praxis. Entsprechend muss die Regel grundsätzlich im Sinne einer **risikobasierten Transparenzpflicht** überarbeitet werden. In grundsätzlicher Hinsicht wäre u.E. eine einfache, transparente Information der betroffenen Personen allenfalls mit einer freiwillig vorzusehenden Kontaktmöglichkeit zur Ausübung ihrer Rechte nicht nur für die Unternehmen einfacher zu handhaben, sondern auch für die betroffenen Personen transparenter und würde zu deren besseren Schutz führen.

Dem VE DSG ist zum einen nicht zu entnehmen, wie die betroffene Person zu informieren sein wird. Individualisierte Informationspflichten würden mit beachtlichen Mehraufwänden einhergehen und stellten für die Unternehmen einen wesentlichen kostentreibenden Faktor dar. Daher regen wir die Einführung von **„standardisierten" Informationspflichten** an. Dies könnte beispielsweise durch einmalige datenschutzrechtliche Erläuterungen in den Allgemeinen Geschäftsbedingungen (AGB), einer Erklärung auf der Webseite („Privacy Note") oder auch durch das Anbringen von Piktogrammen, die etwa auf eine bestimmte datenschutzrelevante Verarbeitung von Daten hinweisen, erfolgen. Solche standardisierten Informationspflichten sollten durch die Verantwortlichen autonom oder allenfalls im Rahmen der guten Praxis entwickelt werden können.

Zum andern ist für uns nicht ersichtlich, über welche Einzelheiten dann im Detail informiert werden soll. Obwohl in Art. 13 Abs. 2-4 VE DSG einige konkrete Angaben enthalten sind, muss die Information letztlich dennoch alle Aspekte umfassen, die für eine betroffene Person notwendig sind, um ihre Rechte nach DSG geltend zu machen. Der erläuternde Bericht hält auf Seite 57 diesbezüglich fest, dass durch die Beschränkung auf Mindestangaben eine flexible Handhabung der Informationspflicht ermöglicht werden soll, um dadurch ein Übermass an Informationen zu verhindern. Wenngleich sich dies vernünftig liest, so führt u.E. jedoch die strafrechtliche Sanktionierung der Informationspflicht vielmehr dazu, dass Verantwortliche und Auftragsbearbeiter infolge einer Risikominimierung und der Absicherung ihrer eigenen Beurteilung sich gezwungen sehen, deutlich mehr Informationen zu liefern, als an sich gesetzlich vorgesehen wäre. Will man den durchaus begrüssenswerten flexiblen Ansatz beibehalten, so wäre die **Sanktionierung dieser Pflicht zu überdenken und nötigenfalls nur geringfügig auszugestalten**.

Hinsichtlich der Begrifflichkeiten in Art. 13 Abs. 3 VE DSG fällt sodann auf, dass die Ausdrücke „**Dritter**" und „**Empfängerinnen** und **Empfänger**" nicht definiert werden sowie keine Klarheit zur **Abgrenzung der Pflichten** des Verantwortlichen und des Auftragsdatenbearbeiters besteht. U.E. sollte dieser lediglich für Verwirrung stiftende Absatz ersatzlos gestrichen werden. Überdies geht die vorgesehene **Informationspflicht bei der indirekten Datenbeschaffung** zu weit und verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Dem Verantwortlichen werden die relevanten Eckwerte, insbesondere die erstmalige Speicherung, oftmals gar nicht bekannt sein; das Aufwand-Ertragsverhältnis ist damit unverhältnismässig. Darüber hinaus

sind solche direkten Informationspflichten nicht erforderlich: eine allgemeine vorgängige Information des Kunden reicht aus. Die Bestimmung ist deshalb ebenso zu streichen.

Mit Blick auf die entsprechenden Regelungen der EU stellen wir weiter fest, dass insbesondere Art. 13 Abs. 4 VE DSG, wonach der Verantwortliche die **Identität sowie Kontaktdaten der Auftragsbearbeiter und darüber hinaus „die Daten oder Kategorien von Daten"** mitzuteilen hat, weiter als die entsprechenden Bestimmungen in Art. 13 und 14 DSGVO geht. Wir können aus dieser Bestimmung keinen Mehrwert für die betroffenen Personen erkennen, zumal mit diesen zusätzlichen Informationen nicht der Transparenz gedient wird, sondern vielmehr eine dieser zuwider laufende Informationsüberflutung auslösen würde. scienceindustries spricht sich deshalb für eine Streichung von Art. 13 Abs. 4 VE DSG aus.

Die in Art. 14 VE DSG vorgesehenen Ausnahmeregelungen entsprechen weitgehend jenen des heutigen Gesetzestextes, wirken sich u.E. im Ergebnis jedoch enger aus, als dies mit der revidierten Konvention 108 beabsichtigt wurde. Kritisch stehen wir insbesondere Art. 14 Abs. 4 lit. a VE DSG gegenüber, wonach die Berufung auf ein **überwiegendes privates Interesse** nur dann möglich ist, wenn Personendaten nicht an Dritte weitergegeben werden. Unserer Ansicht nach wäre hierbei lediglich zu prüfen, ob das Interesse des Datenbearbeiters dem Interesse an der Information der betroffenen Person vorgeht. Ansonsten führte dies zu einer Ungleichbehandlung von Konzerngesellschaften im Vergleich zu einzelnen, unabhängigen Unternehmen, da sich erstere bei konzerninterner Weitergabe von Daten zum Zweck der Auftragsbearbeitung nicht auf diese Bestimmung berufen könnten. Aus diesem Grund regen wir an, den Zusatz *„…und er die Personendaten Dritten nicht bekannt gibt."* ersatzlos zu streichen.

Die Reichweite der neu eingeführten Informations- und Anhörungspflicht bei **automatisierten Einzelfallentscheiden** ist ebenso zu weitgehend und so nicht akzeptabel. Zwar kennen sowohl die Konvention 108 als auch die DSGVO eine entsprechende Regelung. Der Anwendungsbereich von Art. 15 VE DSG ist jedoch viel breiter: der Entwurf unterscheidet stärker zwischen Profiling sowie automatisieren Einfallentscheiden und sieht auch keine Ausnahmen vor. Dies hat Folgen, welche so wohl nicht beabsichtigt waren: So wären beispielsweise Spam- und Virenscanner, Zugangskontrollen via Badge und sehr viele andere Routineentscheide erfasst, die aus Gründen der Effizienz dem Computer übertragen werden.

So bringt v.a. das vorgesehene **Äusserungsrecht** keinen Mehrwert. Es ist angesichts der neu vorgesehen Informationspflicht auch schlicht unnötig und für die Unternehmen wettbewerbs- und innovationsbehindernd. In der Praxis würde es wohl regelmässig zu einer Begründungspflicht führen und damit die Vertragsfreiheit der Unternehmen über Gebühr einschränken. Eine solche Regelung wäre entsprechend auf schwere Fälle - also solche, die erhebliche Auswirkungen auf die betroffene Person haben - zu begrenzen und der Wortlaut an die entsprechende Bestimmung in der DSGVO anzupassen. Auch dann wären sinnvolle Ausnahmen notwendig, welche zumindest auf dem Verordnungsweg vorzusehen wären. Eine einmalige angemessene Information ohne ausdrückliche Einwilligung erschiene uns dabei als ausreichend.

Im Kontext der Informationspflicht spricht sich scienceindustries zudem für eine Prüfung des Konzepts des **„unabhängigen betriebsinternen Datenschutzbeauftragten"** (Data Protection Officer - DPO) aus, da die Ernennung eines mit umfassenden Kompetenzen und Verantwortungen ausgestatteten DPOs hierbei zu einer begrüssenswerten Entlastung des EDÖB wie auch der Unternehmen führen dürfte (vgl. dazu Ausführungen unter dem entsprechenden Absatz auf Seite 12).

Auskunftsrecht

scienceindustries nimmt die vorgesehene Ausweitung des Auskunftsrechts gemäss Art. 20 VE DSG zur Kenntnis, erachtet jedoch den in Abs. 2 eingefügten Zusatz, wonach eine **transparente Datenbearbeitung gewährleistet** sein soll, als unzweckmässig und in einem gewissen Sinne verfänglich. In extensiver Auslegung kann dieser Zusatz dahingehend verstanden werden, dass sich das Auskunftsrecht nicht auf die Daten an sich zu beschränken hat, sondern damit zusätzlich auch die Datenbearbeitungsprozesse impliziert werden. Dies könnte zur Folge haben, dass der Verantwortliche diese auch offenlegen muss, was jedoch nicht den Absichten der Auskunftspflicht entsprechen würde und darüber hinaus möglicherweise bereits an der technischen Umsetzung scheitern könnte. Aus diesen Gründen regen wir an, auf diesen Zusatz zu verzichten.

Desweitern geht der Vorentwurf auch hier hinsichtlich der **automatisierten Einzelentscheide** einiges weiter als die DSGVO, indem in Abs. 3 ein Verantwortlicher verpflichtet wird, bei jedem Entscheid, den er trifft und welchem die Bearbeitung von Personendaten zugrunde liegt, einer betroffenen Person Rechenschaft darüber abzulegen, wie und warum er zu seinem Entscheid gelangt ist und welche Konsequenzen dies für die betroffene Person zusätzlich zu den Daten hat, die hierzu verwendet wurden. Eine derart umfassend verstandene Auskunftspflicht greift in erheblichem Ausmass in die Freiheiten der Unternehmen ein und führt bei diesen zu einem unverhältnismässigen Aufwand, ohne dass daraus ein erkennbarer Nutzen für die betroffenen Personen ersichtlich ist. Die Auskunftspflicht wäre vielmehr auf das Vorliegen einer (automatisierten) Entscheidung zu beschränken, gleichzeitig kann allenfalls noch über deren Ergebnis informiert werden, **indes nicht über deren Wirkungen**, da diese gar nicht immer erkenn- oder gar abschätzbar sind. So sind übrigens vermehrt auch (automatisierte) Einzelentscheidungen denkbar, die gar nicht primär auf eine besondere (Rechts-)Wirkung ausgerichtet sind, sondern der Untersuchung von allgemeinen Verhaltensweisen dienen, womit verbunden kein Schutzbedürfnis erkennbar ist und damit auch keine Auskunftspflichten angezeigt sind. In diesem Kontext sei angefügt, dass uns Art. 20 Abs. 2 lit. e VE DSG nur dann akzeptabel erscheint, wenn ausschliesslich **Auskunft über das blosse Vorliegen einer automatisierten Einzelentscheidung** erteilt werden muss. Wird jedoch beabsichtigt, zusätzlich die Logik der automatischen Verarbeitung miteinzubeziehen, hätte dies die Offenlegung und Umschreibung einer umfassenden Anzahl an hinterlegten Algorithmen in allgemeinverständliche Erklärungen zur Folge, was bei den Unternehmen ebenso einen unverhältnismässigen Aufwand verursachen würde und daher abzulehnen ist.

Schliesslich nehmen wir zustimmend zur Kenntnis, dass die bisherige Regelung, wonach die Auskunft in Form eines Ausdrucks oder einer Fotokopie zu erteilen ist, gestrichen wurde, indes aber kostenlos sein muss. Hierzu regen wir an, spätestens auf dem Verordnungsweg **Ausnahmen von der Kostenlosigkeit** vorzusehen, wie dies in Art. 12 Abs. 5 lit. a DSGVO vorgesehen ist. Ansonsten würde das Prinzip der Kostenlosigkeit dazu führen, dass die Auskunft selbst bei wiederholten, ungerechtfertigten und extrem aufwändigen Anfragen gratis sein muss, was uns nicht hinnehmbar erscheint.

Meldung von Datenschutzverstössen

Mit Art. 17 Abs. 1 VE DSG ist neu vorgesehen, dass jeder Datenschutzverstoss dem EDÖB „unverzüglich“ gemeldet werden muss, es sei denn, dieser führe „voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person“. scienceindustries stellt sich auf den Standpunkt, dass keine plausiblen Gründe ersichtlich sind, weshalb die Schweizer Regelung über den entsprechenden Art. 33

DSGVO hinausgehen soll. Die DSGVO sieht eine Meldung für den Fall vor, wenn im Rahmen einer Datenbearbeitung festgestellt wird, dass eine **getroffene Sicherheitsmassnahme verletzt** wurde und diese **Verletzung zu einem Verlust der Kontrolle an den Daten** führt (vgl. Art. 33 DSGVO i.V.m. Ziff. 87 und 88 der Präambel). In der Schweiz soll die Meldepflicht hingegen jede Datenbearbeitung erfassen, die gegen das DSG verstösst: bspw. eine zweckentfremdete oder unverhältnismässige Nutzung von Daten oder eine Datenbeschaffung, die in nicht transparenter Weise erfolgt. Die Ausnahme, wann keine Meldung zu erfolgen hat, ist dabei wiederum derart formuliert, dass sie im Falle einer Datenschutzverletzung nicht gegeben sein kann, da gemäss Gesetzestext eine unbefugte Datenbearbeitung stets eine Persönlichkeitsverletzung darstellt. Aufgrund des Dargelegten und den Ausführungen zur Inkonsistenz der Bestimmung mit dem restlichen VE DSG ist dieser Artikel u.E. auf das umschriebene Niveau der DSGVO zu reduzieren. Wir regen auch in diesem Kontext an, das Konzept des unabhängigen betrieblichen Datenschutzbeauftragten zu prüfen. Soweit ein solcher in einem Unternehmen eingesetzt ist und in dieser Funktion festgestellte Datenschutzverstösse dokumentiert, könnten u.E. die Auswirkungen von Art. 17 VE DSG gemildert und damit auch die Belastung des EDÖB reduziert werden.

Weitere Pflichten

scienceindustries erachtet die in Art. 19 lit. a VE DSG erwähnte Dokumentationspflicht als umfassend und zeigt sich besorgt über die Ausführungen auf Seite 65 im erläuternden Bericht, wonach die Datenbearbeiter verpflichtet sind, ebenfalls **Datenschutzverstösse** im Sinne von Art. 17 VE DSG zu dokumentieren. Angesichts des breiten Begriffsverständnisses von Art. 17 VE DSG erscheint uns diese Dokumentation unermesslich und ohne sichtbaren Mehrwert für den Datenschutz. Wir regen deshalb an, die **Dokumentationspflicht im Grundsatz auf das Führen eines Verzeichnisses aller Datenbearbeitungen zu beschränken**, für die der Verantwortliche zuständig ist. Selbstverständlich können Unternehmen freiwillig weiter gehen. Ebenso ist die Einführung einer Ausnahme für Kleinstunternehmen sowie der kleinen und mittleren Unternehmen im Sinne einer Entlastung zu prüfen. Die DSGVO sieht hierzu beispielsweise abweichende Regelungen vor für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen.

Weitaus kritischer beurteilt scienceindustries Art. 19 lit. b VE DSG, wonach im Falle einer Berichtigung, Löschung oder Vernichtung von Daten sowie bei Verletzungen des Datenschutzes der Verantwortliche und Auftragsbearbeiter Dritten, denen sie zuvor die betroffenen Daten zugänglich gemacht haben, diese Berichtigungen etc. mitteilen müssen, soweit dies nicht oder nur mit „unverhältnismässigem“ Aufwand möglich ist. Wiederum ist für uns der Mehrwert dieser Ausweitung des entsprechenden Art. 19 DSGVO nicht ersichtlich. Notwendig wäre unserer Ansicht nach die Einführung einer **Begrenzung auf jene Fälle, in denen die betroffene Person ein schützenswertes Interesse** hat, zumal die vorgesehene Bestimmung nicht vorsieht, dass die Berichtigung, Löschung oder Vernichtung auf einen Vorstoss der betroffenen Person zurückzuführen ist. Aufgrund der mannigfaltigen Gründe einer Berichtigung, Löschung oder Vernichtung von Daten, ohne dass sich dabei eine Nachinformation bisheriger Empfänger der Daten aufdrängt, kann dies zu bizarren Situationen führen. Es ist durchaus denkbar, dass eine Löschung erfolgt, weil der Inhaber die Daten nicht mehr braucht, nicht aber, weil die Daten datenschutzwidrig bearbeitet wurden oder die betroffene Person dies verlangt hat. In solchen Fällen sollte keine Pflicht nach Art. 19 lit. b VE DSG ausgelöst werden, müsste doch sonst jedes Unternehmen, das seine Archive und dergleichen bereinigt, laufend prüfen, wem es die Daten schon einmal mitgeteilt hat und diese Empfänger darüber informieren. Es erscheint uns daher nicht opportun, dass die Nachinformation lediglich wegen dem damit allenfalls verbundenen unverhältnismässigen Aufwand wegfällt. Art. 19 lit. b VE DSG ist dahingehend weiter einzuschränken, indem die Be-

stimmung nur zum Tragen kommt, wenn eine Person die **Nachinformation gestützt auf ein überwiegendes privates Interesse ausdrücklich verlangt**.

Sodann erschliesst sich uns auch in diesem Kontext der **Begriff der „Empfängerinnen und Empfänger"** nicht. Hier ist eine klärende Umschreibung zu fordern, wobei wir den Begriff so verstehen, dass der Auftragsbearbeiter nicht tangiert wird.

Datenschutz-Folgenabschätzung

scienceindustries stuft das im Vorentwurf vorgeschlagene Konzept der Datenschutz-Folgenabschätzung in verschiedener Hinsicht als problematisch ein. So erscheinen uns die Voraussetzungen für die Durchführung einer Abklärung gemäss Art. 16 Abs. 1 VE DSG äusserst tief. Ein „erhöhtes" Risiko dürfte sich in der Praxis rasch abzeichnen, wodurch für beinahe alle Datenbearbeitungen vorab entsprechende Abklärungen durchgeführt werden müssen. Seite 61 des erläuternden Berichts entnehmen wir zudem, dass die Bearbeitung von besonders schützenswerten Personendaten oder ein Profiling bereits ein Indiz für ein erhöhtes Risiko darstellen sollen, wie auch die Übermittlung in Drittstaaten ohne angemessenen Datenschutz. Es ist davon auszugehen, dass aufgrund der Strafandrohungen selbst in Fällen, in denen grundsätzlich kein erhöhtes Risiko besteht, ein entsprechendes Verfahren durchgeführt und eine Meldung an den EDÖB erfolgen wird. Der absehbare Aufwand – sei es für die Unternehmen oder den EDÖB – fiele enorm aus, ohne dass der Datenschutz dadurch gestärkt würde. Deshalb befürworten wir den Ansatz, dass die gesetzliche Pflicht zur Erstellung einer formalen, dokumentierten Abklärung auf das beschränkt wird, was die Interessenswahrung der schutzbezogenen Personen als wirklich nötig erkennen lässt. Daher schlagen wir vor, diesbezüglich an Art. 36 DSGVO anzulehnen, der **entsprechende Abklärungen erst bei Vorliegen eines „hohen" Risikos für eine Persönlichkeitsverletzung vorsieht**.

Sodann ist der Begriff der „Voraussehbarkeit" u.E. in der Schweizer Rechtspraxis nicht etabliert. Es bietet sich vielmehr an, den **Begriff der „überwiegenden Wahrscheinlichkeit"** zu verwenden, welcher im Sozialversicherungsrecht gebräuchlich ist und dort eine langjährige Konkretisierung erfahren hat. Gemäss diesem Beweisgrad genügt bundesgerichtlicher Rechtsprechung nach die blosse Möglichkeit eines bestimmten Sachverhaltes nicht; vielmehr ist im konkreten Fall jener Sachverhaltsdarstellung zu folgen, die von allen möglichen Geschehensabläufen als die wahrscheinlichste zu würdigen ist (vgl. BGE 126 V 360). Mit Blick auf die mit einer Datenschutz-Folgenabschätzung zu erwartenden erheblichen Aufwände besteht ein Interesse an einer rechtssicheren Formulierung, die möglichst Klarheit schafft ohne den Schutzgedanken zu unterwandern. Was hierbei für das Sozialversicherungsrecht genügt, darf auch für den Datenschutz als angemessen erachtet werden.

Desweitern bewerten wir die **Meldepflicht gegenüber dem EDÖB und die ihm eingeräumte Frist zur Bearbeitung praxisfern** und sind der Meinung, dass die Datenbearbeiter dadurch in ihrer Arbeit massiv behindert würden. Einige der Unternehmen aus unserer Industrie führen jährlich weit über hundert Datenschutz-Folgenabschätzungen durch, wobei eine konsequente Prüfung durch den EDÖB wohl zur Folge haben würde, dass für jedes dieser Unternehmen nur für diese Prüfungen eine eigene Person abgestellt werden müsste, was weder sinnvoll erscheint, noch möglich ist. Auch die DSGVO geht in Art. 35 weniger weit: sie verlangt eine Konsultation der Aufsichtsbehörde nur dann, wenn der Verantwortliche zum Schluss kommt, dass trotz der von ihm **ergriffenen Schutzmassnahmen ein hohes Risiko der Verletzung der Persönlichkeit**

der betroffenen Personen verbleibt. Zudem erscheint uns die dem EDÖB gewährte Frist zur Beurteilung viel zu lange: in der EU (Art. 36 Abs. 2 DSGVO) muss eine Behörde innert acht Wochen handeln, falls sie sich gegen eine Bearbeitung ausspricht; die Frist kann überdies nur in komplexen Fällen um sechs Wochen verlängert werden. In der Schweiz soll der EDÖB standardmässig drei Monate Zeit haben, mit der Möglichkeit, durch das Einfordern weiterer Information die Frist jedes Mal von neuem beginnen zu lassen. Zudem sollte klar geregelt werden, welche Informationen dem EDÖB weitergeleitet werden müssen und wie diese insbesondere bei Informationszugangsgesuchen nach dem Öffentlichkeitsgesetz (BGÖ) geschützt werden können. Datenschutz-Folgenabschätzungen von Unternehmen werden aber oftmals Geschäftsgeheimnisse enthalten, weshalb eine Einsichtnahme durch Mitbewerber vermieden werden muss.

Zusammenfassend regt scienceindustries aufgrund obiger Ausführungen an, einerseits die Begriffe des erhöhten Risikos sowie der Voraussehbarkeit im vorgeschlagenen Sinn anzupassen und den zeitlichen Rahmen zur Beurteilung der Massnahmen enger zu setzen. Desweitern soll auch die Datenschutz-Folgenabschätzung mit dem Konzept des „unabhängigen internen Datenschutzbeauftragten“ verknüpft werden (vgl. dazu Ausführungen unter dem nachfolgenden Absatz).

Konzept des unabhängigen internen Datenschutzbeauftragten

scienceindustries bedauert es, dass im VE DSG das Konzept des unabhängigen internen Datenschutzbeauftragten (Data Protection Officer - DPO) keinerlei Niederschlag gefunden hat. Wir erkennen darin nicht zuletzt im Vergleich mit der DSGVO einen Mangel, den es zu beheben gilt. Denn das Konzept des DPO scheint den Bedürfnissen der Wirtschaft zu entsprechen, wie ein Blick in die entsprechende Liste des EDÖB deutlich aufzeigt. So ist im revidierten Gesetz in Analogie zur bisherigen Regelung von Art. 11a DSG am **„Institut“ des DPO festzuhalten**, wobei die Unternehmen auch weiterhin **frei in der Entscheidung sein** sollen, einen solchen einzusetzen oder nicht. Die Voraussetzungen an die Stellung sowie die Aufgaben des DPO können in Anlehnung an die heute dazu bestehende Praxis zu den Art. 11a Abs. 5 lit. e DSG sowie Art. 12a und Art. 12b DSG weiterhin auf Verordnungsebene geregelt werden, wobei gleichzeitig die Äquivalenz mit den Art. 37 ff. DSGVO im Auge zu behalten wäre. Angesichts der Tatsache, dass der DPO im VE DSG gar nicht mehr vorgesehen ist, geht man seitens des Bundes offenbar von erheblichem Handlungsspielraum aus, was wir zwar ebenso einschätzen, indes vor dem Hintergrund der Äquivalenz mit den europäischen Vorgaben nicht gar soweit gehen würden, dieses Konzept überhaupt nicht mehr vorzusehen. Entscheidet sich ein Unternehmen, einen DPO einzusetzen, wäre sodann eine damit verbundene **Meldepflicht an den EDÖB** vorzusehen, der analog zur heutigen Regelung ein öffentlich einsehbares Register dieser Firmen führt. Damit ist transparent, welche Firmen von diesem Konzept Gebrauch machen, was mit Blick auf die nachfolgenden Ausführungen von Bedeutung ist.

Neben der Möglichkeit zur freiwilligen Bezeichnung eines DPO sind alsdann die im Zusammenhang mit dieser Bezeichnung verbundenen Rechtswirkungen im DSG aufzuführen. So sollten insbes. diverse **Informations- und Meldepflichten wegfallen** oder aber **mindestens gelockert** werden – soweit sie überhaupt beibehalten werden. Kommt ein DPO beispielsweise im Rahmen einer betriebsinternen Datenschutz-Folgenabschätzung zum Schluss, dass keine wesentlichen Risiken mit Blick auf den Datenschutz gegeben und entsprechend keine nennenswerten Massnahmen angezeigt sind, so können sämtliche damit zusammenhängende Meldungen an den EDÖB unterbleiben. Eine solche wäre nur dann angezeigt, wenn der DPO einerseits hohe Risiken für den Datenschutz der betroffenen Personen erkennt und anderseits deshalb

Massnahmen zur Eindämmung resp. Behebung der erkannten Risiken vorschlägt. Mit dieser Lösung wäre eine breite Abdeckung von Datenschutz-Folgenabschätzungen in den Unternehmen zu erreichen und gleichzeitig würde der EDÖB nur dann in den Prozess involviert, wenn eine Risikosituation sich manifestiert. Dies erscheint uns ein sachgerechter Ansatz, der einen effizienten Umgang mit den knappen Ressourcen auf beiden Seiten sicherstellt und gleichzeitig das Schutzniveau hoch hält. Ebenso wäre in diesem Zusammenhang eine Reduktion allfälliger Meldepflichten im Zusammenhang mit dem Datentransfer ins Ausland vorzusehen.

In diesem Kontext sei angefügt, dass scienceindustries den **Verzicht auf die Anmeldung von Datensammlungen durch private Personen begrüsst**. Ein DPO könnte auch hierbei eine wesentliche Aufgabe erfüllen, indem diese Person gestützt auf ihr Fachwissen, die Kenntnisse über das Unternehmen und seine Geschäftstätigkeiten sowie deren unabhängige Stellung am besten geeignet ist, betriebsinterne Standards für die Etablierung der notwendigen Prozesse auszuarbeiten und dabei den Datenschutz betriebsintern auf hohem Schutzniveau durchzusetzen. Verbunden mit der unsererseits geforderten Lockerung hinsichtlich der Melde- und Informationspflichten sowie ggf. weiterer Pflichten, wäre damit ein erheblicher Anreiz zur Schaffung einer solchen Stelle gegeben, was zum einen wiederum den betriebsinternen Massnahmen zur Sicherstellung des Datenschutzes und zum andern einer Entlastung des EDÖB dienen würde. Entscheidet sich hingegen ein Unternehmen, keinen DPO einzusetzen, so könnte es im Gegenzug von den damit zusammenhängenden Rechtswirkungen nicht profitieren und sähe sich schneller mit Melde- und Informationspflichten konfrontiert. Aus diesem Grund sind wir der Ansicht, dass die mit der Bezeichnung und Bekanntgabe eines DPO verbundenen Rechtswirkungen bis zu einem gewissen Grad positivrechtlich im DSG vorzusehen sind, um diesbezügliche Klarheit und im Ergebnis Rechtssicherheit zu schaffen.

An dieser Stelle wollen wir gleichzeitig festgehalten wissen, dass das unsererseits geforderte Konzept des unabhängigen internen Datenschutzbeauftragten **nicht** dazu führen soll, dass diese **Personen eine erhöhte strafrechtliche Verantwortung** trifft. Vielmehr schlagen wir dazu einen anderen Ansatz als der im Entwurf gewählte vor und verweisen aber hier auf die nachfolgenden Ausführungen zum Sanktionssystem.

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

scienceindustries spricht sich im Grundsatz positiv zum Konzept des Datenschutzes durch Technik und datenschutzfreundlichen Voreinstellungen (Art. 18 VE DSG) aus, auch wenn wir der Ansicht sind, dass sich die Bestimmungen bereits aus einer korrekten Anwendung des Bearbeitungsgrundsatzes gemäss Art. 11 VE DSG ergeben, wonach im Rahmen einer Datenbearbeitung jeweils angemessene technische und organisatorische Massnahmen zu treffen sind, um eine unbefugte Datenbearbeitung zu verhindern. Unter Berücksichtigung der entsprechenden DSGVO-Vorgaben stellen wir jedoch fest, dass die vorgeschlagene Formulierung gemäss VE DSG im Vergleich zu Art. 32 DSGVO deutlich zu restriktiv ausfällt. Insbesondere sollte berücksichtigt werden, dass die in Art. 18 Abs. 1 und 2 VE DSG vorgesehene Verpflichtung einen einklagbaren Anspruch einzelner Personen auf die Einführung solcher Massnahmen nach sich ziehen kann, was u.E. nicht die Absicht der europäischen Regelwerke war und eindeutig zu weit geht. Vielmehr sollte sich das **Schweizer Datenschutzgesetz an der entsprechenden DSGVO-Formulierung ausrichten**, in dem Sinne, dass *„Der Verantwortliche und der Auftragsbearbeiter geeignete (oder angemessene) technische und organisatorischen Massnahmen trifft/treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen“*.

Dabei handelt es sich zwar um im Gesetz festgelegte Ziele, die es anzustreben gilt, indes können diese **nicht zu einklagbaren Ansprüchen einzelner Personen** führen. Diese Differenzierung ist wesentlich, um einer möglichen diesbezüglichen Klageflut entgegen zu wirken. Denn es ist zu vermeiden, dass in gewissen Kontexten realisierbare Standards auf dem Klageweg auf Branchen übertragen werden, in welchen diese keinen Sinn machen oder aus technischen Gründen noch nicht im gleichen Ausmass etabliert sind. U.E. würde sich auch eine entsprechende **Klärung in der Botschaft an das Parlament** aufdrängen.

Keine spezifischen Regelungen für verstorbene Personen

scienceindustries spricht sich aus mehreren Gründen **gegen die Einführung von spezifischen Regelungen für verstorbene Personen** aus. Vorweg möchten wir auf den in Art. 31 Abs. 1 ZGB verankerten Grundsatz hinweisen, wonach die Persönlichkeit mit dem Tod endet und eine verstorbene Person folglich auch keinen Datenschutz erlangen kann. Allenfalls kommt dieser für Personen im Umfeld der verstorbenen Person, die durch die Bearbeitung derer Daten ebenfalls betroffen sind, zum Tragen. Aus Sicht der Unternehmen sind die vorgesehenen Regelungen insofern problematisch, als sie aufgrund ihrer generell abstrakten Natur unzählige weitere, grundsätzlich mit der Bestimmung nicht beabsichtigte Anwendungsfälle miteinbeziehen und daher unvorhergesehene Nebenwirkungen entfalten können. In diesem Zusammenhang gilt es auch die Übertragung von Persönlichkeitsrechten auf Dritte zu berücksichtigen. Würde beispielsweise ein einzelner Erbe die Löschung von Daten beantragen, könnte sich das betroffene Unternehmen lediglich auf überwiegende Interessen von Dritten oder der verstorbenen Person selbst berufen, jedoch nicht auf eigene überwiegende Interessen oder gesetzliche Pflichten, wie z.B. die Aufbewahrungspflicht gemäss Art. 12 Abs. 4 VE DSG. Daraus lässt sich schlussfolgern, dass der Erbe wesentlich mehr Rechte gegenüber einem Datenbearbeiter hat als der Erblasser zu Lebzeiten, was kaum die Absicht hinter Art. 12 VE DSG sein dürfte. Die Tatsache, dass weder in der Konvention 108 noch in der DSGVO spezifische Regelungen für verstorbene Personen aufgenommen wurden, lässt uns auch an der Relevanz einer spezifischen Regelung hinsichtlich der Fortführung der Angemessenheitserklärung durch die EU zweifeln. Angesichts des oben ausgeführten fehlenden datenschutzrechtlichen Nutzens und verbunden mit den einhergehenden Rechtsunsicherheiten muss **Art. 12 VE DSG u.E. unbedingt ersatzlos gestrichen werden**. Solche Sachverhalte sollen hinreichend im Zivilrecht geklärt werden und allfällige Lücken wären entweder über dieses oder durch vertragliche Lösungen zu schliessen.

Verwaltungssanktionen mit unmittelbarer Haftung der fehlbaren Unternehmen

scienceindustries lehnt den Vorschlag des VE DSG, das Sanktionssystem über das ordentliche Strafrecht auszugestalten, entschieden ab, denn dies führte im Ergebnis zu einer Vielzahl unerwünschter Folgen. So zeitigte ein solches Konzept die primäre strafrechtliche Verantwortlichkeit der natürlichen Personen für die Verletzung sanktionierter Tatbestände und nur subsidiär könnte auf die Unternehmen durchgegriffen werden, wobei uns gerade in dieser Hinsicht Art. 53 VE DSG als untauglich erscheint. Angesichts der vorgesehenen, beachtlichen Strafdrohungen ist eine primäre strafrechtliche Verantwortung der natürlichen Personen – sprich der Mitarbeiter von Unternehmungen – nicht nur unverhältnismässig, sondern birgt auch die Gefahr, dass es unternehmensintern zu einer erhöhten gegenseitigen Anzeigeaktivität durch Mitarbeitende kommt. Dies dürfte auch kaum mehr durch interne Vorgaben des Unternehmens in Bahnen gelenkt werden können, weil jeweils ein persönliches Schicksal einer Person mit diesen Fragestellungen verbunden ist, was bekanntlich – und bis zu einem gewissen Grade auch nachvollziehbar – unberechenbare Kräfte auslöst. Mit Blick auf die vielfältigen Aktivitäten, die angesichts der verschärften Datenschutzanforderungen im Tagesgeschäft von Unternehmen zu ungewollten Datenschutzverletzungen führen können, bestünde eine eminente Gefahr, dass ein sehr weiter Kreis von Mitarbeitern laufend zur strafrechtlichen Verantwortung gezogen würde. Entsprechend sähen sich die Unternehmen im Falle von Verurteilungen der betroffenen Personen nur schon aus Gründen ihrer eigenen Compliance gezwungen, das Arbeitsverhältnis mit solchen Mitarbeitern aufzulösen, währenddem diese auf dem Arbeitsmarkt aufgrund möglicher Strafregistereinträge eine deutlich reduzierte Wiedereinstellungschance zu gewärtigen hätten. So dürfte es sich dann auch alsbald als äusserst schwierig erweisen, überhaupt noch Mitarbeiter für solche Positionen rekrutieren zu können, mit dem Ergebnis, dass das unsererseits geforderte **Konzept des unabhängigen internen Datenschutzbeauftragen faktisch nicht mehr greifen würde.** In der Konsequenz wäre gerade der Durchsetzung des Datenschutzes damit nicht gedient, währendem dieser eine zusehends lähmende Wirkung auf das Geschäftsleben entfaltet und zu einem vergifteten Betriebsklima führt. Überdies müssten sich 26 kantonale Strafuntersuchungsbehörden und Jurisdiktionen mit dem strafrechtlichen Vollzug der Datenschutzbestimmungen befassen, was angesichts der oft schwierig lokalisierbaren Datenschutzverletzungen nicht nur zu stetigen Zuständigkeitsfragen, sondern auch zu unterschiedlichen Rechtsauslegungen und entsprechender inkonsistenter Rechtsanwendung führen dürfte.

Aufgrund dieser Analyse **spricht** sich **scienceindustries** für ein System mittels **Verwaltungssanktionen verbunden mit einer primären Verantwortlichkeit** der gegebenenfalls **fehlbaren Unternehmen aus**. Denn die Datenbearbeitung findet in aller Regel in Verrichtung geschäftlicher Aktivitäten statt und generiert letztlich in diesem Kontext einen Vorteil für das Unternehmen, weshalb dieses auch in der Verantwortung stehen soll. Verwaltungssanktionssysteme existieren in der Schweiz bereits heute und man kann auf den gemachten Erfahrungen aufbauen, wobei zu beachten wäre, dass der Bereich des Datenschutzes nicht unbesehen vergleichbar mit anderen Rechtsgebieten ist, in welchen dieser Ansatz bereits gilt (insbes. Kartellrecht) und entsprechend differenzierte Vorgaben und Regelungen angezeigt wären. Wie bereits erwähnt, besteht bei den vielfältigen Aktivitäten von Unternehmungen ein erhöhtes Risiko, ungewollt gegen die verschärften Datenschutzanforderungen zu verstossen, wobei festzustellen ist, dass solche Verstösse in aller Regel nicht zu nennenswerten finanziellen Vorteilen der Unternehmen führen. Im Bereich des Datenschutzes hätte sich das Verwaltungssanktionssystem deshalb nicht an der Massgabe der Abschöpfung von unrechtmässig erworbenen Gewinnen zu orientieren, sondern an jener der Durchsetzung einer effizienten Umsetzung der datenschutzrechtlichen Vorgaben. Deshalb sind wir der Ansicht, dass der Strafrahmen auch bei der Einführung von Verwaltungssanktionen bei der vorgeschlagenen **Höchstbussengrenze von einer halben Million**

CHF begrenzt bleiben muss und dieser nicht nach oben geöffnet werden soll. Vielmehr soll der Sanktionsrahmen nach dem Grundsatz des **Auswirkungsprinzips** ausgestaltet sein, wobei je nach Schwere der vorsätzlich begangenen Datenschutzverletzung in örtlicher wie sachlicher Hinsicht die Strafe höher oder tiefer festzusetzen wäre, begrenzt eben bei der Höchststrafe von CHF 500‘000.-. Eine entsprechende Differenzierung erscheint uns sachgerecht, fällt denn ein Sachverhalt mit lokaler oder regionaler Auswirkung weniger ins Gewicht, als einer mit internationaler Betroffenheit. Dasselbe gilt u.E. wenn beispielsweise eine einfache Informationspflichtverletzung gegenüber einer Einzelperson ins Verhältnis gesetzt wird mit mehrfacher Widerhandlungen gegen das DSG, welche eine Vielzahl von Personen betreffen würde.

Ebenso wäre die Gelegenheit zu nutzen, die seit Jahren im Raum stehende Kritik des ungenügenden Rechtsschutzes der Parteien im Rahmen des verwaltungsstrafrechtlichen Untersuchungsverfahrens zu beherzen und sich stärker an den Grundsätzen der Europäischen Menschenrechtskonvention (EMRK) zu orientieren. Es sollte neu vorgesehen werden, im **gesamten Verwaltungsstrafverfahren dem Grundsatz des „nemo tenetur“ ungeschmälerte Geltung durch gesetzgeberische Auflagen** zu verschaffen, so dass die Parteien sich nach Eröffnung des Verfahrens nicht mehr selber belasten müssen. Möglicherweise könnte Art. 113 der eidgenössischen Strafprozessordnung (StPO) für dieses Untersuchungsverfahren für anwendbar erklärt oder eine analoge Bestimmung im entsprechenden Gesetz vorgesehen werden. Schliesslich wäre ein **System von Rechtfertigungsgründen** oder aber **mindestens Strafmilderungs- resp. Strafminderungsgründen** vorzusehen, welche die Unternehmungen im Verwaltungsstrafverfahren vorbringen können. Zu denken wäre insbes. an vorsätzlich begangene Datenschutzverletzungen durch Mitarbeitende, wie z.B. Datendiebstahl. In diesen Ausnahmefällen könnte scienceindustries auch eine zusätzliche, unmittelbare strafrechtliche Verantwortlichkeit der fehlbaren natürlichen Personen akzeptieren, falls dies dann eben zu einer Reduktion des Strafmasses beim Unternehmen führt. Auch sollte das kooperative Verhalten der Unternehmungen im Rahmen der Untersuchung, das möglicherweise bis hin zu freiwillig selbstbelastenden Aussagen gehen kann, ebenso als klar strafmildernder Grund vorgesehen werden. Schliesslich wären auf technischen Fehlleistungen basierende Datenschutzverletzungen mit geringfügigen Auswirkungen auf den Datenschutz strafmildernd auszugestalten.

Sanktionenkatalog und Strafmass

Nach Ansicht von scienceindustries ist nicht nur das **strafrechtliche Bestimmtheitsgebot** in vielen vorgeschlagenen Strafbestimmungen oft **fraglich**, sondern der **Sanktionskatalog tendenziell überladen** und deshalb ist eine **Reduktion der Straftatbestände** zu prüfen. Im Umfang, wie wir uns in dieser Stellungnahme für eine Reduktion der Rechte der Datenschutzsubjekte und der Pflichten der Verantwortlichen aussprechen, führt dies entsprechend auch zur Aufhebung der damit verbundenen Sanktionierungen, denn wo keine Rechte verbrieft resp. keine Pflichten bestehen, können solche auch nicht verletzt werden und entsprechend keine Sanktionen greifen. Insbesondere sei an dieser Stelle wiederholt, dass die Strafbarkeit der Verletzung von Informationspflichten generell zu überdenken ist oder aber mindestens hierbei nur geringfügige Sanktionen festzulegen wären. Zudem halten wir fest, dass mit Blick auf die Fortführung eines mit Europa äquivalenten Datenschutzniveaus nach unserer Einschätzung gerade in diesem Bereich eine Orientierung am Übereinkommen SEV 108 des Europarates als genügend zu erachten ist.

Ersatzlos zu streichen ist sodann Art. 52 VE DSG, sind denn die angedrohten Freiheitsstrafen von bis zu drei Jahren zum einen absolut unverhältnismässig und diese Straftatbestände zum andern mit Blick auf ein

äquivalentes Datenschutzniveau mit Europa u.E. nicht erforderlich. **Generell ist von Freiheitsstrafen Abstand zu nehmen** und gänzlich auf deren Einführung zu verzichten, wurden denn auch keine solchen in den europäischen Regelwerken vorgesehen, welche ja allesamt wirksame und abschreckende, indes eben auch verhältnismässige Sanktionen verlangen. Offenbar wurde sowohl im Europarat als auch in den Institutionen der EU keine Notwendigkeit zur Einführung derart drastischer Sanktionen erkannt, was sachgerecht ist. Vielmehr erscheint die Strafandrohung von Freiheitsstrafe mit Blick auf den begangenen Rechtsbruch als unverhältnismässig kriminalisierend. Eine derart strenge Straffolge lähmte den Geschäftsverkehr übermässig und stellte einen beachtlichen Standortnachteil für die Schweiz dar.

scienceindustries **lehnt** des weitern jegliche **Strafbarkeit** für **fahrlässige Begehung** von Datenschutzverletzungen entschieden **ab**. Es sei erneut wiederholt, dass bei den vielfältigen Aktivitäten von Unternehmungen ein erhöhtes Risiko, ungewollt gegen die verschärften Datenschutzanforderungen zu verstossen, besteht. Diesem Umstand ist gebührend Rechnung zu tragen, dies nicht zuletzt auch in Anerkennung, dass die Unternehmen dem Schutz von Personendaten ohnehin einen hohen Stellenwert einräumen. Auch wenn heute schon grosse Anstrengungen zur Einhaltung der datenschutzrechtlichen Vorgaben getätigt werden, sind angesichts der zahlreichen Verarbeitungsaktivitäten sowie mit Blick auf die oft komplexen Prozesse unbeabsichtigte Datenschutzverletzungen auch bei Einhaltung hoher Standards in grossen wie in kleinen Unternehmen nicht immer zu vermeiden. Darin kann indes kein kriminelles Verhalten erkannt werden, weshalb die **Strafbarkeit von Datenschutzverstössen ausschliesslich auf deren vorsätzliche Begehung zu begrenzen** ist. Ein auf Vorsatz beschränkter Strafrahmen erscheint auch angesichts der typischerweise schwierigen sowie sehr aufwendigen Bewertungs- und Meldevorgängen bei der Aufklärung als auch Behebung von fahrlässigen Rechtsverstössen als angemessen und entsprechend geboten.

Stellung und Kompetenzen des Eidgenössischen Datenschutzbeauftragten

Vor dem Hintergrund der vorangegangen Ausführungen und in Anerkennung der internationalen Vorgaben, die neu im Bereich des Datenschutzes eine mit beachtlichen Kompetenzen ausgestattete (nationale) Aufsichtsbehörde fordern, schlägt scienceindustries ein vom VE DSG abweichendes Modell vor. Der **EDÖB** mit seiner beratenden, empfehlenden und letztlich anzeigenden Funktion hat sich im Grundsatz bewährt und wir würden es begrüssen, wenn an diesem **System unverändert festgehalten** wird. Nur schon mit Blick auf seine Bezeichnung als „Beauftragter“ und seine organisatorische Einordnung bei der Bundeskanzlei, die von Bundesverfassung (BV) wegen als Stabsstelle des Bundesrates agiert (Art. 179 BV), drängt sich eine Beibehaltung des Systems auf. Im Übrigen wäre es auch fraglich, ob eine mit Verfügungsgewalt ausgestaltete Behörde von Verfassung wegen überhaupt der Bundeskanzlei angehören darf, sind doch die Exekutivgewalten in aller Regel den Departementen zugeordnet. Zudem orten wir Interessenskonflikte, wenn der mit umfassenden beratenden Funktionen ausgestattete Beauftragte des Bundes gleichzeitig auch Untersuchungsaufgaben - bis hin zur Kompetenz zur unangekündigten Hausdurchsuchung - erhält sowie weitere vorsorgliche Massnahmen verfügen kann. Abgesehen von solchen Konflikten führte dieser Umstand auch nicht zur notwendigen Vertrauensbasis, auf welcher beispielsweise das Konzept der guten Praxis wirksam greifen kann.

Wir regen deshalb an, dass der **EDÖB** unverändert als eine **bundesbeauftragte Stelle ohne Verfügungskompetenzen erhalten** bleibt und weiterhin alle im Zusammenhang mit der Umsetzung des DSG bestehenden Beratungs- und Empfehlungstätigkeiten wahrnimmt. So soll er auch inskünftig sowohl private Personen

wie auch Unternehmen in allen Belangen des Datenschutzes beraten, das Verzeichnis der Länder mit vergleichbarem Datenschutzniveau sowie das Verzeichnis der Firmen führen, die auf freiwilliger Basis einen internen unabhängigen Datenschutzbeauftragten gemeldet haben (vgl. Ausführungen auf Seite 12). Er würde im Rahmen der guten Praxis Empfehlungen ausarbeiten, wobei alleine schon aufgrund seiner Stellung nicht zu befürchten wäre, dass dabei eine „Schattengesetzgebung" entstünde, was mit Blick auf die Rechtssicherheit zentral ist. An ihn wären die meldepflichtigen Datenschutz-Folgenabschätzungen sowie weitere gesetzliche Meldepflichten zu richten und ebenso die meldepflichtigen Datenschutzverletzungen anzuzeigen. Zudem würde es in seiner Kompetenz liegen, Datenschutzverletzungen, von denen er Kenntnis erhalten hat, nach seinem Ermessen an eine **neu zu schaffende Bundesspruchbehörde** zu melden, die dann ihrerseits das Verwaltungsverfahren eröffnet, durchführt und allenfalls Verwaltungssanktionen ausspricht.

Entsprechend wäre somit eine **neue Bundesspruchbehörde** zu schaffen, die in einem Departement anzusiedeln wäre (wobei sich u.E. wohl das Eidgenössische Justiz- und Polizeidepartement [EJPD] als am geeignetsten erwiese) und die mit allen notwendigen Verfügungskompetenzen zur Durchführung eines Verwaltungsstrafverfahrens bis mit zur Verhängung von Verwaltungssanktionen auszustatten wäre. Damit würde die Schweiz die internationalen Vorgaben einer bestehenden **Aufsichtsbehörde mit Verfügungskompetenzen** samt jener zur **Verhängung von Verwaltungssanktionen** erfüllen, ohne dass sie das bewährte Institut des EDÖB aufgeben und diesen zudem mit Aufgaben und Kompetenzen ausstatten müsste, die zum einen zu Interessenkonflikten führen dürften und zum andern auch unter dem Aspekt der Gewaltenteilung fragwürdig sind. Zudem bestünde die Chance, eine zentrale Behörde zu etablieren, welche eine einheitliche Rechtsauslegung und -anwendung im Bereich der Sanktionierung gewährleisten könnte – dies im Unterschied zum im VE DSG vorgeschlagenen Ansatz über das ordentliche Strafrecht mit 26 kantonalen Vollzugsorganen. Sie wäre letztlich auch in der Lage, auf Datenschutz spezialisiertes und damit notwendigerweise versiertes Personal zu verpflichten, wie dies auf kantonaler Ebene unmöglich der Fall sein könnte. Dass damit beim Bund zusätzliche Kosten anfallen würden, ist nicht von der Hand zu weisen, doch muss dem auch entgegen gehalten werden, dass die zusätzliche Belastung der kantonalen Strafverfolgungsbehörden sowie deren Justiz vermutlich infolge der geringeren Professionalität volkswirtschaftlich betrachtet gar zu höheren Kosten führen dürfte. Wie bereits erwähnt, sprich sich scienceindustries auch dafür aus, gleichzeitig die Chance zu nutzen und **konkrete Verfahrensvorgaben zu machen, welche die Rechte der Verantwortlichen im Verwaltungsstrafverfahren in adäquater Weise garantieren**. Insbesondere wäre dabei an den Grundsatz des „nemo tenetur" zu denken und festzuschreiben, dass sich Verantwortliche auch dann im Verfahren nicht weiter selber belasten müssen, wenn sie vorgängig ihrer Pflicht zur Meldung der Datenschutzverletzung nachgekommen sind.

Ein solches System getrennter Kompetenzen – beratender EDÖB und Aufsichtsbehörde mit Verfügungs- und Sanktionskompetenzen – führte u.E. zu einer effektiveren Durchsetzung des Datenschutzes in der Schweiz und gleichzeitig könnten all die negativen Konsequenzen, die mit einer Sanktionierung von Datenschutzverletzungen über das ordentliche Strafrecht resultierten, weitgehend vermieden werden. Zudem könnte der EDÖB an sich nur so seine beratende und empfehlende Funktion glaubwürdig wahrnehmen, was in besonderem Mass auch für den Ansatz der guten Praxis gilt. Schliesslich würde die Schweiz damit eine dem Wortsinn der europäischen Regelwerke entsprechende Aufsichtsbehörde schaffen.

Wir sind uns bewusst, dass wir hiermit einen **neuartigen Vorschlag skizzieren**, den es im Detail zu vertiefen und konkret auszugestalten gälte. scienceindustries würde es begrüssen, wenn das **Bundesamt für Justiz**

diesen Ansatz aufnehmen und im Rahmen einer Arbeitsgruppe mit weiteren interessierten Kreisen einen **konkreten Vorschlag ausarbeiten** würde, wobei wir gerne unsere aktive Beteiligung anbieten.

Abschliessend halten wir fest, dass soweit vorliegende Stellungnahme sich nicht explizit zu weiteren Themen im Kontext der DSG-Revision äussert, wir auf die Stellungnahme von economiesuisse verweisen, die wir grundsätzlich unterstützen.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Dr. Beat Moser
Direktor

Jürg Granwehr
Leiter Pharma Schweiz

Kopie an:
economiesuisse, SwissHoldings
ASSGP, Intergenerika, Interpharma, vips

Schweizer Dialogmarketing Verband

SDV, Postfach, 8501 Frauenfeld

Per E-Mail an jonas.amstutz@bj.admin.ch
Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zürich, den 31. März 2017

Stellungahme des SDV zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Mit seinen über 120 Mitgliederfirmen deckt der SDV Schweizer Dialogmarketing Verband Unternehmen sämtliche Aspekte des Direktmarketings ab und ist die führende Dialogmarketing-Organisation der Schweiz. Der SDV versteht sich als moderner Kommunikationsverband und als nachhaltige Interessenvertretung einer zukunftsorientierten Wachstumsbranche. Er bildet das Direktmarketing-Netzwerk für Anbieter, Dienstleister und Konsumenten in der gesamten Schweiz und repräsentiert diese vitale Branche mit einem Jahresumsatz von ca. CHF 3.4 Mia. und rund 11'000 Angestellten.

Wir begrüssen die mit dem vorliegenden Entwurf angestrebte **Modernisierung des Datenschutzrechts und die beabsichtigte Annäherung an die künftige Rechtslage in der EU**. Ebenso sieht der SDV die gesamtwirtschaftliche Bedeutung und Wichtigkeit der Möglichkeiten der Datenbearbeitungen zu Werbezwecken und des Vertrauens in diese Datenbearbeitungen. Die Möglichkeit des reibungslosen Datenaustausches mit den europäischen Nachbarländern ist für die Schweizer Dialog- und Direktmarketingbranche von grosser Wichtigkeit. Der Marktzugang ist sicherzustellen und die Revision darf nicht zu neuen Standortnachteilen oder Handelshemmnissen führen. Im rasanten Wandel des technologischen Umfelds ist es für unsere Verbandsmitglieder, wie auch für alle anderen Unternehmen, sodann zentral, dass mit der künftigen Regelung Rechtssicherheit für die wirtschaftliche Tätigkeit geschaffen wird.

Diese Anforderung ist umso wichtiger, als mit der Revision das Sanktionssystem erheblich verschärft werden soll. Unklarheiten sind daher so weit wie möglich zu vermeiden. Zugleich müssen die Einschränkungen der wirtschaftlichen Freiheit und die administrativen Aufwendungen, die den Unternehmen durch die Änderung der rechtlichen Vorgaben entstehen, auf das absolut Notwendige reduziert werden. Ferner räumt der Bundesrat der Aufrechterhaltung der Angemessenheit des Schweizer Datenschutzrechts zwar zu Recht eine hohe Priorität ein. Zu beachten ist dabei jedoch, dass es hierfür keinesfalls erforderlich ist, über die Vorgaben der E-SEV 108 und der EU-DSGVO hinauszugehen. Leider enthält der Vorentwurf zahlreiche Bestimmungen, die gegenüber den internationalen Verpflichtungen der Schweiz zu verschärften Vorschriften für Schweizer Unternehmen enthält. Durch diese Bestimmungen entstehen direkt Standortnachteile für in der Schweiz ansässige Unternehmen.

Vor diesem Hintergrund **lehnen wir im Grundsatz jegliche Änderungen gegenüber der geltenden Rechtslage ab, die zur Einhaltung der Vorgaben der Europarats-Konvention (E-SEV 108) oder mit Blick auf die Angemessenheits-Beurteilung des Schweizer Datenschutzrechts durch die EU nicht zwingend geboten sind (sog. „Swiss Finish").** Angesichts der Tatsache, dass Datenbearbeitungen bereits heute häufig und künftig noch vermehrt grenzüberschreitend erfolgen, können Schweizer Sonderregelungen in Abweichung der EU-DSGVO, welche die unternehmerische Tätigkeit und die Zusammenarbeit zwischen nationalen Behörden erschweren, nicht im Interesse des Unternehmensstandortes Schweiz sein. Auf solche Sonderregelungen muss deshalb konsequent verzichtet werden. **Selbstregulierende Massnahmen sind einer bürokratischen Gesetzgebung vorzuziehen.**

Insbesondere kostenerhöhende Vorschriften, welche dazu führen, dass die administrativen Kosten und Aufwände und damit die Kosten der betreffenden Werbeaktivitäten zunehmen, sind nur dann akzeptabel, wenn sie aufgrund der zwingenden Vorgaben der Datenschutzkonvention des Europarates erforderlich sind. Unnötige werbebeschränkende Vorschriften, die, auch im Vergleich zur heutigen Ausgangslage, Werbeaktivitäten neu einschränken oder faktisch gar verunmöglichen, lehnen wir kategorisch ab.

Ausgehend davon sind insbesondere der „Swiss Finish" bei der vorgeschlagenen Regelung des „Profiling" und der Sanktionierung von Verstössen strikt abzulehnen. Diese, aber auch zahlreiche weitere punktuelle Bestimmungen, auf die wir in der beiliegenden ausführlichen Stellungnahme zum Vorentwurf eingehen, bedürfen daher einer grundlegenden Überarbeitung. **In der aktuellen Fassung müssen wir den vorgelegten Vorentwurf des neuen DSG ablehnen.**

Schweizer
Dialogmarketing
Verband
Postfach 616
8501 Frauenfeld

T 052 721 61 62
F 052 721 61 63
info@sdv-dialogmarketing.ch

www.sdv-dialogmarketing.ch
www.sdv-konsumenteninfo.ch
www.sdv-award.ch

www.facebook.com/dmverband
www.xing.com/net/sdv
www.xing.com/net/dmpreis

Insbesondere das vorgesehene Sanktionssystem, mit dem eine weitgehende **Kriminalisierung von natürlichen Personen in den datenbearbeitenden Unternehmen** anstelle einer direkten Disziplinierung der wirtschaftlich verantwortlichen Unternehmen erfolgt, ist inakzeptabel. Dieses Sanktionssystem führt zudem zu einer massiven Bevorteilung international tätiger Grossunternehmen gegenüber Schweizer Unternehmen, da die Verfolgung und Vollstreckung gegenüber im Ausland ansässigen Unternehmen faktisch und rechtlich nicht möglich sein wird.

Es ist sodann auch in besonderem Masse **KMU-feindlich**, da die Rechtsverfolgung der entsprechend sanktionierten Tatbestände gegen verantwortliche Personen in kleineren Organisationen viel einfacher und damit für die kantonalen Strafverfolgungsbehörden viel „effizienter" möglich wäre.

Weiter stellt dieses Sanktionssystem für die **Innovationskraft und das Innovationspotential** der Digitalen Wirtschaft in der Schweiz und insbesondere der Schweizer KMU eine grosse Gefahr dar: Die Risikobeurteilung im Rahmen neuer Innovationen in der „Data Economy" müsste immer im Licht einer möglichen strafrechtlichen Verfolgung der Mitarbeiter entsprechender Unternehmen vorgenommen werden. Dies dürfte eine nicht zu unterschätzende abschreckende Wirkung haben.

Schlussendlich stellt dieses Sanktionssystem unseres Erachtens die zentrale Anerkennung der Angemessenheit des Schweizer Datenschutzniveaus in keiner Weise sicher. Entsprechende Sanktionen wären gegenüber Datenbearbeitern aus dem Ausland faktisch und in den meisten Fälle auch rechtlich nicht vollstreckbar. Diese Unternehmen wären damit im Ergebnis nicht betroffen von den neuen Strafandrohungen und gegenüber Schweizer Unternehmen klar im Vorteil. Der SDV lehnt dieses Sanktionssystem deshalb strikt ab und schliesst sich der Forderung der economiesuisse nach einem auf **Verwaltungssanktionen** beruhenden System an.

Im Übrigen verweisen wir auf unsere **detaillierte Stellungnahme** zu den einzelnen Bestimmungen des Vorentwurfs in der Beilage.

Für die Berücksichtigung der Anliegen der Werbebranche zur Schaffung einer verhältnismässigen und praxistauglichen Datenschutzregulierung danken wir Ihnen im Voraus und stehen Ihnen für Rückfragen gerne zur Verfügung.

Mit freundlichen Grüssen

Milo Stössel
Präsident SDV

Lukas Bühlmann
Vorstand SDV (Recht & Regulierung)

Beilage: Stellungnahme zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Schweizer
Dialogmarketing
Verband
Postfach 616
8501 Frauenfeld

T 052 721 61 62
F 052 721 61 63
info@sdv-dialogmarketing.ch

www.sdv-dialogmarketing.ch
www.sdv-konsumenteninfo.ch
www.sdv-award.ch

www.facebook.com/dmverband
www.xing.com/net/sdv
www.xing.com/net/dmpreis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schweizer Dialogmarketing Verband (SDV)

Abkürzung der Firma / Organisation : SDV

Adresse : Postfach 616, 8501 Frauenfeld

Kontaktperson : RA Lukas Bühlmann

Telefon : 052 721 61 62

E-Mail : info@sdv-dialogmarketing.ch; buehlmann@br-legal.ch

Datum : 31. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SDV	Wir begrüssen die mit dem vorliegenden Entwurf angestrebte Modernisierung des Datenschutzrechts und die beabsichtigte Annäherung an die künftige Rechtslage in der EU. Im rasanten Wandel des technologischen Umfelds ist es für unsere Verbandsmitglieder, wie auch für alle anderen Unternehmen, zentral, dass mit der künftigen Regelung Rechtssicherheit für die wirtschaftliche Tätigkeit geschaffen wird. Diese Anforderung ist umso wichtiger, als mit der Revision das Sanktionssystem erheblich verschärft werden soll. Unklarheiten sind daher so weit wie möglich zu vermeiden. Zugleich müssen die Einschränkungen der wirtschaftlichen Freiheit und die administrativen Aufwendungen, die den Unternehmen durch die Änderung der rechtlichen Vorgaben entstehen, auf das absolut Notwendige reduziert werden. Ferner räumt der Bundesrat der Aufrechterhaltung der Angemessenheit des Schweizer Datenschutzrechts zwar zu Recht eine hohe Priorität ein. Zu beachten ist dabei jedoch, dass es hierfür keinesfalls erforderlich ist, über die Vorgaben der E-SEV 108 und der EU-DSGVO hinauszugehen. Leider enthält der Vorentwurf zahlreiche Bestimmungen, die gegenüber den internationalen Verpflichtungen der Schweiz zu verschärften Vorschriften für Schweizer Unternehmen enthält. Dies führt zu Standortnachteilen für in der Schweiz ansässige Unternehmen. Vor diesem Hintergrund lehnen wir im Grundsatz jegliche Änderungen gegenüber der geltenden Rechtslage ab, die zur Einhaltung der Vorgaben der Europarats-Konvention (E-SEV 108) oder mit Blick auf die Angemessenheits-Beurteilung des Schweizer Datenschutzrechts durch die EU nicht zwingend geboten sind (sog. Swiss Finish). Angesichts der Tatsache, dass Datenbearbeitungen bereits heute häufig und künftig noch vermehrt grenzüberschreitend erfolgen, können Schweizer Sonderregelungen in Abweichung der EU-DSGVO, welche die unternehmerische Tätigkeit und die Zusammenarbeit zwischen nationalen Behörden erschweren, nicht gutgeheissen werden. Ausgehend davon sind insbesondere der „Swiss Finish“ bei der vorgeschlagenen Regelung des „Profiling“ und der Sanktionierung von Verstössen strikt abzulehnen. Diese, aber auch zahlreiche weitere punktuelle Bestimmungen, auf die wir nachgehend eingehen, bedürfen daher einer grundlegenden Überarbeitung. In der aktuellen Fassung müssen wir den vorgelegten Vorentwurf des neuen DSG ablehnen. Insbesondere das vorgesehene Sanktionssystem, mit dem eine weitgehende Kriminalisierung von natürlichen Personen in den datenbearbeitenden Unternehmen anstelle einer direkten Disziplinierung der wirtschaftlich verantwortlichen Unternehmen erfolgt ist inakzeptabel. Dieses Sanktionssystem führt zudem zu einer massiven Bevorteilung international tätiger Grossunternehmen gegenüber Schweizer Unternehmen, da die Verfolgung und Vollstreckung gegenüber im Ausland ansässigen Unternehmen faktisch und rechtlich nicht möglich sein wird. Es ist sodann auch in besonderem Masse KMU-feindlich, da die Rechtsverfolgung der entsprechend sanktionierten Tatbeständen gegen verantwortliche Personen in kleineren Organisationen viel einfacher und damit für die kantonalen Strafverfolgungsbehörden viel „effizienter“ möglich wäre.. Darüber hinaus ist zwar der Verzicht auf die zwingende Einführung eines betrieblichen Datenschutzbeauftragten zu begrüssen. Allerdings ist die

	freiwillige Einführung eines solchen zu unterstützen, weshalb das Institut gesetzlich weiter vorgesehen sein sollte. Unternehmen, die einen Beauftragten einführen, sollten ferner von gewissen Meldepflichten befreit werden. Zudem müsste dies bei der Sanktionierung angemessen berücksichtigt werden.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SDV	DSG	1			Entsprechend der Strategie des Bundesrats für eine „digitale Schweiz“ und den Zielsetzungen in der EU-DSGVO ist der Zweck der „Förderung des freien Verkehrs von Personendaten“ in die Bestimmung aufzunehmen.
SDV	DSG	2	1		Im Hinblick auf die Annäherung an die Regelung in der EU-DSGVO und aufgrund der damit verbundenen Erleichterung von Datentransfers ins Ausland ist die Ausklammerung von juristischen Personen grundsätzlich zu begrüssen.
SDV	DSG	3		a	Die Beibehaltung der Definition von Personendaten ist zu begrüssen. Unter Einbezug des erläuternden Berichts ist die vorgeschlagene Regelung jedoch unklar und potentiell widersprüchlich. Auf der einen Seite soll der Begriff „Personendaten“ gemäss Bericht gegenüber dem geltenden Recht zwar inhaltlich nicht geändert werden**. Dabei ist insbesondere die implizite Anerkennung der relativen Methode, wie sie auch in der EU künftig weiterhin gelten soll, zentral und richtig**. Auf der andern Seite wird im Bericht jedoch eine natürliche Person als bestimmbar erklärt, wenn sie „über Hinweise auf eine Identifikationsnummer oder eine Online-Identität“ identifiziert werden kann. Diese Formulierung ist gerade in diesem für sämtliche Online-Aktivitäten fundamentalen Punkt missverständlich und je nach Interpretation widersprüchlich. Denn nach der wohl herrschenden Auffassung genügt es unter dem geltendem DSG nicht, wenn Angaben bloss einer bestimmten „eindeutigen Kennung“ oder „Identifikationsnummer“, wie z.B. einer IP-Adresse oder Cookie-Kennungen zugeordnet werden können, hinter welcher letztlich eine Person steht, diese aber nicht namentlich identifiziert werden kann (sog. Singularisierung). Bei der

					Qualifikation von IP-Adressen etc. muss daher auch künftig eine Einzelfallbeurteilung entscheidend sein, unter Berücksichtigung des Aufwands zur Identifizierung mit den zur Verfügung stehenden technischen Möglichkeiten (objektive Seite) sowie dem Interesse an der Identifizierung (subjektive Seite). Insbesondere beim Einsatz von Cookies zur Auslieferung von individualisierter Werbung auf Websites, bei welchem regelmässig auch die IP-Adresse mitbearbeitet wird, besteht dabei kein Interesse an der namentlichen Identifikation des Nutzers, sondern lediglich an der Kategorisierung. Würde hier stets von Personendaten ausgegangen werden müssen**, hätte dies erhebliche Auswirkungen auf die gesamten Online-Aktivitäten, sodass letzten Endes zahlreiche heute werbefinanzierte, unentgeltliche Angebote künftig nicht mehr allgemein zur Verfügung stehen würden. Vor diesem Hintergrund ist eine Klarstellung in der Botschaft, dass das Konzept der Singularisierung abgelehnt wird, von zentraler Bedeutung.** Der Umstand, dass nach Auffassung einzelner Autoren unter der EU-DSGVO eine Singularisierung für das Vorliegen von Personendaten ausreichen soll, ändert daran nichts. Denn zum einen wird diese Auffassung von anderen Autoren mit überzeugenden Argumenten abgelehnt. **Zum anderen ergibt sich eine derart strenge Auslegung auch nicht aus dem E-SEV 108. Deshalb besteht keine Notwendigkeit, sie im Schweizer Recht einzuführen (Swiss Finish).**
SDV	DSG	3		c. 4.	Der Begriff der biometrischen Daten ist zu präzisieren: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Bilder in Zeitungen wären damit ausgenommen (der vorgesehene Wortlaut würde dazu führen, dass solche Bilder unter den Begriff der „biometrischen Daten“ fallen.
SDV	DSG	3		f	**Die vorgeschlagene Definition und die damit einhergehende Regelung (siehe dazu Anmerkungen zu Art. 23 unten) des „Profiling“ werden abgelehnt. Die Definition geht ohne Not weit über diejenige der EU-DSGVO**

					(Art. 4 Ziff. 4) hinaus (Swiss Finish). Zudem enthält der E-SEV 108 keinerlei Vorgaben für das Profiling. Vielmehr verlangt dieser nur eine Regelung von automatisierten Entscheidungen (vgl. Art. 8 Abs.1 lit. a). Ausgehend davon sollte auf spezifische Vorgaben für das Profiling verzichtet werden. Wird gleichwohl an einer Regelung festgehalten, sollte diese aber **jedenfalls auf automatisierte Bearbeitungen beschränkt bleiben. Keinesfalls darf die Regelung jedoch derart weit gefasst werden, dass die Vorgaben (systemwidrig) sogar für das Profiling mit nicht personenbezogenen Daten gelten.** Für die im erläuternden Bericht angesprochenen Bearbeitungen bspw. im Rahmen von Big Data Analysen genügen die übrigen Regelungen vollends. Denn bei einem Profiling, das am Ende zu Personendaten führt, gelten diese ohnehin bereits. Darüber hinaus wird die Unsicherheit, welche konkreten Bearbeitungen in der Praxis als Profiling zu betrachten sind, durch den entsprechenden Zusatz weiter verstärkt.
SDV	DSG	4			Das Festhalten an den bestehenden Datenbearbeitungsgrundsätzen ist im Allgemeinen zu begrüssen.
SDV	DSG	4	3		Das Erfordernis der „klaren“ Erkennbarkeit ist zu streichen. Da eine Änderung der geltenden Rechtslage hiermit nicht beabsichtigt und eine solche auch nicht erforderlich ist, sorgt der Zusatz lediglich für Unsicherheit.
SDV	DSG	4	5		Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Seite 47 des Erläuterungsberichts sind hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten, sonst wird nur neue Unsicherheit geschaffen. Eventualiter: Beschränkung von Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind", Streichung des Restes dieses Passus'. Bekanntlich fängt die "Bearbeitung" ja schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE). Eine fortdauernde Verpflichtung zur

					Nachführung wäre offensichtlich unerfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status' einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Schliesslich ist ausdrücklich klarzustellen, dass die Pflicht nur den Verantwortlichen trifft. Nur der Verantwortliche ist in der Lage, allfälligen Änderungsbedarf zu erkennen.
SDV	DSG	4	6		**Die vorgeschlagene Änderung hinsichtlich des überaus zentralen Begriffs der „Einwilligung" ist unter Einbezug des erläuternden Berichts unklar.** Gemäss erläuterndem Bericht (S. 47) ermöglicht die Neuformulierung eine terminologische Annäherung an die DSGVO. Es wird allerdings nicht klargestellt, ob damit eine inhaltliche Annäherung bezweckt wird. Die Definition ist nicht nur, aber in besonders ausgeprägter Form gerade für die Werbebranche von fundamentaler Bedeutung, weshalb eine klare Regelung und damit Rechtssicherheit erforderlich ist**. Die Übernahme der gegenüber der E-SEV 108 unnötig strengen Vorgaben der EU-DSGVO in Bezug auf die „Freiwilligkeit der Einwilligung" (Art. 7 Abs. 4) hätte jedenfalls eine massive Verschärfung der Rechtslage gegenüber dem geltenden Recht sowie eine erhebliche Beschränkung der Vertragsfreiheit zur Folge, die unnötig und daher abzulehnen ist.** Der E-SEV 108 (Art. 5 Abs. 2) verlangt denn auch lediglich, dass die Einwilligung freiwillig sein muss („free consent"), ohne eine derart strenge Interpretation, wie sie die EU-DSGVO enthält, vorzuschreiben. **In der Botschaft muss deshalb eine entsprechende Klarstellung aufgenommen werden**. **Darüber hinaus sind die Ausführungen im erläuternden Bericht zur „ausdrücklichen Einwilligungen" unklar bzw. unvollständig.** Es geht daraus letztlich nicht hervor, welche Anforderungen konkret an eine solche Einwilligung gestellt werden, was gerade aufgrund des (noch) übermässig weit gefassten Begriffs des Profiling und dessen Bedeutung für die Werbebranche besonders problematisch ist**. Es ist daher in der Botschaft auch klar zu stellen, dass – wie nach geltendem Recht – eine Einwilligung dann ausdrücklich ist, wenn**

					die Datenbearbeitung, in welche eingewilligt wird, also z.B. das Profiling, bspw. in der Datenschutzerklärung beim Namen genannt wird und es insofern genügen würde, wenn bloss aus den Umständen auf ein Profiling geschlossen werden müsste. Schliesslich ist in der Botschaft auch festzulegen, dass – entsprechend dem geltenden Recht – **eine Einwilligung in Datenbearbeitungen auch durch Zustimmung zu einem Dokument, das weitere Informationen erhält (wie z.B. AGB oder Datenschutzerklärungen), erteilt werden kann** und keine separate Information bzw. Einwilligung erforderlich ist.
SDV	DSG	5	3-6		**Die Regelung zur Bekanntgabe ins Ausland bei fehlendem Angemessenheitsbeschluss in verschiedener Hinsicht anzupassen**. Insbesondere geht die Regelung vereinzelt weiter als diejenige der EU-DSGVO **(Swiss Finish).** Generell ist die Unterscheidung zwischen spezifischen und standardisierten Garantien unklar. Es sollte einzig zwischen Standardverträgen und anderen Verträgen/Garantien unterschieden werden. Ferner ist analog der EU-DSGVO die Pflicht zur Information des EDÖB in Art. 5 Abs. 6 VE-DSG zu streichen. Denn es erscheint zweifelhaft, ob und inwiefern eine entsprechende Information letztlich zum Datenschutz beiträgt. Zudem ist die Genehmigungsfrist in Art. 5 Abs. 5 VE-DSG unverhältnismässig lang und kontraproduktiv. Schliesslich ist auch die Ausdehnung der Pflichten auf Auftragsdatenbearbeiter abzulehnen.
SDV	DSG	6	1	b	**Auch an dieser Stelle geht die Regelung unnötig über diejenige der EU-DSGVO (Art. 49 Abs. 1 lit. c) hinaus (Swiss Finish).** Deshalb muss eine Bekanntgabe ins Ausland auch dann erlaubt sein, wenn ein Vertrag lediglich im Interesse der betroffenen Person abgeschlossen worden ist.
SDV	DSG	6	2		Die Informationspflicht bei Vorliegen eines Ausnahmetatbestands ist weder in der EU-DSGVO noch im E-SEV 108 vorgesehen. Die Bestimmung ist daher zu

					streichen.
SDV	DSG	7			Die grundsätzliche Beibehaltung der geltenden Rechtslage hinsichtlich der Auftragsdatenbearbeitung ist zu begrüssen. **Abzulehnen ist jedoch die vorgesehene Ausdehnung der Vergewisserungspflicht dahingehend, ob die Bearbeitung durch den Auftragsbearbeiter die Rechte der betroffenen Personen gewährleisten kann.** Diese Ausdehnung der Vergewisserungspflicht ist unklar und würde zu erheblichem Mehraufwand für das Outsourcing führen. Der Auftragsbearbeiter ist nie der Ansprechspartner der betroffenen Personen. Vielmehr müsste sichergestellt sein, dass der Auftragsbearbeiter das Erforderliche dafür tut, dass der Verantwortliche die Rechte der betroffenen Personen gewährleisten kann. **Zu verzichten ist auch auf die unbeschränkte Delegation an den Bundesrat zur Festlegung weiterer Pflichten. Zudem ist Abs. 3 zu streichen.** Eine zwingende Zustimmung zum Beizug von Sub-Auftragsdatenbearbeiter ist weder durch die internationalen Verpflichtungen gefordert, noch entspricht sie der bisher geltenden Rechtslage (**Swiss Finish**). Sie wäre in der Praxis auch nicht praktikabel. Sollte daran festgehalten werden, müsste die Bestimmung zumindest dahingehend angepasst werden, dass nicht „Schriftlichkeit" erforderlich ist, sondern eine Form, die den „Nachweis durch Text" ermöglicht. Andernfalls wäre die Ermächtigung zur Einsetzung von Unterauftragnehmern namentlich in Verträgen, die Online abgeschlossen werden, nicht mehr möglich.
SDV	DSG	8			Die vorgeschlagene Regelung und die Einführung von Empfehlungen der guten Praxis ist im Grundsatz zu begrüssen. Allerdings kann das Genehmigungsverfahren nicht dem EDÖB alleine unterliegen. Die Genehmigungsinstanz ist genau zu definieren und zu erweitern. **Generell muss jedoch klargestellt werden, wer zu den interessierten Kreisen gehört.** Eine Mitwirkung von Konsumentenverbänden ist auszuschliessen, da deren Interessen bereits durch den Genehmigungsvorbehalt

					des EDÖB ausreichend berücksichtigt werden. Schlussendlich muss gegen die Entscheide des EDÖB, resp. der Genehmigungsinstanz ein Rechtsmittel gegeben sei.
SDV	DSG	8	1		Die Kompetenz des EDÖB zum eigenständigen Erlass von Empfehlungen ist in mehrerer Hinsicht problematisch und deshalb zu streichen. So bestünde die Gefahr, dass der EDÖB letztlich im Alleingang ohne ausreichende Berücksichtigung der branchenspezifischen Bedürfnisse und Besonderheiten Empfehlungen erlässt. Die entsprechenden Empfehlungen dürften in der Regel einen über die gesetzlichen Vorgaben hinausgehenden Standard setzen, der faktisch, trotz der sinnvollen Klarstellung in Art. 9 Abs. 3 VE-DSG, zum Gesetz wird. Darüber hinaus erscheint fraglich, ob es sich dabei um Verfügungen handelt. Sofern die Regelung beibehalten würde, müsste den betroffenen Unternehmen jedenfalls eine Anfechtung ermöglicht werden. Es wäre demnach eine klare Regelung der Rechtsmittel im Gesetz selbst erforderlich.
SDV	DSG	8	2		Nach einem allfälligen Entscheid über die Genehmigung von Empfehlungen wird sich stets die Frage nach den Rechtsmitteln und insbesondere nach der Legitimation zur Ergreifung eines solchen stellen. Zur Klärung der Rechtslage wären hier zumindest Erläuterungen in der Botschaft angezeigt. Die Rechtsmittel, welche allgemein auch im E-SEV 108 verlangt werden (Art. 12bis Abs. 6), sind umso mehr von Bedeutung, als aufgrund der Pflicht zur Genehmigung durch den EDÖB zu erwarten ist, dass mit den Empfehlungen ein über die gesetzlichen Vorgaben hinausgehender Standard gesetzt wird. Dieser wird letztlich auch trotz der expliziten Regelung in Art. 9 Abs. 2 VE-DSG faktisch zum Gesetz werden. **Folglich muss eine klare Regelung bestehen, die es den betroffenen Verbänden bzw. Unternehmen ermöglicht, die Nicht-Genehmigung bzw. Ablehnung einer Empfehlung, die den gesetzlichen Vorgaben entspricht, gerichtlich anzufechten.**

SDV	DSG	12			Die Einführung einer Regelung zu Daten verstorbener Personen ist im Hinblick auf die Angemessenheit des Schweizer Datenschutzrechts nicht zwingend erforderlich und führt für die Unternehmen zu einem erheblichen administrativen Mehraufwand **(Swiss Finish)**. **Auf die Regelung ist daher zu verzichten**. Andernfalls sollte sie zumindest sinnvoll eingeschränkt werden. Insbesondere muss es Unternehmen möglich sein, sich auf überwiegende eigene Interessen oder gesetzliche Pflichten zu berufen, wenn ihnen gegenüber Rechte verstorbener geltend gemacht werden. Erben dürfen im Verhältnis zu einem Datenbearbeiter jedenfalls nicht über mehr Rechte verfügen als der Erblasser zu Lebzeiten selbst.
SDV	DSG	13			Die Einführung einer generellen Informationspflicht ist mit Blick auf den E-SEV 108 zwingend und insofern richtig**. Allerdings gehen diverse Punkte der vorgeschlagenen Regelung zu weit und sind daher abzulehnen** (vgl. dazu nachfolgend). Unklar ist danach ferner, inwiefern die Informationspflicht auch gilt, wenn nachträglich neue Bearbeitungszwecke hinzukommen oder andere Bearbeitungen an die Stelle der ursprünglichen treten. Diesbezüglich ist eine Klarstellung erforderlich, dass nur über das informiert werden muss, was schon zum Zeitpunkt der Beschaffung feststand bzw. dass sich die Information auf den Zeitpunkt der Beschaffung bezieht. Denn in solchen Fällen wäre in der Regel ohnehin eine Einwilligung oder ein anderer Rechtfertigungsgrund erforderlich und eine Sanktionsbewehrung folglich unverhältnismässig. Eine Pflicht zur Nachinformation ist klar auszuschliessen. **Zudem muss zwingend müsste klargestellt werden, dass – entsprechend der geltenden Rechtslage und der Praxis des EDÖB – bei der Beschaffung grundsätzlich ein Verweis auf die auf der Website enthaltenen Detailinformationen ausreicht.** Die Erwägung im erläuternden Bericht, wonach es nicht genügt, wenn die betroffene Person nach den Informationen suchen muss, sollte deshalb zumindest im Rahmen der Botschaft in diesem Sinne

					präzisiert werden.
SDV	DSG	13	2		Angesichts der Sanktionsdrohung sollte eine abschliessende Aufzählung der mitzuteilenden Informationen erfolgen. Andernfalls würden sich Unternehmen zur Vermeidung von Risiken dazu gezwungen sehen, den betroffenen Personen die Vielzahl der Informationen, wie sie in der EU-DSGVO vorgesehen sind, mitzuteilen. Den Betroffenen wäre mit einer solchen Vielzahl von Informationen letztlich nicht gedient. Sie führt nicht zu mehr, sondern im Ergebnis zu weniger Transparenz. Die Mitteilungspflichten gemäss EU-DSGVO gehen über den durch die SEV-108 vorgegebenen Standard hinaus **(Swiss Finish)**. Hier ist eine abschliessende, schlanke Aufzählung vorzusehen. Zudem ist hinsichtlich des Zeitpunkts der Information für den Online-Kontext eine Klarstellung erforderlich. Denn beim Zugriff auf eine Website wird regelmässig eine Bearbeitung von IP-Adressen erfolgen (Erfassung in Log-Datei, Zählung der Website-Zugriffe etc.) und dies in der Regel bereits bevor der Nutzer allfällige Informationen hierzu z.B. in einer Datenschutzerklärung zur Kenntnis nehmen kann. Aufgrund der Tatsache, dass IP-Adressen je nach Einzelfall Personendaten darstellen können und dass eine vorgängige Information hier technisch grundsätzlich nicht möglich ist, **muss klargestellt werden, dass die ausreichend kenntlich gemachte Information in einer Datenschutzerklärung nach Abruf der Website als rechtzeitig gilt.**
SDV	DSG	13	4		Diese Vorgabe hinsichtlich der Information bei einer Auftragsdatenbearbeitung ist weder im E-SEV 108 noch in der EU-DSGVO vorgesehen **(Swiss Finish)**. Sie ist daher ersatzlos zu streichen, da sie für den Betroffenen keinerlei Mehrwert bringt.
SDV	DSG	13	5		Die Ausdehnung der Pflicht auf die indirekte Datenbeschaffung wird in der Praxis jegliche Beschaffung von Daten bei Dritten verunmöglichen. Die Bestimmung ist daher zu streichen. Sofern daran festgehalten wird, ist zu beachten, dass der Entwurf auch hier über die Vorgaben der EU-DSGVO hinausgeht. Analog der EU-Regelung (Art. 14 Abs. 3) müsste es daher in jedem Fall für die

					Datenbeschaffung bei Dritten auch in der Schweiz zulässig sein, die Information zu späteren Zeitpunkten zu erteilen.
SDV	DSG	14			**Der Katalog der Ausnahmen ist enger gefasst, als es nach dem E-SEV 108 erforderlich wäre (Swiss Finish)**. So ist insbesondere der einschränkende Zusatz „*und er die Personendaten nicht Dritten bekannt gibt*“ in Art. 14 Abs. 4 lit. a zu streichen. Solange ein überwiegendes Interesse des Verantwortlichen besteht, ist nicht einzusehen, wieso die Ausnahme nicht gelten soll, wenn Personendaten an Dritte bekannt gegeben werden. Darüber hinaus ist auch Art. 14 Abs. 3 lit. a zu eng gefasst, da sich konkrete Bearbeitungen selten „ausdrücklich“ aus dem Gesetz selbst ergeben. Schliesslich ist auch Abs. 5 zu streichen, da die Umsetzung dieser Vorgabe in der Praxis, insbesondere hinsichtlich überwiegenden Interessen, zu einem unverhältnismässigen Aufwand führt und nicht praktikabel ist. Schliesslich sind hier auch weitere Ausnahmen vorzusehen, um einer missbräuchlichen Geltendmachung des Auskunftsrechts entgegenzuwirken.
SDV	DSG	15			Der Anwendungsbereich der Informations- und Anhörungspflicht ist viel zu weit gefasst, indem gemäss den Erläuterungen bereits „beliebige rechtliche Wirkungen“ genügen. Hier müsste **klargestellt werden, dass auch rechtliche Auswirkungen eine gewisse Schwere erreichen müssen.** Die Regelung zu automatisierten Einzelfallentscheidungen geht zudem wiederum unverständlicherweise über die Vorgaben der EU-DSGVO (Art. 22) hinaus **(Swiss Finish)**. Die dort vorgesehenen Ausnahmen müssen ebenfalls übernommen werden. **Eine derart strenge Regelung ist jedenfalls auch nach dem E-SEV 108 nicht erforderlich.**
SDV	DSG	16			**Die Anknüpfung an das Vorliegen „erhöhter Risiken“ führt zu einem viel zu weit gefassten Anwendungsbereich und geht unverständlicherweise über die Vorgaben in der EU-DSGVO (Art. 35) hinaus (Swiss Finish)**.Der Entwurf und die Erläuterungen bleibt denn auch unklar, was ein „erhöhtes Risiko“ sein

					soll. Jedes noch so kleine Risiko kann als „erhöht“ gegenüber keinem Risiko angesehen werden. Diese Formulierung ist schon deshalb untauglich und zu streichen. Bleibt es bei dieser Formulierung, würde diese zu einem übermässigen Aufwand führen, der sowohl für die Unternehmen als auch für den EDÖB nicht zu bewältigen ist. Denn, wie aus dem erläuternden Bericht hervorgeht, könnte eine solche Pflicht zur Datenschutz-Folgeabschätzung letztlich bei jeder Übermittlung in Länder wie die USA, jedem Profiling und jeder Bearbeitung von besonders schützenswerten Daten bestehen. Dies würde für die Werbebranche zu massiven Kosten führen, da die Pflicht bspw. auch für das Profiling zur Einblendung personalisierter Werbung oder beim Web-Tracking bestehen würde. Entsprechend der EU-Regelung **sollte daher zumindest auf Datenbearbeitungen mit „hohem Risiko“ (oder besser „besonders hohem Risiko“) abgestellt werden**. Dabei sollten auch diejenigen Fälle, in denen die Pflicht besteht, (zumindest beispielhaft) konkretisiert und Ausnahmen vorgesehen werden. Ausgenommen werden sollten namentlich Fälle, in welchen die Betroffenen mit den Datenbearbeitungen einverstanden sind. **Des Weiteren ist die Bezugnahme auf die Risiken für die „Grundrechte“ von Betroffenen bei Datenbearbeitungen durch Private unpassend und folglich zu streichen.** Die vorgeschlagene Regelung geht sodann auch in weiteren Punkten über die EU-DSGVO hinaus **(Swiss Finish)**: So ist die Pflicht entsprechend der EU-Vorschriften (Art. 35 DSGVO) auf den Verantwortlichen zu beschränkt. Eine Ausdehnung auf den Auftragsdatenbearbeiter ergibt letztlich keinen Sinn. Darüber hinaus ist, wenn überhaupt, nur dann eine Meldepflicht gegenüber dem EDÖB vorzusehen, wenn trotz der getroffenen Schutzvorkehrungen nach Auffassung des Verantwortlichen gleichwohl ein „hohes Risiko“ besteht. Mehr verlangt auch die EU-DSGVO nicht (Art. 36 Abs. 1). Mit der vorgeschlagenen Regelung wäre die Meldepflicht derart weit gefasst, dass der Aufwand wiederum weder durch die Unternehmen noch den EDÖB

					bewältigt werden kann. **Schliesslich ist auch die Frist von drei Monaten zur Beurteilung durch den EDÖB länger als diejenige in der EU-DSGVO (Art. 36 Abs. 2). Das Abwarten dieser Frist nicht praktikabel und führt zu einer erheblichen Einschränkung der Handlungsfreiheit der Unternehmen und letztlich zu einer Lähmung der Wirtschaft. Die Frist muss daher entsprechend erheblich verkürzt werden.**
SDV	DSG	17	1		**Nach der vorgeschlagenen Regelung besteht gegenüber dem EDÖB grundsätzlich für jede „unbefugte Datenbearbeitung" eine Meldepflicht**. Daher hat eine Meldung im Grundsatz bei jedem auch noch so geringfügigen Verstoss zu erfolgen. Dabei handelt es sich wiederum um ein **schweizerisches Überschiessen (Swiss Finish),** welches zudem viel weiter geht, als zum Schutz der Betroffenen erforderlich ist. Die vorgesehene Einschränkung auf Fälle, die voraussichtlich nicht zu einem „Risiko für die Persönlichkeit" des Betroffenen führen, vermag den Anwendungsbereich sodann auch nicht hinreichend zu begrenzen. Entsprechend der Vorgabe im E-SEV 108 (Art. 7 Abs. 2**) ist die Meldepflicht daher auf Verletzungen zu beschränken, welche die Rechte der Betroffenen „schwerwiegend" („seriously") gefährden könnten.** In diesem Sinne sollte die Meldepflicht wie auch in der EU-DSGVO auf Fälle beschränkt werden, die zu einem Bruch oder Verlust des Gewahrsams an Daten führen. Bei der vorgeschlagenen Meldepflicht zeigt sich ferner auch deutlich, dass die vorgesehene Sanktionsregelung, welche auf die Bestrafung natürlicher Personen fokussiert, falsch ist. So werden Mitarbeiter vollkommen unangebracht in eine Drucksituation versetzt, sofern sie Kenntnis von einer Verletzung erlangen: Entweder denunzieren sie den zuständigen Mitarbeiter oder machen sich andernfalls unter Umständen gar selbst strafbar. Dies hätte nachhaltige Auswirkungen auf die interne Organisation und Governance rund um datenschutzrechtliche Risiken innerhalb eines Unternehmens. Dieses müsste letztlich immer damit rechnen, dass einzelne Mitarbeiter entsprechende Meldungen machen. Aufgrund der persönlichen strafrechtlichen Verantwortung der Mitarbeiter könnten auch keine Vorgaben an die Ausübung der

					entsprechenden Meldepflichten gemacht werden. Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien. Wieso dieser im Bereich des Datenschutzes plötzlich nicht mehr gelten soll, ist völlig unerfindlich; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen (sofern am strafrechtlichen Sanktionssystem festgehalten werden sollte). Der Verantwortliche müsste sich m.a.W. nicht nur an das datenschutzrechtliche, sondern auch noch an das strafrechtliche Messer liefern. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer regelrechten Flut an Selbstanzeigen zu rechnen, die nur den Apparat des Beauftragten übermässig aufblähen würde.
SDV	DSG	17	2		Wiederum als Schweizer Sonderregelung abzulehnen ist die Meldepflicht gegenüber Dritten. Eine derart weitgehende und aufwändige administrative Zusatzbelastung ist auch in der EU-DSGVO (Art. 19) nicht vorgesehen. Die Pflicht ist auf Fälle zu beschränken, in welchen der betroffenen Person ein schwerwiegender, nicht wiedergutzumachender Nachteil droht..
SDV	DSG	18			Die Einführung dieser neuen Pflichten (Privacy by Default und Privacy by Design) ist namentlich deshalb problematisch, weil deren Verletzung unmittelbar sanktioniert werden soll. Bei beiden Pflichten gibt es nicht eine einzige richtige Vorgehensweise. Nach dem vorgeschlagenen Wortlaut sind „angemessene Massnahmen“ bzw. „geeignete Voreinstellungen“ vorzunehmen. **Hier muss den Datenbearbeitern im Sinne der „Business Judgement Rule“ ein gewisser Ermessensspielraum eingeräumt werden. In der Botschaft ist dies**

					klarzustellen. Ansonsten wäre die Sanktionierung insbesondere auch mit Blick auf das strafrechtliche Bestimmtheitsgebot problematisch. Schliesslich werden die Pflichten wiederum in Abweichung von der EU-DSGVO (Art. 25) ohne ersichtlichen Grund auch den Auftragsbearbeitern auferlegt, für welche die Vorgaben in der Praxis kaum umsetzbar sind. Die Pflichten sind deshalb auf die Verantwortlichen zu beschränken.
SDV	DSG	19			Der vorgeschlagene Entwurf geht auch hier unverständlicherweise über die die Vorgaben der EU-DSGVO hinaus (Art. 19 und 30), indem die Pflichten, nicht nur dem Verantwortlichen auferlegt werden **(Swiss Finish)**. Die Auftragsbearbeiter sind hier in jedem Falle in Bezug auf die in Art. 19 Abs. 2 VE-DSG vorgesehene Informationspflicht aus der Pflicht zu nehmen.
SDV	DSG	19		a	Die vorgeschlagene Dokumentationspflicht ist zu weit gefasst und führt für Unternehmen zu einem erheblichen und unnötigem Aufwand. **Die Regelung darf keinesfalls über das in der EU-DSGVO (Art. 30) vorgeschriebene Verzeichnis der Datenbearbeitungen hinausgehen.** Damit ein solches Verzeichnis überhaupt seinen Zweck erfüllen kann, muss es jedenfalls auf regelmässige Datenbearbeitungen beschränkt sein, andernfalls müsste bereits jegliche Korrespondenz darin erfasst werden. Darüber hinaus sind, wie auch im Rahmen der EU-DSGVO (Art. 30 Abs. 5), entsprechende Ausnahmen vorzusehen. In der aktuell vorgesehenen Form stellt auch diese Bestimmung ein schweizerisches Überschiessen **(Swiss Finish)**.
SDV	DSG	19		b	**Eine solche Mitteilungspflicht ist im E-SEV 108 nicht vorgesehen (Swiss Finish). Sie ist deshalb ersatzlos zu streichen.** Sofern an ihr festgehalten werden sollte, dann ist die Pflicht zur Mitteilung von Berichtigungen, Löschungen oder Vernichtungen von Personendaten im aktuellen Entwurf zu weit gefasst. **Es bedarf hier einer zusätzlichen Einschränkung, wonach eine Mitteilung nur erfolgen muss, wenn die betroffene Person ein schützenswertes Interesse hat**. Zudem geht die

					vorgeschlagene Regelung **wiederum unverständlicherweise über die Vorgaben der EU-DSGVO (Art. 19) hinaus, indem Verletzungen des Datenschutzes auch den Empfängern offen gelegt werden müssen (Swiss Finish)**. Schliesslich ist auch eine zeitliche Beschränkung vorzusehen, sodass nur Empfänger informiert werden müssen, wenn die Daten während einer gewissen Frist weitergegeben wurden (z.B. innert der letzten 5 Jahre, gerechnet vom Zeitpunkt der Informationspflicht).
SDV	DSG	20	1		**Die Anforderung der Kostenlosigkeit des Auskunftsrechts ergibt sich nicht aus dem E-SEV 108 und ist zu streichen (Swiss Finsih)**. Im Gegenteil wird nur verlangt, dass die Auskunftserteilung ohne übermässige Kosten zu erfolgen hat („without excesive expense"; Art. 8 Abs. 1 lit. b). Folglich muss es den Unternehmen möglich sein, **eine angemessene Aufwandsentschädigung** zu verlangen. Die Auswirkungen der Kostenlosigkeit insbesondere auf KMU-Unternehmen darf nicht unterschätzt werden. Sie kann durchaus eine existentielle Bedrohung darstellen, sollte davon inskünftig extensiver Gebrauch gemacht werden. Es ist davon auszugehen, dass diese Rechte inskünftig zunehmend und in einem intensiveren Ausmass genutzt werden, als bislang. Hier ist die Einschätzung von PWC im Rahmen der Regulierungsfolgeabschätzung in besonderem Ausmass unrealistisch.
SDV	DSG	20	3		**Das Auskunftsrecht hinsichtlich von Entscheidungen aufgrund einer automatisierten Datenbearbeitung ist viel zu weit gefasst und nach der vorgeschlagenen Regelung geradezu uferlos.** Entsprechend der Regelung in der EU-DSGVO (Art. 15 Abs. 1 lit. h) ist das Auskunftsrecht auf diejenigen Fälle zu beschränken, in welchen auch eine Informations- und Anhörungspflicht nach Art. 15 VE-DSG besteht, also auf Entscheidungen, die automatisiert erfolgen und entsprechende Auswirkungen haben. Die aktuell vorgesehene Regelung ist wiederum unnötig überschiessend **(Swiss Finish)** und ist zwingend einzuschränken.

SDV	DSG	23			**Das generelle Erfordernis der ausdrücklichen Einwilligung für das Profiling stellt eine der problematischsten Schweizer Verschärfungen dar und ist zwingend zu streichen (Swiss Finish)**. Für die Werbewirtschaft hat diese Anforderung erhebliche Konsequenzen, welche unnötig sind. Denn nach dem E-SEV 108 ist eine entsprechende Vorgabe nicht verlangt. Ferner ist auch nach der EU-DSGVO nicht für jegliche Form des Profiling eine Einwilligung erforderlich. Aber auch in der Sache besteht keine Notwendigkeit, das Profiling per se als Persönlichkeitsverletzung einzustufen. Solange die Datenbearbeitungsgrundsätze eingehalten werden, ist nicht ersichtlich, wieso neben der Information stets zusätzlich auch eine Einwilligung erforderlich sein soll. **Wird diese Vorschrift Gesetz, verunmöglicht sie faktisch einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung / Marketing und stellt eine Bedrohung für den Standort Schweiz dar**. Profiling und damit personalisierte Werbung wäre dann nur noch den grossen (insbesondere internationalen) Log-in Giganten wie Facebook, Google, Apple und Co. vorbehalten. Diese Unternehmen können sich meist problemlos auf eine ausdrückliche Einwilligung im Rahmen der Account-Registrierungen stützen. Das Ergebnis wäre sodann auch aus kartellrechtlichen Überlegungen höchst problematisch.
SDV	DSG	23	3		Die Beibehaltung der geltenden Regelung von allgemein zugänglich gemachten Daten ist zu begrüssen. Dabei ist jedoch die Erwägung im erläuternden Bericht, wonach die Regelung nur zum Tragen komme, wenn die Bearbeitung dieser Daten auch rechtmässig erfolgt (S. 69), unzutreffend und daher in der Botschaft klar zu stellen.
SDV	DSG	24	2		**Die Neuformulierung, wonach die aufgezählten Sachverhalte bloss „möglicherweise“ ein überwiegendes Interesse darstellen, ist abzulehnen.** Zweck der Aufzählung ist die Schaffung von Rechtssicherheit. Mit der neuen

					Formulierung wird diese aber sogleich wieder aufgehoben. Der SDV fordert sodann, dass entsprechend der EU-DSGVO (Erw.-Gr. 47) zumindest in der Botschaft darauf hinzuweisen ist, dass die Bearbeitung von Personendaten zum Zwecke der Direktwerbung ein überwiegendes Interesse darstellen kann.
SDV	DSG	24	2	a.	**Das Wort „unmittelbar" ist zu streichen**. Es führt zu einer zu starken Einschränkung und lässt unnötigen Interpretationsspielraum.
SDV	DSG	24	2	C3	**Volljährigkeit: Absatz 2 lit. c (3) ist ersatzlos zu streichen.** Eine Volljährigkeit kann häufig erst mit einer Datenprüfung festgestellt werden (oder eben auch nicht). Hier ist die Formulierung so zu wählen, dass es bei einer Kreditprüfung Pflicht ist, die Volljährigkeit zu prüfen. Online-Versandhändler führen in den meisten Fällen für den Kauf auf Rechnung eine Kreditprüfung durch. Dabei ist Volljährigkeit ein entscheidendes Merkmal für das Zustandekommen des Vertrages. Zudem bestehen diverse Umstände, die eine Prüfung auf Volljährigkeit gesetzlich erforderlich machen. Die Durchführung einer Kreditprüfung ist häufig das zuverlässigste Mittel zur Prüfung der Volljährigkeit.
SDV	DSG	25			Zu begrüssen ist das grundsätzliche Festhalten am bisher bewährten zivilrechtlichen Rechtschutz und namentlich der Verzicht auf eine besondere Regelung des „Rechts auf Vergessen". Das geltende Recht gewährt bereits ausreichende und ausgewogene Möglichkeiten, um sich gegen eine Datenbearbeitung zur Wehr zu setzen. **Allerdings ist der letzte Satz in Absatz 2 ersatzlos zu streichen**. Weder die E-SEV 108 noch die DSGVO sehen vor, dass neben dem Bestreitungsvermerk auch eine Beschränkung der Datenbearbeitung verlangt werden kann. Die Umsetzung dieser überschiessenden neuen Bestimmung **(Swiss Finish)** ist nicht praktikabel.

SDV	DSG	37-49			Die erforderliche Anpassung des Sanktionssystems (Verwaltungs- anstelle von Strafsanktionen, siehe unten) bedingt auch eine Überarbeitung der vorgeschlagenen Regelungen zum EDÖB. Zur Vermeidung einer zu grossen Machtfülle durch Bündelung von Untersuchungs- und Spruchkompetenzen und zur Ermöglichung einer vertrauensvollen Kooperation zwischen Unternehmen und EDÖB ist eine Datenschutz-Kommission zu bilden, welche über Verfügungs- und Sanktionskompetenzen verfügt. Der EDÖB hätte in dieser Struktur seine bisherigen Aufgaben wahrzunehmen und namentlich eine Vorselektion der ihm zugetragenen Fälle durchzuführen. Bei Verdacht auf einen Verstoss, würde er die Angelegenheit an die Datenschutz-Kommission weiterleiten. Auf dieser Stufe des Verfahrens ist auch auf eine Mitwirkungspflicht der Unternehmen zu verzichten (Stichwort: Selbstbelastungsverbot). Zur Anfechtung der Entscheide der Kommission müsste ein Rechtmittel vor Bundesverwaltungsgericht ergriffen werden können. Im Übrigen verweisen wir auf die ausführlichen entsprechenden Stellungnahmen in der Vernehmlassungsantwort der economiesuisse.
SDV	DSG	44	3		**Unabhängig vom letztlich gewählten Modell ist jedenfalls eine Regelung abzulehnen, wonach vorsorgliche Massnahmen der zuständigen Behörde per se keine aufschiebende Wirkung haben sollen.** Da die Einstellung oder Anpassung von Datenbearbeitungen während der ungewiss langen Dauer des Verwaltungsverfahrens **massive und durchaus auch irreparable Schäden** für die Unternehmen verursachen kann, muss den Betroffenen zumindest die Möglichkeit gegeben werden, die Erteilung der aufschiebenden Wirkung durch die zuständige Rechtsmittelinstanz zu beantragen.
SDV	DSG	50 ff.			**Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt**. Dieses vorgesehene Sanktionssystem steht der Digitalen Strategie der Schweiz diametral entgegen. Es ist in höchstem Mass innovationshemmend und etabliert eine Kultur des Denunziantentums in den Unternehmen. Es führt zu einem ganz erheblichen Standortnachteil der Schweiz. Kein innovatives digitales

					Start-Up wird bereit sein, seine Gründer und Mitarbeiter solch drastischen strafrechtlichen Risiken auszusetzen. Gute Mitarbeiter werden nicht mehr bereit sein Verantwortung in den Unternehmen mitzutragen. Insbesondere aufgrund der vorgesehenen Strafbarkeit fahrlässigen Verhaltens wird potentiell jeder Mitarbeiter durch heute alltägliche Verrichtungen am Arbeitsplatz ständig Gefahr laufen, sich strafbar zu machen. Dies ist auch gesellschaftspolitisch komplett inakzeptabel. Gleichzeitig ist es gegenüber Datenbearbeitungen durch ausländische Unternehmen faktisch nicht durchsetzbar, was sodann einerseits den Datenschutz in der Schweiz nicht erhöht und andererseits ausländischen Unternehmen einen immensen Wettbewerbsvorteil verschafft. Sodann würde die Schweiz damit gegenüber der EU in diesem grundlegenden Punkt einen Sonderweg einschlagen. Selbst wenn gemäss dem E-SEV 108 nicht zwingend administrative Bussen verlangt werden, wird gleichwohl eine unnötige Unsicherheit im Hinblick auf die Beurteilung der Angemessenheit des Schweizer Datenschutzrechts geschaffen. Ferner wird die Abweichung wie erwähnt international aber auch schon im europäischen Kontext zu vollstreckungsrechtlichen Schwierigkeiten führen (Stichwort: Voraussetzung der doppelten Strafbarkeit), was letztlich zu einer Bevorzugung von ausländischen Unternehmen gegenüber den einheimischen führt. **In jedem Falle wird die vorgeschlagene Regelung aber auch die für die Schweizer Wirtschaft zentralen Verhandlungen zwischen der Schweiz und der EU über die Koordinierung der Anwendung des jeweiligen Datenschutzrechts und die Abgrenzung der Zuständigkeit der Aufsichtsbehörden (Motion Fiala, 16.3752) erheblich erschweren.** Es erscheint gänzlich unrealistisch, dass die EU eine entsprechende Vereinbarung abschliesst, wenn in der Schweiz Unternehmen, die Datenschutzverletzungen gegenüber EU-Bürgern begehen, nur in Ausnahmefällen bzw. nach Ermessen der Untersuchungsbehörden verfolgt werden können.

					Darüber hinaus greift auch die Begründung „mit Blick auf die Kosten“ im erläuternden Bericht viel zu kurz. Die Kosten werden mit der vorgeschlagenen Regelung lediglich auf die kantonalen Strafbehörden übertragen. Es ist nicht ersichtlich, inwiefern sich diese hierdurch verringern sollten. Im Gegenteil ist ein solches **System ineffizient und wird gesamtwirtschaftlich deutlich höhere Kosten verursachen**, da neben dem Verwaltungsverfahren des EDÖB bei Verdacht auf strafrechtlich relevante Verhaltensweisen ein zusätzliches Strafverfahren mit neuerlichen Untersuchungsmassnahmen durchzuführen ist. Der gleiche Fall müsste folglich zweimal untersucht werden. Dies würde auch für die Unternehmen zu einem nicht vertretbaren und unnötigen Mehraufwand führen. **Schliesslich ist auch die primäre strafrechtliche Sanktionierung der natürlichen Personen an sich unverhältnismässig und mit Blick auf den Datenschutz nicht zielführend.** Die betroffenen Mitarbeiter würden durch das Risiko einer strafrechtlichen Verurteilung massiv unter Druck gesetzt. Namentlich bei Kenntnis einer Verletzung müssten sie entweder den zuständigen Mitarbeiter denunzieren oder würden sich andernfalls unter Umständen gar selbst strafbar machen. Ferner besteht die Gefahr, dass Unternehmen nach Möglichkeit einen unliebsamen Mitarbeiter im Sinne eines „Bauernopfers“ für den massgeblichen Verstoss als zuständig bezeichnen und sich so letztlich aus der Verantwortung nehmen können. **Zudem würde gerade die Position von betrieblichen Datenschutzverantwortlichen, die eigentlich zur Erhöhung des Datenschutzes beitragen sollten, mit dem vorgeschlagenen System erheblich geschwächt.** Statt der Förderung des betrieblichen Datenschutzes würde damit eine Kultur der Verschleierung geschaffen. Insbesondere in kleineren Unternehmen, in welchen die zuständige Person einfacher ausfindig zu machen ist, dürfte kaum mehr jemand bereit sein, eine entsprechende Stelle, resp. die entsprechende Verantwortung zu übernehmen.

					Geradezu absurd erscheint die Schärfe des vorgeschlagenen Sanktionssystems, wenn man bedenkt, dass damit ausgerechnet der materielle Kern eines wirksamen Datenschutzes, nämlich die Beachtung der Bearbeitungsgrundsätze, nicht sanktionsbedroht sein soll. Dies im Übrigen natürlich zu Recht. Spätestens in diesem Zusammenhang wird nämlich klar, dass sich das Strafrecht als disziplinierendes Instrument in diesem Bereich nicht eignet. In einem Rechtsstaat kann ein Verhalten nur strafbar sein, wenn der zugrundeliegende Tatbestand eindeutig bestimmt ist. Gerade dies ist aber im Bereich des Datenschutzes in den meisten Fällen nicht der Fall: wie soll ein Mitarbeiter voraussehen können, ob die mit einer Bearbeitung verbundenen Risiken genügend „erhöht“ sind, um damit die strafrechtlich sanktionierte Pflicht einer Risiko-Folgenabschätzung im Sinne von Art. 16 VE-DSG auszulösen? **Vor diesem Hintergrund sind anstelle von Strafsanktionen verwaltungsrechtliche Bussen einzuführen.** Für Binnensachverhalte ist es allerdings nicht angezeigt, die Bussenrahmen der EU-DSGVO zu übernehmen. Hier genügen tiefere Maximalsanktionen. Mit Blick auf eine allfällige Koordinations-Vereinbarung mit der EU sollten die Obergrenzen für Verstösse, die den EU-Markt betreffen, allerdings höher ausfallen. Der SDV schliesst sich der Forderung der economiesuisse nach einem Sanktionssystem entsprechend den folgenden Grundsätzen an: Die Sanktionen sollen sich primär an die Unternehmen richten und verwaltungsrechtlicher Natur sein. Eine Sanktionierung von Mitarbeitenden ist nur für Fälle von direkt vorsätzlichen Verstössen vorzusehen, in welchen sich das Handeln des Mitarbeiters gegen die Interessen des Unternehmens oder der betroffenen Person richtet. Der Kreis der potentiell verantwortlichen Mitarbeitenden muss dabei klar definiert und angemessen eingeschränkt werden. Des Weiteren ist der Strafkatalog anzupassen. Dieser darf in keinem Fall über die EU-DSGVO hinausgehen. Zu offen formulierte Tatbestände sind dabei entweder

					aus dem Katalog zu entfernen oder zu konkretisieren. Zudem ist eine Erheblichkeitsschwelle einzuführen, die sich an der Schwere der Persönlichkeitsverletzung oder an der Höhe des entstandenen Schadens orientiert. Auf die Sanktionierung von fahrlässig begangenen Verstössen ist zu verzichten. Schliesslich ist auch kooperatives Verhalten durch geeignete Anreize zu fördern, indem Sanktionen bei Vorliegen von schadensminderndem Verhalten wegfallen oder zumindest reduziert werden. Im Übrigen verweisen wir auf die ausführliche Stellungnahme der economiesuisse in deren Vernehmlassungsantwort.
SDV	DSG	52			**Der vorgeschlagene Ausbau der geltenden Regelung (Art. 35 DSG) ist abzulehnen.** Ein berechtigter Grund oder die Notwendigkeit hierfür besteht nicht. Sofern die Regelung extensiv interpretiert wird, würde die Konzeption des Schweizerischen Datenschutzrechts auf den Kopf gestellt werden – zumindest betreffend die Bekanntgabe von Daten an Dritte. Bis anhin durften „normale“ Personendaten grundsätzlich ohne einen Rechtfertigungsgrund an Dritte weitergegeben werden – sofern auch die anderen Datenbearbeitungsgrundsätze eingehalten wurden. Nur für besonders schützenswerte Personendaten und Persönlichkeitsprofile wurde vermutet, dass die Bekanntgabe an Dritte ohne Zustimmung der betroffenen Person eine Persönlichkeitsrechtsverletzung darstellt. Art. 52 VE-DSG würde diesen Mechanismus auf den Kopf stellen. Obwohl eigentlich der materielle Teil des Datenschutzgesetzes für die Bekanntgabe von normalen Personendaten an Dritte keinen Rechtfertigungsgrund verlangt, würde eine solche Pflicht zumindest bei der Bekanntgabe von „geheimen“ Personendaten über den Umweg der strafbewehrten Schweigepflicht eingeführt werden. Eine solche Umkehr des geltenden Mechanismus ist nicht begründet und wird auch weder von der E-K108 verlangt, noch ist eine entsprechende Pflicht in der DSGVO vorgesehen. Hier schiesst der Vorentwurf damit klar und ohne Not über das Ziel hinaus. **Hinzu kommt, dass der Begriff der „geheimen Personendaten“ unklar ist. Letztlich würde damit ein allgemeines**

					Berufsgeheimnis für jedermann geschaffen, wonach praktisch jeder Berufstätige einer Geheimhaltungspflicht unterstehen würde, was unverhältnismässig ist.
SDV	DSG	55			Sollte es bei der strafrechtlichen Sanktionen bleiben, so ist die Verjährungsfrist auf 3 Jahre zu reduzieren. Dies entspricht Art. 109 StGB und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
SDV	ZPO	99	3	d	Der SDV lehnt die Abschaffung der Möglichkeit einer Sicherstellungspflicht für die Parteientschädigung der beklagten Partei ab. Es ist fragwürdig, die Konkretisierung der datenschutzrechtlichen Normen und damit die Rechtssicherheit über eine Incentivierung zivilrechtlicher Streitigkeiten erreichen zu wollen. Diese Konkretisierung ist in erster Linie Aufgabe des Gesetzgebers und sodann durch die Empfehlungen und Entscheidpraxis des EDÖB's zu erreichen. Entsprechend lehnt der SDV alle vorgesehenen Instrumente des Entwurfes ab, mit dem der Zugang zu zivilrechtlichen Verfahren für die klagenden Parteien über eine Abschaffung von Verfahrenskosten vereinfacht werden sollen ab. In aller Regel sind es nicht die gesetzlich vorgesehenen Gerichtskosten und damit zusammenhängenden zivilprozessualen Voraussetzungen, die in Bezug auf den Entscheid, eine Klage zu erheben, abschreckend wirken.
SDV	ZPO	113	2	g	Der SDV lehnt die Befreiung von Gerichtskosten in zivilrechtlichen Verfahren zur Durchsetzung des Datenschutzgesetzes (Verfahren nach Art. 25 VE-DSG) ab.
SDV	ZPO	114		F	Der SDV lehnt die Befreiung von Gerichtskosten in zivilrechtlichen Verfahren zur Durchsetzung des Datenschutzgesetzes (Verfahren nach Art. 25 VE-DSG) ab.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
SDV	3 lit. a	Die **Ausführungen zum Begriff der Personendaten sind unklar und potentiell widersprüchlich**. Auf der einen Seite soll der Begriff „Personendaten“ gemäss Bericht gegenüber dem geltenden Recht zwar inhaltlich nicht geändert werden. Dabei ist insbesondere die implizite Anerkennung der relativen Methode, wie sie auch in der EU künftig weiterhin gelten soll, zentral und richtig. Auf der andern Seite wird im Bericht jedoch eine natürliche Person als bestimmbar erklärt, wenn sie „über Hinweise auf eine Identifikationsnummer oder eine Online-Identität“ identifiziert werden kann. Diese Formulierung ist gerade in diesem für sämtliche Online-Aktivitäten fundamentalen Punkt missverständlich und je nach Interpretation widersprüchlich. Denn nach der wohl herrschenden Auffassung genügt es unter dem geltendem DSG nicht, wenn Angaben bloss einer bestimmten „eindeutigen Kennung“ oder „Identifikationsnummer“, wie z.B. einer IP-Adresse oder Cookie-Kennungen zugeordnet werden können, hinter welcher letztlich eine Person steht, diese aber nicht namentlich identifiziert werden kann (sog. Singularisierung). Bei der Qualifikation von IP-Adressen etc. muss daher auch künftig eine Einzelfallbeurteilung entscheidend sein, unter Berücksichtigung des Aufwands zur Identifizierung mit den zur Verfügung stehenden technischen Möglichkeiten (objektive Seite) sowie dem Interesse an der Identifizierung (subjektive Seite). Insbesondere beim Einsatz von Cookies zur Auslieferung von individualisierter Werbung auf Websites, bei welchem regelmässig auch die IP-Adresse mitbearbeitet wird, besteht kein Interesse an der namentlichen Identifikation des Nutzers, sondern lediglich an der Kategorisierung. Würde hier stets von Personendaten ausgegangen werden müssen, hätte dies erhebliche Auswirkungen auf die gesamten Online-Aktivitäten, sodass letzten Endes zahlreiche heute werbefinanzierte, unentgeltliche Angebote künftig nicht mehr allgemein zur Verfügung stehen würden. **Vor diesem Hintergrund ist eine Klarstellung in der Botschaft, dass das Konzept der Singularisierung abgelehnt wird, von zentraler Bedeutung**. Der Umstand, dass nach Auffassung einzelner Autoren unter der EU-DSGVO eine Singularisierung für das Vorliegen von Personendaten ausreichen soll, ändert daran nichts. Denn zum einen wird diese Auffassung von anderen Autoren mit überzeugenden Argumenten abgelehnt. Zum anderen ergibt sich eine derart strenge Auslegung auch nicht aus dem E-SEV 108, weshalb keine Notwendigkeit besteht, sie im Schweizer Recht einzuführen.
SDV	3 lit. f	Der **Begriff des Profiling** ist nach der vorgeschlagenen Regelung **untauglich und realitätsfremd**. Hier sind Konkretisierungen und Beispiele angezeigt, damit Klarheit herrscht, welche konkreten Tätigkeiten als Profiling zu betrachten sind.

SDV	4 Abs. 6	**Die vorgeschlagene Änderung hinsichtlich des Begriffs der „Einwilligung" ist unter Einbezug des erläuternden Begriffs unklar**. Gemäss erläuterndem Bericht (S. 47) ermöglicht die Neuformulierung eine terminologische Annäherung an die DSGVO. Es wird allerdings nicht klargestellt, ob damit eine inhaltliche Annäherung bezweckt wird. **Die Definition ist nicht nur, aber in besonders ausgeprägter Form gerade für die Werbebranche von fundamentaler Bedeutung, weshalb eine klare Regelung und damit Rechtssicherheit erforderlich ist.** Die Übernahme der Vorgaben der EU-DSGVO in Bezug auf die „Freiwilligkeit der Einwilligung" (Art. 7 Abs. 4) hätte jedenfalls eine massive Verschärfung der Rechtslage gegenüber dem geltenden Recht sowie eine erhebliche Beschränkung der Vertragsfreiheit zur Folge, die unnötig und daher abzulehnen ist. **Der E-SEV 108 (Art. 5 Abs. 2) verlangt denn auch lediglich, dass die Einwilligung freiwillig sein muss („free consent"), ohne eine derart strenge Interpretation, wie sie die EU-DSGVO enthält, vorzuschreiben.** In der Botschaft muss deshalb eine entsprechende Klarstellung aufgenommen werden. Darüber hinaus sind die Ausführungen im erläuternden Bericht zur „ausdrücklichen Einwilligungen" unklar bzw. unvollständig. Es geht daraus letztlich nicht hervor, welche Anforderungen konkret an eine solche Einwilligung gestellt werden, was gerade aufgrund des (noch) übermässig weit gefassten Begriffs des Profiling und dessen Bedeutung für die Werbebranche besonders problematisch ist. **Es ist daher in der Botschaft auch klar zu stellen, dass – wie nach geltendem Recht – eine Einwilligung dann ausdrücklich ist, wenn die Datenbearbeitung, in welche eingewilligt wird, also z.B. das Profiling bspw. in der Datenschutzerklärung beim Namen genannt wird und es insofern nicht genügen würde, wenn bloss aus den Umständen auf ein Profiling geschlossen werden müsste**. **Schliesslich ist in der Botschaft auch festzulegen, dass – entsprechend dem geltenden Recht – eine Einwilligung auch zu einem Dokument, das weitere Informationen erhält (wie z.B. AGB oder Datenschutzerklärungen), erteilt werden kann und keine separate Information bzw. Einwilligung erforderlich ist.**
SDV	8	**Es muss zumindest in der Botschaft klargestellt werden, wer zu den interessierten Kreisen gehört**. So sollte insbesondere eine Mitwirkung von Konsumentenverbänden ausgeschlossen werden, da deren Interessen bereits durch den Genehmigungsvorbehalt des EDÖB ausreichend berücksichtigt werden. **Sodann ist ein Rechtsmittel gegen die Genehmigungsentscheide vorzusehen.** Zur Klärung der Rechtslage in Bezug auf die Rechtsmittel (insb. Legitimation) gegen einen Entscheid über die Genehmigung von Empfehlungen sind hier zumindest Erläuterungen in der Botschaft angezeigt. Die Rechtsmittel, welche allgemein auch im E-SEV 108 verlangt werden (Art. 12bis Abs. 6), sind umso mehr von Bedeutung, als aufgrund der Pflicht zur Genehmigung durch den EDÖB zu erwarten ist, dass mit den Empfehlungen ein über die gesetzlichen Vorgaben hinausgehender Standard gesetzt wird. Dieser wird letztlich auch trotz der expliziten Regelung in Art. 9 Abs. 2 VE-DSG faktisch zum Gesetz werden. Folglich muss eine klare Regelung bestehen, die es den betroffenen Verbänden bzw. Unternehmen ermöglicht, die Nicht-Genehmigung bzw.

		Ablehnung einer Empfehlung, die den gesetzlichen Vorgaben entspricht, gerichtlich anzufechten.
SDV	13	Nach der vorgeschlagenen Regelung ist unklar, inwiefern die Informationspflicht auch gilt, wenn nachträglich neue Bearbeitungszwecke hinzukommen oder andere Bearbeitungen an die Stelle der ursprünglichen treten. Diesbezüglich ist zumindest in der Botschaft eine Klarstellung erforderlich, dass nur über das informiert werden muss, was schon zum Zeitpunkt der Beschaffung feststand. Denn in solchen Fällen wäre in der Regel ohnehin eine Einwilligung oder ein anderer Rechtfertigungsgrund erforderlich und eine Sanktionsbewehrung folglich unverhältnismässig. Zudem müsste klargestellt werden, dass – entsprechend der geltenden Rechtslage und der Praxis des EDÖB – bei der Beschaffung grundsätzlich ein Verweis auf die auf der Website enthaltenen Detailinformationen ausreicht. Die Erwägung im erläuternden Bericht, wonach es nicht genügt, wenn die betroffene Person nach den Informationen suchen muss, sollte deshalb zumindest im Rahmen der Botschaft in diesem Sinne präzisiert werden. Hinsichtlich des Zeitpunkts der Information ist für den Online-Kontext eine Klarstellung erforderlich. Denn beim Zugriff auf eine Website wird regelmässig eine Bearbeitung von IP-Adressen erfolgen (Erfassung in Log-Datei, Zählung der Website-Zugriffe etc.) und dies in der Regel bereits bevor der Nutzer allfällige Informationen hierzu z.B. in einer Datenschutzerklärung zur Kenntnis nehmen kann. Aufgrund der Tatsache, dass IP-Adressen je nach Einzelfall Personendaten darstellen können und dass eine vorgängige Information hier technisch grundsätzlich nicht möglich ist, muss klargestellt werden, dass die ausreichend kenntlich gemachte Information in einer Datenschutzerklärung nach Abruf der Website als rechtzeitig gilt.
SDV	15	Hier muss klargestellt werden, dass auch „rechtliche Auswirkungen“ eine gewisse Schwere aufweisen müssen.
SDV	18	Hier muss den Datenbearbeitern im Sinne der „Business Judgement Rule“ ein gewisser Ermessensspielraum eingeräumt werden. In der Botschaft ist dies klarzustellen.
SDV	23 Abs. 3	Die Erwägung im erläuternden Bericht, wonach die Regelung nur zum Tragen komme, wenn die Bearbeitung dieser Daten auch rechtmässig erfolgt (S. 69), ist unzutreffend und daher in der Botschaft klar zu stellen.
Fehler! Verweisquelle konnte nicht gefunden werden.	24 Abs. 2	Der SDV fordert sodann, dass entsprechend der EU-DSGVO (Erw.-Gr. 47) zumindest in der Botschaft darauf hinzuweisen ist, dass die Bearbeitung von Personendaten zum Zwecke der Direktwerbung ein überwiegendes Interesse darstellen kann.
Fehler! Verweisquelle	50 ff	**Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen**

konnte nicht gefunden werden.		**Personen abstellt, wird strikt abgelehnt**. Dieses vorgesehene Sanktionssystem steht der Digitalen Strategie der Schweiz diametral entgegen. Es ist in höchstem Mass innovationshemmend und etabliert eine Kultur des Denunziantentums in den Unternehmen. Es führt zu einem ganz erheblichen Standortnachteil der Schweiz. Kein innovatives digitales Start-Up wird bereit sein, seine Gründer und Mitarbeiter solch drastischen strafrechtlichen Risiken auszusetzen. Gute Mitarbeiter werden nicht mehr bereit sein Verantwortung in den Unternehmen mitzutragen. Insbesondere aufgrund der vorgesehenen Strafbarkeit fahrlässigen Verhaltens wird potentiell jeder Mitarbeiter durch heute alltägliche Verrichtungen am Arbeitsplatz ständig Gefahr laufen, sich strafbar zu machen. Dies ist auch gesellschaftspolitisch komplett inakzeptabel. Gleichzeitig ist es gegenüber Datenbearbeitungen durch ausländische Unternehmen faktisch nicht durchsetzbar, was sodann einerseits den Datenschutz in der Schweiz nicht erhöht und andererseits ausländischen Unternehmen einen immensen Wettbewerbsvorteil verschafft. Sodann würde die Schweiz damit gegenüber der EU in diesem grundlegenden Punkt einen Sonderweg einschlagen. Selbst wenn gemäss dem E-SEV 108 nicht zwingend administrative Bussen verlangt werden, wird gleichwohl eine unnötige Unsicherheit im Hinblick auf die Beurteilung der Angemessenheit des Schweizer Datenschutzrechts geschaffen. Ferner wird die Abweichung wie erwähnt international aber auch schon im europäischen Kontext zu vollstreckungsrechtlichen Schwierigkeiten führen (Stichwort: Voraussetzung der doppelten Strafbarkeit), was letztlich zu einer Bevorzugung von ausländischen Unternehmen gegenüber den einheimischen führt. **In jedem Falle wird die vorgeschlagene Regelung aber auch die für die Schweizer Wirtschaft zentralen Verhandlungen zwischen der Schweiz und der EU über die Koordinierung der Anwendung des jeweiligen Datenschutzrechts und die Abgrenzung der Zuständigkeit der Aufsichtsbehörden (Motion Fiala, 16.3752) erheblich erschweren.** Es erscheint gänzlich unrealistisch, dass die EU eine entsprechende Vereinbarung abschliesst, wenn in der Schweiz Unternehmen, die Datenschutzverletzungen gegenüber EU-Bürgern begehen, nur in Ausnahmefällen bzw. nach Ermessen der Untersuchungsbehörden verfolgt werden können. Darüber hinaus greift auch die Begründung „mit Blick auf die Kosten“ im erläuternden Bericht viel zu kurz. Die Kosten werden mit der vorgeschlagenen Regelung lediglich auf die kantonalen Strafbehörden übertragen. Es ist nicht ersichtlich, inwiefern sich diese hierdurch verringern sollten. Im Gegenteil ist ein solches **System ineffizient und wird gesamtwirtschaftlich deutlich höhere Kosten verursachen**, da neben dem Verwaltungsverfahren des EDÖB bei Verdacht auf strafrechtlich relevante Verhaltensweisen ein zusätzliches Strafverfahren mit neuerlichen Untersuchungsmassnahmen durchzuführen ist. Der gleiche Fall müsste folglich zweimal untersucht werden. Dies würde auch für die Unternehmen zu einem nicht vertretbaren und unnötigen Mehraufwand führen. **Schliesslich ist auch die primäre strafrechtliche Sanktionierung der natürlichen Personen an sich unverhältnismässig und**

		mit Blick auf den Datenschutz nicht zielführend. Die betroffenen Mitarbeiter würden durch das Risiko einer strafrechtlichen Verurteilung massiv unter Druck gesetzt. Namentlich bei Kenntnis einer Verletzung müssten sie entweder den zuständigen Mitarbeiter denunzieren oder würden sich andernfalls unter Umständen gar selbst strafbar machen. Ferner besteht die Gefahr, dass Unternehmen nach Möglichkeit einen unliebsamen Mitarbeiter im Sinne eines „Bauernopfers" für den massgeblichen Verstoss als zuständig bezeichnen und sich so letztlich aus der Verantwortung nehmen können. **Zudem würde gerade die Position von betrieblichen Datenschutzverantwortlichen, die eigentlich zur Erhöhung des Datenschutzes beitragen sollten, mit dem vorgeschlagenen System erheblich geschwächt.** Statt der Förderung des betrieblichen Datenschutzes würde damit eine Kultur der Verschleierung geschaffen. Insbesondere in kleineren Unternehmen, in welchen die zuständige Person einfacher ausfindig zu machen ist, dürfte kaum mehr jemand bereit sein, eine entsprechende Stelle, resp. die entsprechende Verantwortung zu übernehmen. **Geradezu absurd erscheint die Schärfe des vorgeschlagenen Sanktionssystems, wenn man bedenkt, dass damit ausgerechnet der materielle Kern eines wirksamen Datenschutzes, nämlich die Beachtung der Bearbeitungsgrundsätze, nicht sanktionsbedroht sein soll**. Dies im Übrigen natürlich zu Recht. Spätestens in diesem Zusammenhang wird nämlich klar, dass sich das Strafrecht als disziplinierendes Instrument in diesem Bereich nicht eignet. In einem Rechtsstaat kann ein Verhalten nur strafbar sein, wenn der zugrundeliegende Tatbestand eindeutig bestimmt ist. Gerade dies ist aber im Bereich des Datenschutzes in den meisten Fällen nicht der Fall: wie soll ein Mitarbeiter voraussehen können, ob die mit einer Bearbeitung verbundenen Risiken genügend „erhöht" sind, um damit die strafrechtlich sanktionierte Pflicht einer Risiko-Folgenabschätzung im Sinne von Art. 16 VE-DSG auszulösen? **Vor diesem Hintergrund sind anstelle von Strafsanktionen verwaltungsrechtliche Bussen einzuführen.** Für Binnensachverhalte ist es allerdings nicht angezeigt, die Bussenrahmen der EU-DSGVO zu übernehmen. Hier genügen tiefere Maximalsanktionen. Mit Blick auf eine allfällige Koordinations-Vereinbarung mit der EU sollten die Obergrenzen für Verstösse, die den EU-Markt betreffen, allerdings höher ausfallen. Der SDV schliesst sich der Forderung der economiesuisse nach einem Sanktionssystem entsprechend den folgenden Grundsätzen an: Die Sanktionen sollen sich primär an die Unternehmen richten und verwaltungsrechtlicher Natur sein. Eine Sanktionierung von Mitarbeitenden ist nur für Fälle von direkt vorsätzlichen Verstössen vorzusehen, in welchen sich das Handeln des Mitarbeiters gegen die Interessen des Unternehmens oder der betroffenen Person richtet. Der Kreis der potentiell verantwortlichen Mitarbeitenden muss dabei klar definiert und angemessen eingeschränkt werden.

		Des Weiteren ist der Strafkatalog anzupassen. Dieser darf in keinem Fall über die EU-DSGVO hinausgehen. Zu offen formulierte Tatbestände sind dabei entweder aus dem Katalog zu entfernen oder zu konkretisieren. Zudem ist eine Erheblichkeitsschwelle einzuführen, die sich an der Schwere der Persönlichkeitsverletzung oder an der Höhe des entstandenen Schadens orientiert. Auf die Sanktionierung von fahrlässig begangenen Verstössen ist zu verzichten. Schliesslich ist auch kooperatives Verhalten durch geeignete Anreize zu fördern, indem Sanktionen bei Vorliegen von schadensminderndem Verhalten wegfallen oder zumindest reduziert werden. Im Übrigen verweisen wir auf die ausführliche Stellungnahme der economiesuisse in deren Vernehmlassungsantwort.
Fehler! Verweisquelle konnte nicht gefunden werden.	Seite 64	Datenschutzfreundliche Voreinstellungen 1. Wir sind nicht einverstanden mit der Feststellung, dass das Anlegen eines Benutzerkontos schon zu einer umfassenderen Bearbeitung von Personendaten führt. Jede Online-Bestellung führt zu einem Zusammenführen von Einkaufshistorie und Kunde, das Anlegen eines Benutzerkontos oder Benutzerprofils ist eine reine administrative Tätigkeit, welche nicht zwingend zu umfassenderen Daten führt! 2. Nicht eingegangen wird hier auf das Thema Cookies / Nachverfolgung von Kundenbewegungen.
Fehler! Verweisquelle konnte nicht gefunden werden.	Seite 88	Übergangsbestimmungen Die Übergangsbestimmungen müssen insbesondere für Altdaten ergänzt worden. Es ist ausdrücklich festzuhalten, dass Personendaten, die unter dem alten Recht rechtmässig erhoben und bearbeitet wurden, im entsprechenden Umfang auch unter dem neuen Recht weiterhin bearbeitet werden dürfen. Schlussendlich ist eine angemessene Übergangsfrist von mindestens zwei Jahren für die Umsetzung aller neuen Pflichten unter dem Gesetz vorzusehen um den Unternehmen die Umstellung ihrer Prozesse zu ermöglichen. Eine entsprechende Übergangsfrist hat auch die EU-DSGVO nach ihrem Inkrafttreten vorgesehen. Diese wird im Frühling 2018 auslaufen.

Amstutz Jonas BJ

Von: Patricia Feubli <patricia.feubli@semsea.ch>
Gesendet: Mittwoch, 29. März 2017 15:19
An: Amstutz Jonas BJ
Cc: Mike Wieland
Betreff: Vernehmlassungsantwort zum Entwurf des neuen Datenschutzgesetzes
Anlagen: Vernehmlassungsantwort_SEMSEA.DOC

Sehr geehrter Herr Amstutz

Da die SEMSEA Suchmaschinenmarketing AG mit ihrer Data Science-Abteilung direkt von der Neuregelung des Datenschutzes betroffen ist, bringen wir uns aktiv in die politische Diskussion ein. Gerne sende ich Ihnen deshalb unsere Vernehmlassungsantwort zum Entwurf des neuen Datenschutzgesetzes.

Wir haben für unsere Antwort die unveränderte Word-Vorlage verwendet und hoffen, dass Sie das Dokument problemlos öffnen und lesen können.

Besten Dank und freundliche Grüsse

Patricia Feubli

……...
Dr. Patricia Feubli · Data Scientist
Economics PhD

SEMSEA Suchmaschinenmarketing AG
ADS & ADWORDS / DATA SCIENCE
Zürich | Salzburg | Hamburg
Schulhausstrasse 41
8002 Zürich

Fon: +41 44 520 33 88
Fax: +41 44 515 33 20

http://www.semsea.ch

……...

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : SEMSEA Suchmaschinenmarketing AG

Abkürzung der Firma / Organisation : SEMSEA

Adresse : Schulhausstrasse 41, 8002 Zürich

Kontaktperson : Dr. Patricia Feubli

Telefon : 044 520 33 88

E-Mail : patricia.feubli@semsea.ch

Datum : 29. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SEMSEA	Grundsätzlich begrüssen wir die angestrebte Modernisierung des Datenschutzrechts und die gesetzliche Annäherung an die Rechtslage in der EU. Für uns als Schweizer KMU ist es zentral, dass bezüglich des Datenschutzes Rechtssicherheit für unsere wirtschaftliche Tätigkeit geschaffen wird. Gerade als KMU ist es für uns jedoch ebenfalls zentral, dass die administrativen Kosten der Neuregelungen auf das absolut Notwendige reduziert werden. Das neue Datenschutzrecht muss einfach nachzuvollziehen sowie die Umsetzung kostengünstig sein. Denn die Regulierungskosten sind für uns als KMU bereits heute sehr hoch, eine weitere Steigerung dieser Kosten können wir nur sehr schwer verkraften. Ausserdem dürfen durch das neue Datenschutzrecht keine zusätzlichen Standortnachteile für uns Schweizer KMU entstehen. Wir lehnen den vorliegenden Entwurf des neuen Datenschutzgesetzes ab und schlagen eine grundlegende Überarbeitung der unten aufgeführten Artikel vor. Wir lehnen insbesondere die Definition von Profiling in Artikel 3, den schwammigen Begriff „interessierte Kreise“ (Artikel 8), die Pflicht zur Datenschutz-Folgeabklärung bei „erhöhtem“ Risiko (Artikel 16) und das vorgeschlagene Sanktionssystem ab (Artikel 50-55). Gerne verweisen wir auch auf die Stellungnahme des Schweizer Dialogmarketing Verbands (SDV), die wir unterstützen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SEMSEA	DSG	3		f	Wir lehnen die Definition von Profiling ab. Sie ist sehr breit gefasst und beinhaltet sogar nicht personenbezogene Daten. Eine solch breite Definition wird dazu führen, dass ein Grossteil der möglichen Datenauswertungen als Profiling zu verstehen ist. Mit dem Profiling einhergehende Regelungen müssen dementsprechend auf einen Grossteil der möglichen Datenauswertungen angewendet werden. Dies ist eine unnötige Verschärfung der Gesetzgebung. Zudem enthält der E-SEV 108 keine Vorgaben für das Profiling. Eine Profiling-Regelung in der Schweiz bringt Standortnachteile für uns als in der Schweiz ansässiges KMU mit sich.
SEMSEA	DSG	4	5		Der Begriff „unvollständige“ muss gestrichen werden. Es gibt keinen Grund, Personendaten in jedem Fall vollständig zu führen. Zudem ist es in der Regel nicht möglich oder sehr schwierig, fehlende Personendaten zu ergänzen. Eine entsprechende Verpflichtung wäre nicht erfüllbar.
SEMSEA	DSG	4	6		Dieser Absatz muss klarer formuliert werden. Für uns ist nicht ersichtlich, was unter angemessener Information, eindeutiger und ausdrücklicher Einwilligung zu verstehen ist und welche Anforderungen an diese drei Begriffe gestellt werden. Je nach Anforderung ist die neue Gesetzgebung eine deutliche Verschärfung gegenüber der bestehenden, insbesondere im Bereich Profiling.
SEMSEA	DSG	7	2		Wir lehnen den Zusatz „Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters“ ab. Die Pflichten der Auftragsbearbeiter müssen im Rahmen des Datenschutzgesetzes geregelt werden. Eine separate Regelung kann zu einer deutlichen Überregulierung für Auftragsbearbeiter führen.
SEMSEA	DSG	8			Der Begriff „interessierte Kreise“ ist nicht klar definiert. Es muss festgelegt werden, wer zu den interessierten Kreisen zählt, denn diese üben einen massgebenden Einfluss auf die Empfehlungen der guten Praxis aus. Ohne eine klare Festlegung besteht eine grosse Unsicherheit bezüglich Ausgestaltung der Empfehlungen der guten Praxis.

					Es ist zudem nicht klar, wie die Empfehlungen zu handhaben sind. Aus dem Artikel muss hervorgehen, welche Konsequenzen ein Nichteinhalten der (oder einiger) Empfehlungen hat. Es braucht hier eine klare Regelung der Rechtslage und der Rechtsmittel.
SEMSEA	DSG	13			Hier ist nicht klar, was unter „Informationspflicht“ verstanden wird. Als KMU sind wir darauf angewiesen, dass der Verweis auf die auf der Webseite enthaltenen Detailinformationen zur Beschaffung von Personendaten ausreicht. Alles andere übersteigt unsere Kapazitäten.
SEMSEA	DSG	13	2		Problematisch ist die Regelung „spätestens bei der Beschaffung“. Insbesondere im Onlinebereich werden häufig Daten erhoben, bevor ein Unternehmen die Möglichkeit hat, die betroffene Person über die Beschaffung zu informieren. Ein Beispiel hierzu sind Google AdWords-Kampagnen. Klickt eine Person auf eine AdWords-Anzeige, wird dieser Klick gespeichert und für das Unternehmen sichtbar. Das Unternehmen hatte jedoch noch keine Möglichkeit, die Person über die Speicherung des Klicks zu informieren. Würde der vorliegende Artikel Gesetz, wäre Werbung im Online-Such- und Displaynetzwerk praktisch unmöglich. Deshalb muss hier festgelegt werden, dass die klar ersichtliche Information in der Datenschutzerklärung nach Aufruf der Webseite als rechtzeitig gilt.
SEMSEA	DSG	13	4		Dieser Absatz ist ersatzlos zu streichen, da er keinerlei Mehrwert bringt. Der Auftragsbearbeiter darf gemäss Artikel 7 Bst. a nur so bearbeiten, wie der Verantwortliche selbst es tun dürfte. Es besteht deshalb kein Grund zur Informationspflicht gegenüber der betroffenen Person.
SEMSEA	DSG	16			Dieser Artikel muss angepasst werden. Da der Artikel völlig offenlässt, was unter einem „erhöhten Risiko“ zu verstehen ist, müssten wir für jede vorgesehene Datenbearbeitung eine Datenschutz-Folgeabschätzung durchführen, um uns abzusichern. Dieser enorme Aufwand können wir als KMU nicht bewältigen. Deshalb muss im Artikel festgehalten werden, dass nur bei sehr hohem Risiko eine Datenschutz-Folgeabschätzung vorgenommen werden muss. Ausserdem muss klar definiert werden, was unter „Risiko“ verstanden wird.
SEMSEA	DSG	17	1		Der Begriff „unbefugte Datenbearbeitung“ ist extrem breit gefasst und muss zwingend eingeschränkt werden. Wird Artikel 17 gesetzlich verankert, müsste womöglich bereits das Öffnen eines Daten-Excel-files durch Unbefugte dem Beauftragten gemeldet werden. Das ist unverhältnismässig.

SEMSEA	DSG	19		a	Dieser Artikel ist zu breit gefasst. Wird eine umfassende Dokumentation zu den Datenbearbeitungen gefordert, entsteht ein massiver zusätzlicher Aufwand, für die wir als KMU keine Kapazitäten haben. Die Dokumentation zu den Datenbearbeitungen muss schlank und für KMU umsetzbar bleiben.
SEMSEA	DSG	20	1		Der Begriff „kostenlos“ ist ersatzlos zu streichen. Zum einen kann es sehr aufwändig sein zu prüfen, ob Daten von einer Person bearbeitet werden. Insbesondere, wenn keine zentrale Datenbank vorhanden ist und Daten an unterschiedlichen Orten mit unterschiedlichen Zugriffsberechtigungen gespeichert werden. Zum anderen kann eine hohe Nachfrage nach solchen Auskünften dazu führen, dass ein Unternehmen zusätzliche Ressourcen für die Bearbeitung der Auskunftsanfragen zur Verfügung stellen muss. Ohne eine angemessene Aufwandsentschädigung kann dies rasch zu einer existentiellen Bedrohung für ein KMU werden.
SEMSEA	DSG	23		d	Diese Bestimmung ist zu streichen. Zum einen ist der Begriff Profiling sehr breit gefasst, wodurch dieser Begriff sich auf einen Grossteil der Datenanalysen anwenden lässt (siehe unsere Bemerkungen zum Artikel 3 Bst f). Damit würde auch ein Grossteil der Datenanalysen der ausdrücklichen Einwilligung unterliegen. Dies ist eine äusserst starke Verschärfung gegenüber den Richtlinien der EU und würde bei gesetzlicher Verankerung zu einem massiven Standortnachteil für Schweizer Unternehmen führen. Zudem lässt der Artikel völlig offen, wie eine ausdrückliche Einwilligung definiert ist. Somit ist nicht klar, wann eine Datenauswertung bzw. ein Profiling eine Persönlichkeitsverletzung darstellt und wann nicht.
SEMSEA	DSG	44	3		Wir lehnen diese Regelung ab. Die korrekte Handhabung und Auswertung von Daten erfordert in der Regel eine kontinuierliche Datenbearbeitung. Muss diese Datenbearbeitung während eines Verwaltungsverfahrens eingestellt werden, entstehen grosse Datenlücken, die im Nachhinein nicht mehr geschlossen werden können. Dies ist insbesondere dann mit grossen (finanziellen und wirtschaftlichen) Schäden verbunden, wenn sich der Verdacht gegen Personen oder Bundesorgane im Verwaltungsverfahren nicht erhärten lässt und die Datenbearbeitung nach dem Verfahren wieder fortgeführt werden kann. Beschwerden gegen vorsorgliche Massnahmen müssen deshalb eine aufschiebende Wirkung haben.
SEMSEA	DSG	50-55			Wir lehnen das vorgeschlagene Sanktionssystem, das vorwiegend die strafrechtliche Verfolgung von natürlichen Personen vorsieht, strikt ab. Dieses Sanktionssystem führt dazu, dass keine qualifizierten

					Mitarbeiterinnen und Mitarbeiter mehr bereit sein werden, Datenbearbeitungen und Datenanalysen vorzunehmen. Da inzwischen unzählige Berufsbilder und Arbeitsgebiete mit Daten in Berührung kommen, werden praktisch alle Mitarbeiterinnen und Mitarbeiter dem Risiko ausgesetzt sein, sich strafbar zu machen. Das ist inakzeptabel. Zudem würde dieses Risiko die Transparenz in der Datenverwendung und den Datenschutz schwächen, stattdessen würden Verschleierungstaktiken zunehmen. Das vorgeschlagene Sanktionssystem würde massive Standortnachteile mit sich ziehen und zu Abwanderungen von Unternehmen ins Ausland führen. Anstelle der Strafsanktionen für natürliche Personen schlagen wir die Einführung von verwaltungsrechtlichen Bussen vor.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")		
Name/Firma	**Kapitel-Nr.**	**Bemerkung/Anregung**

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"		
Name/Firma	**Art.**	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.		

SGB | USS
www.sgb.ch | www.uss.ch
Schweizerischer Gewerkschaftsbund
Union syndicale suisse
Unione sindacale svizzera

Bundesamt für Justiz

jonas.amstutz@bj.admin.ch

Bern, 07. April 2017

Vernehmlassungsverfahren: Totalrevision des Datenschutzgesetzes (DSG)

Sehr geehrte Damen und Herren

Besten Dank für die Möglichkeit, an der oben genannten Vernehmlassung teilnehmen zu dürfen.

Grundsätzliches

Die vielen Anfragen sowohl an die Rechtsdienste der Gewerkschaften wie auch an den Eidg. Datenschutzbeauftragten (EDÖB)[1] zeigen, dass sehr häufig weder den Arbeitgebern noch den Arbeitnehmern klar ist, was wirklich zulässig ist. Das hat u.a. mit der wenig klaren Sprache des heutigen DSG zu tun. Leider verpasst es die nun vorliegende Totalrevision, klare und spezifische Bestimmungen für Arbeitgeber und Arbeitnehmende zu erlassen. Damit hat es der Gesetzgeber verpasst, Rechtssicherheit in diesem Bereich zu schaffen.

Der SGB fordert deshalb im Rahmen der Überarbeitung der Vorlage, den Datenschutz am Arbeitsplatz spezifischer zu regeln bzw. beispielhaft anzugeben, welche Artikel am Arbeitsplatz wie umgesetzt werden müssen. Insbesondere müssen für die Videoüberwachung, Internet- und Email- sowie Telefonüberwachung klare Vorgaben im Gesetz gemacht werden. Aber auch neue Formen der möglichen (Big-Data-)Überwachung wie z.B. der “refraktiven Überwachung” von Arbeitnehmenden.[2] Somit würde auch gesetzessystematisch Kongruenz zwischen dem DSG und Art. 26 der Verordnung 3 zum Arbeitsgesetz (ArGV3) hergestellt werden.

Grundsätzlich muss ein revidiertes DSG auch die Datenhoheit der Arbeitnehmenden statuieren – auch dies ist in der Überarbeitung der Vorlage nachzuholen. Jeder Arbeitnehmende muss das Recht haben, über das Erheben der persönlichen Daten proaktiv informiert zu werden und dieses einzuschränken sowie zu bestimmen, was die Unternehmen mit seinen persönlichen digitalen Daten machen dürfen und was nicht.

[1] Vgl. bspw. Tätigkeitsbericht EDÖGB
https://www.edoeb.admin.ch/dokumentation/00153/00154/00165/index.html?lang=de
[2] Zur refraktiven Datenüberwachung am Arbeitsplatz vgl. statt vieler https://hbr.org/2016/08/the-unintended-consequence-of-customer-data-collection .

Monbijoustrasse 61, 3007 Bern / Postfach, 3000 Bern 23
031 377 01 01, Fax: 031 377 01 02, info@sgb.ch, info@uss.ch

123 LC/jh/rk

Zu den einzelnen Artikeln

Art. 2 – Räumlicher und persönlicher Geltungsbereich

Der vorliegende Entwurf zum revidierten Datenschutzgesetz (DSG) sieht keine besondere Bestimmung zum räumlichen Geltungsbereich vor. Nach Auffassung des Bundesrates würde bereits das geltende Recht die Möglichkeit bieten, das Gesetz weitgehend auf Situationen mit internationalem Charakter anzuwenden. Er verweist hierzu auf das Bundesgerichtsurteil zu "Google Street View". In diesem Urteil ist, wie vom Bundesrat erwähnt, ein überwiegender Anknüpfungspunkt in der Schweiz gegeben, da Google Inc. mit Hilfe von Google Switzerland GmbH Bilder von Strassenzügen in der Schweiz aufnehmen liess. Diese Situation ist jedoch nicht mit Datenbearbeitern und Inhabern von Datensammlungen – nach heutiger Terminologie – vergleichbar, die komplett aus dem Ausland operieren, sich aber an Arbeitnehmende in der Schweiz richten. Zu erwähnen sind etwa Plattformen wie Amazon Turk, Uber oder andere Arbeitgeber im Bereich spezifischer Telearbeitsformen. Es ist hier aber auch an Tools zu denken, die im Arbeitsverhältnis, z.B. im Büro, zum Einsatz kommen, und die ebenfalls komplett aus dem Ausland operieren: Bspw. Amazon Web Services, Skype, Google Docs, Microsoft (unter anderem mit Office 365), Salesforce, etc.

In all diesen Fällen kann das schweizerische Datenschutzgesetz weiterhin nicht ohne Weiteres angewendet werden. Die Auffassung des Bundesrates, das geltende Recht biete bereits die Möglichkeit, das DSG weitgehend auf Situationen mit internationalem Charakter anzuwenden, lässt sich denn auch in der gängigen Praxis nicht nachvollziehen. Ein entsprechendes Marktortprinzip muss daher vorgesehen werden.

Der vorliegende Entwurf weist eine grosse Neuerung beim persönlichen Geltungsbereich auf: Der Schutz juristischer Personen fällt weg. Erfasst sein soll neu nur noch die Bearbeitung von Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Der SGB ist damit nicht einverstanden. Die Geschichte zeigt, dass auch juristische Personen wie Gewerkschaften oder Vereine Opfer zweifelhafter Datenbearbeitung sein können. Der Ausschluss der juristischen Personen vom Schutzbereich des DSG ist auch weder systemtreu noch wirklich konsequent. Nach Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB), welcher durch das DSG konkretisiert wird, geniessen auch juristische Personen Persönlichkeitsschutz, und sie tun es weiterhin; Art. 13 der Bundesverfassung (BV) gewährleistet den Schutz der Persönlichkeit auch von juristischen Personen. Diesen soll u.E. deshalb ein eigenständiger Schutz sowie Aktivlegitimation zustehen. Es muss deshalb auch juristischen Personen der Schutz des Gesetzes gewährt werden.

Art. 3 – Begriffe

Die Streichung des Begriffs und des Konzepts der "Datensammlung" wird ausdrücklich begrüsst. Entscheidend ist die Erschliessbarkeit der Daten: Alle Informationen über eine bestimmte Person, die mit einem vernünftigen Aufwand gefunden werden können, müssen als personenbezogene Daten gelten – unabhängig vom Speicherverfahren oder dem Speicherort.

Ebenfalls scheint begrüssenswert, dass der Begriff "Persönlichkeitsprofil" durch "Profiling" ersetzt wird. Die Begriffe sind allerdings nicht deckungsgleich. Wichtig ist, dass der Zweck der Datenbearbeitung durch den Begriff erfasst bleibt, der darauf abzielt, wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Der SGB begrüsst grundsätzlich den vorliegenden Ersatz des bis heute unklaren Begriffs des "Persönlichkeitsprofils" (als "gefähr-

liche" Art von Daten) durch das "Profiling" (als "gefährliche" Art des Bearbeitens von Daten). Jedoch ist es ungenügend, wenn dann im bereichsspezifischen Datenschutzrecht (in den anzupassenden Bundesgesetzen) mit Blankettermächtigungen das Profiling quasi "durchgewinkt" wird. Zu fordern ist, dass klare und strenge Rahmenbedingungen für das Profiling in den Bundesgesetzen konkretisiert werden, insbesondere für das Profiling von Arbeitnehmenden durch den Arbeitgeber.

Der Begriff des Profiling muss nämlich sowohl traditionelle wie auch neuartige mögliche Formen der unerwünschten Überwachung am Arbeitsplatz beinhalten, welche z.B. durch Auswertung von Big Data und anderen Datenvolumen am Arbeitsplatz anfallen.

Weiter ist auch der Begriff der "biometrischen Daten" missverständlich. Auch in den Erläuterungen wird er nicht geklärt: Ein Gesichtsbild oder die Stimme sind grundsätzlich auch "biometrisches Daten", sollen aber hier nicht als Unterkategorie der besonders schützenswerten Personendaten erfasst werden. Deshalb ist die folgende Definition aufzunehmen:

"Ziff. 4. mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten)".

Weiter lassen biometrische Merkmale nicht immer eine eindeutige Identifizierung zu. Zudem werden die Möglichkeiten zur automatisierten Erkennung von Personen aufgrund ihrer Stimme, dem Aussehen oder der Art der Fortbewegung noch massiv zunehmen und sind heute schon am Arbeitsplatz gang und gäbe und sehr problematisch: So werden in der Logistik Bewegungsmuster von Logistik-Mitarbeitern oder Kurieren automatisch gespeichert und dem Arbeitgeber in Echtzeit übermittelt; oder automatische, durch Algorithmen ausgeführte Stimmkontrollen in Callcentern gemacht. Wenn folglich biometrische Merkmale zur Identifizierung geeignet sind oder zur Identifikation, zur Messung der Abläufe bzw. gar zur Bewertung der Mitarbeitenden bearbeitet werden, müssen sie als besonders schützenswerte Personendaten gelten.

Das Wort "eindeutig" ist daher zu streichen.

Art. 4 Abs. 2 – Verhältnismässigkeit

"Datenvermeidung" und "Datensparsamkeit" fehlen als explizite Grundkonzepte und als Teil der notwendigen Verhältnismässigkeit (s. Art. 4 Abs. 6). Gerade Arbeitgeber tendieren häufig dazu, unnötig Daten von Arbeitnehmenden zu sammeln, z.B. die Online-Tätigkeit im Home-Office, die je nach Verwendung des Computers oder bestimmter Programme dem Arbeitgeber mitgeteilt wird, ohne dass der Arbeitnehmende dies verhindern kann.

Der Absatz ist zu ergänzen mit: "Die Bearbeitung personenbezogener Daten sowie die Auswahl und Gestaltung der Datenbearbeitungssysteme sind dahingehend auszurichten, dass so wenig personenbezogene Daten wie möglich von der Bearbeitung betroffen sind."

Art. 4 Abs. 3 – Zweckbestimmung

Da die Weiterverarbeitung von Personendaten zu kompatiblen Zwecken erlaubt sein soll, muss der Zweck – wie im Vorentwurf vorgesehen – für die betroffene Person klar erkennbar sein.

An der Bestimmung soll – wie im Vorentwurf vorgesehen – festgehalten werden.

Art. 4 Abs. 6 – Einwilligung

Die Bestimmung ist nur zusammen mit den Grundsätzen der Datenvermeidung und der Datensparsamkeit wirksam. Dies zeigen aktuelle Beispiele:

Ein „Cookies-Balken" oder eine Kommunikations-Software auf einem portablen Computer, auf welchem der Arbeitnehmer z.B. auch von zuhause aus arbeitet, der nicht abgelehnt oder ausgeschaltet werden kann, ist für die betroffene Person inakzeptabel. Es muss jederzeit die Möglichkeit des Widerrufs einer Einwilligung gegeben sein. Zudem müssen gerade Personen in einem Abhängigkeitsverhältnis wie Arbeitnehmende vor unwillentlich abgegebenen und unverhältnismässigen Zustimmungen geschützt werden. Es darf nicht sein, dass Arbeitnehmende dem Arbeitgeber mit Pauschalvollmachten das Recht zur freien Überwachung geben. Dies gilt z.B. auch bei der Aufnahme in eine Kranken- oder Unfallversicherung oder Pensionskasse

An den Grundsätzen der Datenvermeidung und der Datensparsamkeit muss entsprechend festgehalten werden. Es darf auch nicht bereits davon ausgegangen werden, dass eine ausdrückliche Einwilligung vorliegt, wenn bspw. ein entsprechendes (Software-Dialog-)Kästchen – womöglich mit einer missverständlichen Beschriftung – bereits vorausgefüllt ist und auf die Schaltfläche "weiter" geklickt wird. Eine Verdeutlichung in Art. 4. Abs. 2 ist daher vorzunehmen.

Art. 8 – Empfehlungen der guten Praxis

Das Prinzip der "Empfehlungen der guten Praxis" wird begrüsst. Dieser Vorschlag ist insbesondere einer (alleinigen) Selbstregulierung durch die Branchen vorzuziehen, da erst der Einbezug interessierter und betroffener Kreise, d. h. sowohl der Anwender wie auch der Anbieter von Produkten und Dienstleistungen, zu angemessenen Regelungen der Empfehlungen der guten Praxis führen.

Art. 11 – Sicherheit von Personendaten

Der Artikel im Vorentwurf ist wie der bestehende Art. 7 DSG vage. Er hält insbesondere keine Schutzziele fest. Der SGB erwartet vom Bundesrat, dass die Schutzziele explizit im Gesetz zu erwähnen und die konkreten technischen Massnahmen in der Verordnung präzise vorzuschreiben sind.

Art. 15 Abs. 1 – Informationspflicht bei einer automatisierten Einzelentscheidung

Von Bedeutung ist diese Regelung vor allem im Privatrecht, also u.a. im Arbeitsrechtsverhältnis. Diese kann bei den oben erwähnten elektronischen bzw. Big-Data-Überwachungen zum Zuge kommen. Zum einen ist deshalb die Regelung (ohne Abs. 3) in den Abschnitt zum Datenbearbeiten durch Private zu verschieben.

Weiter ist zu befürchten, dass in der Praxis von einer Information über eine automatisierte Einzelentscheidung abgesehen werden dürfte, wenn eine rein theoretische Möglichkeit zur Einflussnahme besteht. Falls nicht, könnte sie gar zur Umgehung geschaffen werden.

In den nicht offensichtlichen Fehlbeurteilungen ist zudem nur die betroffene Person in der Lage, die Richtigkeit der automatisierten Einzelentscheidung abzuschätzen. Die Auswirkungen können aber dennoch erheblich sein. Das Wort "ausschliesslich" ist daher zu streichen.

Art. 15 Abs. 2 – Anhörungspflicht bei einer automatisierten Einzelentscheidung

Die betroffene Person muss sich nicht nur zur automatisierten Einzelentscheidung und den bearbeiteten Daten äussern können. Sie muss sich gegebenenfalls auch ein Bild des angewandten Verfahrens machen können. Da dies sinngemäss auch für das Profiling im Sinne von Art. 3 lit. f gelten muss, ist eine Regelung in der Auskunftspflicht nach Art. 20 vorzusehen.

Art. 16 – Datenschutz-Folgenabschätzung

Die Regelung der Datenschutz-Folgeabschätzung wird begrüsst. Dies entspricht dem gewählten, ausdrücklich risikobasierten Ansatz im revidierten DSG.

Art. 16 Abs. 5 (neu) – Periodische und rückwirkende Datenschutz-Folgenabschätzung

Eine einmalige Datenschutz-Folgeabschätzung ist in einem schnell ändernden Umfeld ungenügend. Es gilt explizit festzuhalten, dass diese periodisch oder bei Änderung der Risiken erneut vorzunehmen sei. Dies muss gerade angesichts der sich ständig ändernden digitalen Arbeitswelt gelten.

Art. 16 Abs. 1, 3, 4 sowie 5 (neu) – Datenschutz-Folgeabschätzung für Gesetzeserlasse i.V.m. Art. 59 lit. a

Nicht nur private Verantwortliche oder Bundesorgane sollen zu Datenschutz-Folgeabschätzungen verpflichtet werden. Bereits beim Erlass neuer Gesetze muss dem Datenschutz und dem Schutz der Persönlichkeitsrechte mehr Beachtung geschenkt werden. Entsprechend ist auch in diesen Fällen eine Datenschutz-Folgeabschätzung zu erstellen und bei Änderungen zu wiederholen.

Auch diese Datenschutz-Folgenabschätzungen müssen rückwirkend für bereits bestehende Gesetze (spätestens fünf Jahre nach Inkrafttreten des DSG) durchgeführt werden:

"[...] der Verantwortliche oder der Auftragsbearbeiter" ist jeweils zu ergänzen: "der Verantwortliche, der Auftragsbearbeiter oder Gesetzgeber".

Dies ist insbesondere für Gesetze im Bereich des Arbeitsrechts zu machen.

Art. 16 Abs. 6 (neu): Evaluation von Gesetzeserlassen

Gesetze, welche eine Überwachung von Personen beinhalten, werden mit einem "Verfallsdatum" versehen. Sie müssen nach den ersten fünf Jahren seit Inkrafttreten zwingend einer Evaluation, welche die Wirksamkeit und Verhältnismässigkeit prüft, unterzogen werden. Das Resultat bestimmt darüber, ob das Gesetz weiter angewendet werden kann. Wir schlagen daher folgende Ergänzung vor:

"Handelt es sich um ein Gesetz, welches eine Überwachung von Personen beinhaltet, ist es auf eine Anwendungsdauer von fünf Jahren zu beschränken. Eine Evaluation der Wirksamkeit und Verhältnismässigkeit bestimmt darüber, ob das Gesetz weiter angewendet werden darf."

Alternativ kann das Resultat der Evaluation auch als Grundlage für eine zwingende Neuberatung durch das Parlament verwendet werden.

Art. 19 lit. a – Weitere Pflichten

Gemäss dem erläuternden Bericht wird dadurch für Private die bisherige Verpflichtung ersetzt, Datensammlungen beim Beauftragten zu registrieren. Dies ist für den SGB nicht akzeptabel.

Vielmehr muss weiterhin über eine Registrierung nachgewiesen werden können, dass die Datenschutzbestimmungen eingehalten werden.

Art. 20 – Auskunftsrecht

Das Auskunftsrecht ist ein zentrales Element des Datenschutzes und schafft die Grundlage für die Durchsetzung weiterer Rechtsansprüche der betroffenen Personen.

Art. 20 Abs. 1 – Auskunftsrecht und Kosten

Der SGB begrüsst diese Bestimmung. Die Auskunft ist zu Recht kostenlos vom Verantwortlichen zu leisten.

Art. 20 Abs. 2 lit. c – Auskunftsrecht zur Rechtsgrundlage

Gegenüber der Bestimmung im geltenden DSG wurden hinsichtlich des Auskunftsrechts die Angaben zur Rechtsgrundlage gestrichen. In den Erläuterungen lässt sich keine Begründung hierzu finden. Eine Angabe zur Rechtsgrundlage dient dazu, dass die betroffene Person ihre Rechte nach dem DSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.

Wir schlagen daher vor, lit. c. zu ergänzen: "…der Zweck der Bearbeitung und die Rechtsgrundlage;"

Art. 20 Abs. 2 lit. g – Auskunftsrecht und Informationspflicht

Zur Erfüllung der Informationspflicht ist die Bekanntgabe der Kategorien der bearbeiteten Daten, der Kategorien der zur Auftragsbearbeitung übergebenen Daten und der Kategorien der Datenempfänger gemäss Art. 13 Abs. 3 und 4 ausreichend. Die Auskunftspflicht hingegen muss neben den Daten auch die Empfänger der Daten – und nicht nur deren Kategorien umfassen. Eine Unterscheidung der Auskunftspflicht und der Informationspflicht ist daher sinnvoll.

Lit. g und h (neu) sind wie folgt zu formulieren:

"g. gegebenenfalls Empfängerinnen und Empfänger der Personendaten;

h. gegebenenfalls die Identität und Kontaktdaten des Auftragsbearbeiters der Personendaten."

Art. 20 Abs. 3 – Auskunftsrecht und Entscheidungen

Bereits heute finden massenhaft automatisierte Einzelentscheidungen – die ausschliesslich auf Algorithmen beruhen und ohne menschliches Eingreifen getroffen werden – auf Grund von Personendaten, die z.B. gewisse Arbeitsmuster und Abläufe der Arbeitnehmenden registrieren, statt.

In Zukunft werden noch viel mehr persönliche Daten aus der Leistungsmessung, über Mobilitäts- und Gesundheitsdaten bis zu Sensordaten zur automatisierten Auswertung zur Verfügung stehen.

Für die Nachvollziehbarkeit sind Informationen über die verwendeten Algorithmen wichtig. Die Bestimmung greift daher zu kurz und muss grundsätzlich ein Auskunftsrecht über die Bearbeitung mit Algorithmen enthalten. Die Mechanismustransparenz muss in geeigneter Form (beschreibend oder als Algorithmus selber) erfolgen.

Neue Formulierung für Art. 20 Abs. 3:

“Werden Personendaten automatisiert bearbeitet, erhält die betroffene Person das Ergebnis und Informationen über das Zustandekommen des Ergebnisses, bei einer automatisierten Einzelentscheidung zusätzlich die Auswirkungen der Entscheidung, mitgeteilt.”

Art. 20 Abs. 7, 8, 9 und 10 (neu) – Datenauskunft und Daten Portabilität

Bis anhin ist es für Betroffene nur umständlich und mit viel zeitlichem Aufwand möglich, das Datenauskunftsrecht wahrzunehmen. Die Anfragen werden von den Verantwortlichen oft (lange) ignoriert, unvollständig gewährt und beinhalten lediglich einige ausgedruckte Screenshots. Auch die neuen Bestimmungen zum Auskunftsrecht enthalten keine zeitlichen und formellen Vorgaben, keine Pflicht zur Vollständigkeitsbestätigung und keine Angaben zu den Rechten der Betroffenen, einschliesslich Angaben entsprechend einer Rechtsmittelbelehrung. Diese wären zum Ausgleich des Machtgefälles wichtig.

Das Recht auf Datenportabilität ist im vorliegenden Entwurf nicht vorgesehen. Dies ist unverständlich. Wir schlagen folgende Ergänzungen vor:

Abs. 7 (neu): “Die Auskunft wird in der Regel innerhalb von 30 Tagen erteilt. Ist die Informationsbeschaffung mit unverhältnismässigem Aufwand verbunden, erhält die betroffene Person nach spätestens 30 Tagen eine Übersicht zu den Kategorien und dem Zweck der bearbeiteten Daten. Die betroffene Person bestimmt, zu welchen Kategorien die vollständige Auskunft zu erteilen ist.”

Abs. 8 (neu): “Die Auskunft hat in der Regel elektronisch und in einem Format zu erfolgen, das sich zur Weiterverarbeitung eignet, es sei denn die Bearbeitung der Daten findet nicht elektronisch statt.”

Abs. 9 (neu): “Die Vollständigkeit und Korrektheit der Datenauskunft ist zu bestätigen.”

Abs. 10 (neu): “Die Datenauskunft enthält Angaben zu den Betroffenenrechten.”

Art. 25 – Rechtsansprüche

Verletzungen der Auskunfts-, Melde- und Mitwirkungspflichten, der Sorgfaltspflichten sowie der beruflichen Schweigepflicht sollen gemäss vorliegendem Entwurf nach Art. 50 bis 52 bestraft werden können. Nicht strafrechtlich relevant blieben Persönlichkeitsverletzungen durch Datenbearbeitungen und Verstösse gegen die Datenbearbeitungsgrundsätze. Verstösse gegen diesen Kernbereich des Datenschutzes müssten aber ebenfalls sanktioniert werden können. Dies ist entsprechend in Kapitel 8 “Strafbestimmungen” vorzusehen (siehe Art. 50).

Bei Verstössen gegen das Datenschutzrecht ist in der Regel ein Organisationsverschulden anzunehmen. Die Feststellung des schuldhaften Verhaltens einzelner Personen, z.B. einzelner Arbeitnehmenden, ist u.E. nicht relevant. Anstatt Strafrecht anzuwenden, wären u.E. eher Verwaltungssanktionen vorzusehen (s.a. Ausführungen zu Art. 50 ff.).

Art. 25 Abs. 4 (neu) – Verbands- und Sammelklagen

Bereits heute kann sich der Beauftragte aufgrund knapper Ressourcen nur auf wenige exemplarische Fälle von (möglichen) Datenschutzverletzungen konzentrieren. Mit dem totalrevidierten Datenschutzgesetz sollen dem Beauftragten neue Aufgaben zufallen. Gleichzeitig dürften die Ressourcen nicht nennenswert aufgestockt werden.

Auch mit dem neuen Gesetz bleibt die Grundschwierigkeit bestehen, die zustehenden Rechte in der Praxis durchsetzen zu können. In Art. 25 ist zum Beispiel nicht vorgesehen, dass Verstösse

gegen den Kernbereich des Datenschutzes der Schwere entsprechend sanktioniert werden können.

Als Arbeitnehmer in einem Abhängigkeitsverhältnis ist es schwierig gegen (mögliche) Datenschutzverstösse vorzugehen. Ein wirkungsvolles Mittel wäre eine Regelung zur kollektiven Rechtsdurchsetzung (Erweiterung des Verbandsklagerechts und Einführung einer Sammelklage bzw. eines Sammelvergleichs).

Folgerichtig muss im neuen DSG eine Regelung zur kollektiven Rechtsdurchsetzung (Verbandsklagerecht und Sammelklage), analog beispielsweise zum Arbeitsgesetz etc., vorgesehen sein. Gewerkschaften müssen die Möglichkeit haben, gemäss DSG zu klagen, wenn die Interessen von Arbeitnehmenden tangiert wurden.

Art. 25 Abs. 4 (neu): “Klageberechtigt sind auch Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die sich statutengemäss unter anderem dem Arbeitnehmerschutz bzw. Datenschutz widmen.”

Art. 25 Abs. 5 (neu) – Beweislastumkehr

Eine unrechtmässige Bearbeitung von Daten ist nur schwierig und/oder in einem langwierigen Verfahren nachzuweisen, wenn zur Klärung des Sachverhalts die Mitarbeit und Informationen der beschuldigten Partei notwendig sind. In schwerwiegenden Fällen muss die Beweislast daher umgedreht werden.

Der Anbieter ist zu einer angemessenen Mithilfe zu verpflichten. Den Beweis einer rechtmässigen Bearbeitung kann durch den Verantwortlichen beispielsweise durch Darlegung der Einhaltung von Empfehlungen der guten Praxis erbracht werden. Andernfalls muss davon ausgegangen werden, dass eine unrechtmässige Bearbeitung vorliegt. Daher schlagen wir folgende Präzisierung vor:

“Besteht der Verdacht auf eine schwerwiegende und systematische Verletzung der Persönlichkeit, ist der Verantwortliche verpflichtet, die rechtmässige Bearbeitung der Daten nachzuweisen.”

Art. 41 – Untersuchung

Die erweiterten Untersuchungsbefugnisse werden begrüsst. Der anzeigenden Person sollte ein Recht auf einen Entscheid und eine Anfechtmöglichkeit zugestanden werden:

Abs. 1: “Der Beauftragte eröffnet von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.”

Abs. 5: Ist verbindlicher zu formulieren und eine Behandlungsfrist festzuhalten.

Art. 50 bis 52 - Strafbestimmungen

Verletzungen der Auskunfts-, Melde- und Mitwirkungspflichten, der Sorgfaltspflichten sowie der beruflichen Schweigepflicht sollen gemäss vorliegendem Entwurf nach Art. 50 bis 52 bestraft werden können. Nicht strafrechtlich relevant blieben Persönlichkeitsverletzungen durch Datenbearbeitungen und Verstösse gegen die Datenbearbeitungsgrundsätze gemäss Art. 25. Verstösse gegen diesen Kernbereich des Datenschutzes müssten aber ebenfalls sanktioniert werden können. Dies ist entsprechend in Kapitel 8 “Strafbestimmungen” vorzusehen.

Bei Verstössen gegen das Datenschutzrecht ist ein Organisationsverschulden anzunehmen. Die Feststellung des schuldhaften Verhaltens einzelner, abhängiger Personen wie Arbeitnehmer ist nicht relevant. Dies ist so zu präzisieren.

Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen.

Art. 52 – Verletzung der beruflichen Schweigepflicht

Der SGB lehnt diese Bestimmung mit Bestimmtheit ab.

Mit der Bestimmung würde (im Bereich der Personendaten) ein Tatbestand für Mitarbeiter von Privatfirmen geschaffen, welcher der Amtsgeheimnisverletzung bei staatlichen Angestellten entspricht. Dies wird negative Auswirkungen für Informanten (Whistleblower) haben, welche berechtigterweise auf Missstände in ihren Unternehmen aufmerksam machen wollen. Wir lehnen die neue Bestimmung deshalb ab.

Zivilprozessordnung (ZPO)

Die Erleichterungen für die private Rechtsdurchsetzung durch den Verzicht auf Gerichtskosten und Leistung einer Sicherheit werden begrüsst.

Besten Dank für die Berücksichtigung der oben gemachten Ausführungen.

Freundliche Grüsse

SCHWEIZERISCHER GEWERKSCHAFTSBUND

Paul Rechsteiner
Präsident

Luca Cirigliano
Zentralsekretär

Schweizerische
Gesellschaft für Geschichte
Société suisse d'histoire
Società svizzera di storia
Societad svizra d'istorgia

Villettemattstrasse 9
CH-3007 Bern
Telefon +41 (0)31 381 38 21
Mail generalsekretariat@sgg-ssh.ch

Eidgenössisches Justiz- und
Polizeidepartement
Vorsteherin
Bundesrätin Simonetta Sommaruga

Per Mail: jonas.amstutz@bj.admin.ch

Bern, 6. April 2017

Eingabe der Schweizerischen Gesellschaft für Geschichte zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Die Schweizerische Gesellschaft für Geschichte (SGG) ist der Dachverband der Historikerinnen und Historiker der Schweiz. Sie vertritt insbesondere die Interessen der Forscherinnen und Forscher, die Zugang zu Archivquellen brauchen und für die die Regelung und Handhabung des Datenschutzes von grosser Wichtigkeit sind. Insofern bedauern wir, dass wir zur Vernehmlassung zur Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz nicht eingeladen wurden und freuen uns, wenn wir künftig bei Vorlagen, die unser Fach betreffen, begrüsst werden. Um den Eingang von geistes-, kultur-, und sozialwissenschaftlichem Wissen in die politischen Prozesse zu sichern, empfehlen wir auch, die Schweizerische Akademie der Geistes- und Sozialwissenschaften (SAGW) verstärkt als Vernehmlassungsadressatin zu berücksichtigen.

Wir vertreten eine Berufsgruppe, die zwecks wissenschaftlichen Erkenntnisgewinns in fundamentalem Masse auf personenbezogene Nachforschungen angewiesen ist. Daher möchten wir betonen, dass die Revision des Datenschutzgesetzes auf keinen Fall zu Hemmnissen für Nachforschungen über das Wirken von Personen des öffentlichen Lebens führen darf. Das neue Datenschutzgesetz soll nicht zum Instrument des umfassenden Schutzes von Personen werden, deren öffentliches Leben oder politische Tätigkeit ein legitimes historisches und damit öffentliches Interesse mit sich bringen. Die Schweizer Historikerinnen und Historiker sind in Bezug auf ihre Forschungstätigkeit auf eine liberale und progressive Handhabung des Zugangs zu Informationen über Personen des öffentlichen Lebens angewiesen. Die Mitglieder der SGG sind für datenschutzrechtliche Probleme sensibilisiert und gemäss berufsethischen Standards verpflichtet, die Einsicht in vertrauliche und schützenswerte Personendaten nicht zu missbrauchen.[1]

[1] Vgl. Art. 8 des Ethik-Kodex der Schweizerischen Gesellschaft für Geschichte (SGG), abrufbar unter: http://sgg-ssh.ch/sites/default/files/files/SGG-NUR_EthikKodex.pdf (besucht am 3.4.2017).

Für den vorliegenden Vorentwurf zum Datenschutzgesetz (VE-DSG) möchten wir unter Berücksichtigung der im vorangehenden Abschnitt festgehaltenen Grundsätze die folgenden Punkte hervorheben:

- Begrüssenswert ist die **Änderung von Art. 2 Abs. 1 VE-DSG, wonach der Schutz von Daten juristischer Personen aufgehoben wird**. Wiederholt wurde Mitgliedern der SGG bei der Einsichtnahme in Archivgut des Bundesarchivs nach Art. 13 Abs. 3 des Bundesgesetzes über die Archivierung (BGA) die Auflage gemacht, bei der Bearbeitung von Personendaten juristischer Personen deren Einwilligung einzuholen. Abgesehen davon, dass die SGG die Notwendigkeit der Einwilligung, insbesondere von Personen der Zeitgeschichte, generell ablehnt, stösst die Forschungspraxis bei solchen Auflagen stets auf unüberwindbare Hürden, zumal bei vielen in historischen Dokumenten erwähnten juristischen Personen unklar ist, wer deren Rechtsnachfolger und damit für die Einwilligung zuständig ist.

- Die materielle Übernahme des Grundsatzes der **Anbietepflicht von Unterlagen an das Bundesarchiv in Art. 31 VE-DSG**, der seit 1. Januar 2008 im DSG verankert ist, wird von unserer Seite befürwortet. Indem Personendaten vor einer allfälligen Vernichtung zuerst dem Bundesarchiv zur Prüfung der Archivwürdigkeit angeboten werden müssen, wird sichergestellt, dass kein archivwürdiges Material vernichtet wird.

- Wir nehmen zur Kenntnis, dass **in Art. 12 VE-DSG neu ein Einsichtsrecht (Abs. 1) für Angehörige und ein Löschungs- und Vernichtungsrecht für Erben festgelegt wird (Abs. 4)**. Der Vorbehalt von Art. 12 Abs. 5 VE-DSG zugunsten weiterer Spezialgesetze des Bundesrechts, insbesondere des BGA, ist für uns zentral und darf auf keinen Fall aus dem Gesetzesentwurf fallen. Namentlich dürfen gemäss Art. 15 Abs. 3 BGA keine archivierten Daten vernichtet oder berichtigt werden. Dieser «Löschungsschutz» nach Art. 15 Abs. 3 BGA muss Art. 12 VE-DSG immer vorsehen, denn jede nachträgliche Änderung in Archivmaterialien kommt aus Sicht der historischen Forschung einer Quellenverfälschung gleich. Mangelhaft ist zudem, dass die bearbeitende Person gegen die Löschung lediglich Interessen des Erblassers oder Dritter einwenden kann, nicht jedoch überwiegende öffentliche Interessen oder gesetzliche Pflichten. Hier müssen im Entwurf die öffentlichen Interessen oder gesetzliche Pflichten explizit festgehalten werden.[2]

- Aus wissenschafts- und erkenntnistheoretischer Sicht ist ein **«Recht auf Vergessen(werden)»** immer problematisch. Die Konkretisierung dieses Rechts **in Art. 25 VE-DSG** darf insbesondere für Personen der Zeitgeschichte explizit nicht angewendet werden. Aus Sicht der SGG ist für die Forschung zudem eine Ausnahmebestimmung in Art. 25 VE-DSG für die Bearbeitung von Daten aus Archiven und anderen Gedächtnisinstitutionen notwendig, in Analogie zur Regelung für Bundesorgane gemäss Art. 34 Abs. 4 VE-DSG. Historische Dokumente aus Archiven dürfen vor oder während eines Forschungsprozesses nicht durch Berichtigung, Vernichtung oder Löschung abgeändert werden, ansonsten wird der Nutzen solcher Dokumente für historische Zwecke hinfällig.

[2] Vgl. ROSENTHAL DAVID, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017, Rz. 74.

Wir sind ausserdem der Meinung, dass die folgenden Punkte im laufenden Revisionsprozess zu wenig oder gar keine Beachtung fanden:

- Die SGG nimmt die materielle Übernahme des **Rechtfertigungsgrundes der** «**Person des öffentlichen Lebens»** vom geltenden Datenschutzrecht in Art. 24 Abs. 2 lit. f VE-DSG mit Zustimmung zur Kenntnis. Allerdings erachten wir es als zentral, dass die Konzepte der «absoluten» und «relativen Personen» der Zeitgeschichte unter dem Begriff der «Person des öffentlichen Lebens» Eingang im Gesetz finden. Diese beiden Konzepte sind von der Rechtsprechung anerkannt[3] und konkretisieren den Begriff der Person des öffentlichen Lebens in entscheidender Weise. Die historische Forschung ist darauf angewiesen, dass diese Begrifflichkeiten operational sind. Zudem ist die Formulierung der Anwendbarkeit der Rechtfertigungsgründe zu wenig scharf im Vergleich mit der derzeit geltenden Formulierung in Art. 13 Abs. 2 DSG («…fällt insbesondere in Betracht…»). Die neu eingefügte Abschwächung «möglicherweise» in Art. 24 Abs. 2 VE-DSG verleiht den Rechtfertigungsgründen bloss fakultativen Charakter und muss gestrichen werden. Wir möchten betonen, dass Historikerinnen und Historiker, die über den öffentlichen Wirkungskreis einer Person der Zeitgeschichte Nachforschungen anstellen, **immer** im überwiegenden öffentlichen Interesse handeln. Entscheidend ist auch, dass Art. 24 Abs. 2 lit. f VE-DSG lediglich das Sammeln von Daten rechtfertigt, nicht zwingend auch deren Veröffentlichung, was somit einen geringeren Eingriff in die Persönlichkeitsrechte der betroffenen Person darstellt. Daher müssen auch geringere Anforderungen an die Rechtfertigung des Sammelns von Personendaten gem. lit. f gestellt werden als an die anderen Rechtfertigungsgründe, die eine Bearbeitung einschliessen.
  Schliesslich haben Historikerinnen und Historiker häufig ein Interesse an der blossen Einsicht in Daten über Personen der Zeitgeschichte, um einen Überblick über komplexe Sachverhalte zu gewinnen, während häufig der Zweck der Veröffentlichung von personenbezogenen Daten nicht im Zentrum historischer Forschungen steht. In der Verwaltungspraxis wird diesem Umstand leider allzu selten Rechnung getragen. Vermehrt wird Mitgliedern der SGG die Einsicht in Archivgut des Bundesarchivs auch nach Ablauf der Schutzfrist von 30 bzw. 50 Jahren mit Verweis auf Art.11 oder Art. 12 BGA verwehrt. Meist bleibt dabei ein allfälliges überwiegendes öffentliches Interesse (z.B. nach Art. 13 Abs. 2 lit. f DSG) gänzlich unberücksichtigt. Wir halten dies für einen krassen Fehler der Verwaltungspraxis, die zu Ungunsten der historischen Forschung ausfällt.

- Die Diskussion über die **Rechte von Erbinnen und Erben an Personendaten des Erblassers** ist in der DSG-Revision mit dem blossen Verweis des erläuternden Berichts auf das Erbrecht zu kurz geraten. Auf keinen Fall dürfen die Rechte an Daten von Personen der Zeitgeschichte an ihre Nachkommen übergehen, sodass für die Bearbeitung solcher Daten die Einwilligung der gesetzlichen Erben notwendig ist. Die SGG hat in einem aktuellen Befragungsverfahren bei ihren Mitgliedern festgestellt, dass Einsichtsgesuche nach Art. 13 BGA von Seiten der aktenabliefernden Stellen, d.h. der Organe der Bundesverwaltung, mehrfach mit der Auflage genehmigt wurden, die Einwilligung der Erben der verstorbenen Person der Zeitgeschichte einzuholen. Nach unserer dezidierten Auffassung sind solche Auflagen mit **keiner Regelung**

[3] Vgl. BGE 127 III 481 ff., S. 488 E. 2 a/aa.

des geltenden Rechts vereinbar. Deshalb müsste im Rahmen der Revision des DSG festgehalten werden, dass der Datenschutz, mit Ausnahme der Regelung von Art. 12 VE-DSG, ausschliesslich für betroffene Personen und nicht deren Erben gilt.
Nach den Grundsätzen von Art. 31 Abs. 1 ZGB endet die Persönlichkeit mit dem Tode. An diesem Grundsatz darf auch unter dem Regime des neuen DSG nicht gerüttelt werden.

Wir danken für Ihre Kenntnisnahme unserer Ausführungen und stehen für Rückfragen gerne zur Verfügung.

Freundliche Grüssen

Sacha Zala
Präsident SGG

Peppina Beeli
Generalsekretärin

SGHVR
SDRCA
Schweizerische Gesellschaft für Haftpflicht- und Versicherungsrecht

Société suisse du droit de la responsabilité civile et des assurances

Per E-Mail an:
jonas.amstutz@bj.admin.ch

EJPD
Frau Bundesrätin Sommaruga
Bundeshaus West
3003 Bern

Rodersdorf, 31. März 2017

Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Vernehmlassung

Sehr geehrte Frau Bundesrätin
sehr geehrte Damen und Herren

Die Schweizerische Gesellschaft für Haftpflicht- und Versicherungsrecht (SGHVR) bedankt sich für die Möglichkeit, sich im Rahmen der Vernehmlassung zur oben erwähnten Vorlage äussern zu können. Entsprechend der Ausrichtung unserer Gesellschaft gilt unser primäres Interesse der wissenschaftlichen Durchdringung der geregelten Materie. Im Übrigen steht fest und bedarf keiner weiteren Ausführungen, dass die Versicherungswirtschaft von der Vorlage ausserordentlich stark betroffen ist. Sowohl beim Abschluss von Versicherungsverträgen wie auch bei deren Erfüllung werden zum Teil sehr sensible Personendaten bearbeitet.

Stephan Fuhrer | Prof. Dr. iur., Präsident | Oberdorfstrasse 16 | 4118 Rodersdorf | Tel: 061 731 16 26 | stephan.fuhrer@sghvr.ch

I. Grundsätzliche Bemerkungen

1. Vorbemerkung

Die Schweiz ist – im Rahmen des „Schengen-Übereinkommens" – völkerrechtlich verpflichtet, die Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen umzusetzen. Es ist für uns daher eine Selbstverständlichkeit, dass die Schweiz jene Rechtsanpassungen vornimmt, die durch diese Richtlinie bedingt sind. Einverstanden sind wir auch damit, dass die Schweiz das revidierte Übereinkommen SEV 108 ratifiziert und soweit nötig umsetzt. Dabei gehen wir davon aus, dass im Zeitpunkt der Verabschiedung der Botschaft dieses Übereinkommen cum grano salis in der heute vorliegenden Form verabschiedet worden sein wird.

Skeptisch sind wir, was die vom Bundesrat angestrebte Anlehnung des schweizerischen Rechts an die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten betrifft. Diese Verordnung bindet die Schweiz bekanntlich nicht. Es gibt seitens der EU auch keinerlei Garantien dafür, dass der „autonome Nachvollzug"[1] dieser Verordnung der Schweiz und ihrer Wirtschaft irgendwelche Vorteile verschaffen könnte. Daran ändert auch der Hinweis im Begleitbericht nichts, wonach sich ein künftiger Angemessenheitsbeschluss der EU-Kommission an der Respektierung dieser Verordnung orientieren werde (S. 14): Mehr Rechtssicherheit mit der EU verspricht einzig ein Staatsvertrag, der auch den Datenschutz zum Gegenstand hat (vgl. die vom Parlament überwiesene Motion 16.3752 der FDP-Liberale Fraktion "Gegen Doppelspurigkeiten im Datenschutz"). Im Übrigen ist klar, dass sich die schweizerischen Unternehmen an diese EU-Verordnung zu halten haben, wenn sie EU-Raum tätig sind bzw. EU-Bürger bedienen (vgl. David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017, insbes. Rz. 130-132). Dies allein kann nun aber kein Grund sein, das schweizerische Recht an jenes der EU anzupassen.

2. Verzicht auf Totalrevision

Bei der geschilderten Ausgangslage halten wir den Entscheid des Bundesrates zu Gunsten einer Totalrevision des Datenschutzgesetzes für nicht sachgerecht. Eine Teilrevision genügt dem im Begleitbericht ausgewiesenen Handlungsbedarf vollauf. Das vorgeschlagene Datenschutzgesetz folgt in seinen Grundzügen und seiner Struktur dem alten: Es baut auf dem nämlichen, weiten Begriff der (Personen-)Daten auf (Art. 3 Bst. a VE-DSG), formuliert Pflichten des Verantwortlichen und des Auftragsbearbeiters (Art. 13 ff. VE-DSG) und unterscheidet im Übrigen zwischen der Datenbearbeitung durch private Personen (Art. 23 ff. VE-DSG) und Bundesorgane (Art. 26 ff. VE-DSG). Nach wie vor keine Anwendung findet das Datenschutzgesetz auf Kantonsorgane. Auch institutionell bleibt mit dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten alles beim Alten (Art. 37 VE-DSG). Zusätzliche Verpflichtungen und der Wunsch

[1] Die Idee, die EU-Verordnung nachzuvollziehen, macht auch deshalb keinen Sinn, weil eine Verordnung nach der Definition des europäischen Rechts in den Mitgliedstaaten unmittelbar anwendbar ist und daher gar keiner Umsetzung bedarf. Die vom Bundesrat angestrebte blosse Anlehnung an die EU-Verordnung erweist sich damit zum vorneherein als widersprüchlich.

nach einer neuen, vermeintlich moderneren Terminologie – vgl. zum Beispiel den Begriff des Profiling (Art. 3 Bst. f VE-DSG) – genügen als Begründung für eine Totalrevision des im Vergleich mit dem ZGB oder OR noch jungen Datenschutzgesetzes nicht. Eine Teilrevision zwingt den Gesetzgeber dazu, sich im Detail zu überlegen, wo tatsächlich Handlungsbedarf besteht und sich auf die wirklich nötigen Anpassungen des schweizerischen Rechts zu konzentrieren. Auch hat eine Teilrevision den Vorteil, dass viel leichter auf die Lehre und die Rechtsprechung zum bisherigen Recht zurückgegriffen werden kann.

2. Status quo bezüglich juristischer Personen

Im gleichen Zusammenhang lehnen wir es auch ab, dass das Datenschutzgesetz künftig nur noch die Daten natürlicher Personen erfasst (Art. 2 Abs. 1 VE-DSG). Auch für diesen Entscheid liefert der Begleitbericht keine substantielle Begründung, sieht man vom Hinweis ab, dass auch ausländische und internationale Vorbilder nur Personendaten natürlicher Personen schützen. Der bundesrätliche Vorschlag ignoriert, dass die Datenschutzgesetzgebung in der Schweiz historisch aus dem Persönlichkeitsschutz (Art. 28 ZGB) herausgewachsen ist, auf den sich auch juristische Personen berufen können. Den juristischen Personen ist es nicht zuzumuten, dass für den Schutz ihrer Daten künftig wieder ausschliesslich Art. 28 ZGB zum Zuge käme. Die Gerichte ihrerseits wären wohl veranlasst, in diesem Fall regelmässig das Datenschutzgesetz für analog anwendbar zu erklären. Mehr Rechtsunsicherheit wäre die Folge.

II. Im Einzelnen

1. Bekanntgabe ins Ausland (Art. 5 und 6 VE-DSG)

Wir begrüssen es, dass künftig die Verantwortung für die Bekanntgabe von Daten ins Ausland nicht mehr auf den Schultern Privater lastet. Allerdings bringt das vorgeschlagene Regime insoweit keinen Fortschritt, als nicht der Bundesrat die Gleichwertigkeit der ausländischen Gesetzgebung feststellt und das Ergebnis in einer Verordnung festhält. Im Gegenteil: Der Vorentwurf erweist sich im Fall, dass ein Land nicht in der bundesrätlichen Liste figuriert, zumindest dann als viel zu kompliziert, wenn es um die Datenbearbeitung durch private Personen geht. Wir sind der Meinung, dass in diesem Fall die Bekanntgabe von Daten diese Länder zum vorneherein nur dann in Frage kommt, wenn dafür die Zustimmung der von der Bekanntgabe betroffenen Person vorliegt. Dabei sind wir offen dafür, dass diese Zustimmung nicht nur im Einzelfall erteilt werden kann (so aber Art. 6 Abs. 1 Bst. a VE-DSG), sondern auch im Rahmen Vertragsbedingungen.

Eine Bekanntgabe von Personendaten ins Ausland kommt selbstverständlich auch nicht in Frage, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet wird (Art. 5 Abs. 1 VE-DSG). Dies gilt unseres Erachtens entgegen Art. 6 Abs. 1 Bst. a VE-DSG auch im Fall einer vermeintlichen Einwilligung: Jede andere Lösung verstiesse gegen Art. 27 ZGB.

2. Ausarbeitung von Empfehlungen der guten Praxis (Art. 8 und 9 VE-DSG)

Das Datenschutzgesetz arbeitet mit Generalklauseln und unbestimmten Rechtsbegriffen. Wir begrüssen diese Offenheit, auch wenn diese zwangsläufig mit Rechtsunsicherheit verbunden ist. Um das Ganze in geordnete Bahnen zu lenken, begrüssen wir es auch, dass die interessierten Kreise allein oder zusammen mit dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten Empfehlungen der guten Praxis erarbeiten. Solche Empfehlungen dürfen nun aber nicht die korrekte Auslegung des Gesetzes präjudizieren. Der diesbezügliche Entscheid muss vielmehr immer dem unabhängigen Richter vorbehalten bleiben. Soweit Art. 9 Abs. 1 VE-DSG und der Begleitbericht diesen Empfehlungen einen weitergehenden Gehalt geben, indem die Einhaltung der Empfehlungen rechtskonformes Verhalten bestätigen, ist davon Abstand zu nehmen. Würde man sich anders entscheiden, hätten diese Empfehlungen der guten Praxis einen höheren Stellenwert als eine das Gesetz konkretisierende bundesrätliche Verordnung.

3. Daten einer verstorbenen Person (Ar. 12 VE-DSG)

Wir begrüssen es, dass der Vorentwurf den Versuch unternimmt, den Umgang mit den Daten verstorbener Person systematisch zu regeln. Allerdings dürfte das Unterfangen in der vorgeschlagenen Form auf beträchtliche Schwierigkeiten stossen. So ist nicht klar, wie das Opting-out von Art. 12 Bst. a VE-DSG zu handhaben ist: Welche Anforderungen sind an ein ausdrückliches Untersagen zu stellen? Genügt dafür auch eine Anordnung in einem Testament? Unklar ist auch, welche überwiegenden Interessen der verstorbenen Person oder von Dritten einer Auskunftserteilung im Wege stehen könnten.

Abs. 2 führt den Begriff der faktischen Lebensgemeinschaft in die Rechtsordnung ein, ohne zu sagen, was damit genau gemeint ist. Wie verhält es sich beispielsweise, wenn eine Klostergemeinschaft Auskünfte über eine verstorbene Mitschwester oder einen verstorbenen Mitbruder verlangt oder verweigert?

Als noch heikler erachten wir es, wenn Art. 12 Abs. 4 VE-DSG jedem Erben das Recht gibt, Daten des Erblassers (kostenlos) löschen oder vernichten zu lassen. Der Erbe tritt in die vermögensrechtliche Stellung des Erblassers ein; Erbe zu sein bedingt keine besondere Nähe zu den Personendaten des Erblassers. Folgt man dem Vorentwurf könnte der Erbe beispielsweise verlangen, dass Personendaten des Erblassers auch aus einem elektronischen Zeitungsarchiv entfernt werden, ausser man bejahe in diesem Fall ein überwiegendes Interesse des Verlags, diese Daten nicht löschen zu müssen. Ähnliche Probleme können sich auch bei der Archivierung von Daten anderer Unternehmen ergeben. Wir zweifeln daran, dass der Vorbehalt spezieller Bestimmungen anderer Bundesgesetze (Art. 12 Abs. 5 VE-DSG) die möglichen Probleme befriedigend lösen kann.

4. Datenschutz-Folgenabschätzung (Art. 16 VE-DSG)

Wir sind damit einverstanden, dass die für den Datenschutz Verantwortlichen in gewissen Fällen eine Datenschutz-Folgenabschätzung durchführen und das Ergebnis dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten melden müssen. Allerdings scheinen uns die Voraussetzungen, die Anlass zu einer Datenschutz-Folgenabschätzung geben, einen viel zu grossen Kreis von Betroffenen zu erfassen. Auszugehen ist davon, dass die Bearbeitung von Personendaten immer mit einem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person verbunden ist. Was also bedeutet es, wenn Art. 16 Abs. 1 VE-DSG von einem „erhöhten Risiko" spricht? Man denke zum Beispiel an die Installation einer Videokamera zur Überwachung des Eingangsbereichs eines Mehrfamilienhauses. Verlangt eine solche Massnahme nach einer Datenschutz-Folgenabschätzung? Hängt die Antwort auf die Frage davon ab, wie viele Mieter auf diese Weise kontrolliert werden? Spielt eine Rolle, ob die Eingänge rund um die Uhr oder nur während gewisser Zeiten überwacht werden?

Im Übrigen sind wir der Meinung, dass die Datenschutz-Folgenabschätzung zwingend vom Verantwortlichen durchzuführen ist. Der Vorentwurf spricht davon, dass die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung den Verantwortlichen *oder* den Auftragsbearbeiter trifft (Art. 16 Abs. 1 VE-DSG). Auf diese Weise werden unnötig Verantwortlichkeiten vermischt.

5. Meldung der Verletzungen des Datenschutzes (Art. 17 und 19 VE-DSG)

Die in Art. 17 und 19 VE-DSG vorgesehenen Meldepflichten gehen unseres Erachtens zu weit. Verletzungen des Datenschutzgesetzes dürften immer wieder vorkommen. Und zweifellos ist es auch richtig, wenn diese Verletzungen den davon Betroffenen gemeldet werden, wenn durch eine Meldung von diesen weiterer Schaden abgewendet werden kann. Hingegen erachten wir es als nicht zielführend, wenn jede unbefugte Datenbearbeitung und jeder Verlust von Daten auch noch dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten gemeldet werden muss. Die vorgesehene Einschränkung, dass eine Meldung nur erfolgen muss, wenn die geschilderte Verletzung zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt, ist nicht zielführend, weil man sich nicht vorstellen kann, welche Verletzungen des Datenschutzgesetzes a priori kein Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person darstellen.

Im Ergebnis dürfte die vorgeschlagenen Meldepflichten den Effekt haben, dass der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte entweder mit Meldungen überhäuft wird, die er nicht sinnvoll verarbeiten kann, oder dass sich die Verantwortlichen schlicht um die Meldepflicht drücken. Gedient ist damit niemandem, schon gar nicht denjenigen, die das Opfer von Verletzungen des Datenschutzgesetzes werden.

6. Vorsorgliche Massnahmen (Art. 42 VE-DSG) und Verwaltungsmassnahmen (Art. 43 VE-DSG) – Verfahren (Art. 44 VE-DSG)

Wir sind damit einverstanden, dass dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten neu die Kompetenz zusteht, Verfügungen zu erlassen und er dafür nicht länger einen Entscheid des Bundesverwaltungsgerichts provozieren muss. Nicht einverstanden sind wir aber damit, wenn Art. 44 Abs. 2 VE-DSG nur das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wird, als Partei bezeichnet wird. Unseres Erachtens dürfen Dritte nicht zum vorneherein als Partei ausgeschlossen werden. Die allgemeinen Regeln über die Beschwerdelegitimation genügen: Sie sollen weder erweitert noch eingeschränkt werden.

7. Amtshilfe zwischen schweizerischen und ausländischen Behörden (Art. 47 VE-DSG)

Wir haben Mühe damit, wenn der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte im Rahmen der Rechtshilfe Informationen an ausländische Behörden liefert, die Aufschluss über die Identität der betroffenen Person geben. Daran ändert auch nichts, dass dies nur in Frage kommt, wenn die Mitteilung der Identität der betroffenen Personen unumgänglich ist, damit die ausländische Behörde ihre gesetzlichen Aufgaben erfüllen können (Art. 47 Abs. 1 Bst. c Ziff. 2 VE-DSG). Die Gefahr ist zu gross, dass auf diese Weise jene Garantien ausgehebelt werden, die heute die Verfahren der Zivil- und Strafrechtshilfe bieten. Hält der Bundesrat an diesem Vorschlag fest, müsste zumindest geregelt werden, wie der Betroffene von der Amtshilfehandlung erfährt und sich dagegen zur Wehr setzen kann.

8. Strafbestimmungen

a) Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten (Art. 50 VE-DSG) und Verletzung der Sorgfaltspflichten (Art. 51 VE-DSG)

Wir begrüssen den Verzicht auf Verwaltungssanktionen. Dieser Verzicht darf nun aber nicht mit allzu offen formulierten Strafbestimmungen erkauft werden. Strafrecht stellt im Konzept des schweizerischen Rechts ultima ratio dar und soll nur dann eingreifen, wenn für die Betroffenen klar ist, welches Verhalten von ihnen verlangt wird. Unseres Erachtens ist dies zumindest insofern nicht der Fall, als Art. 50 Abs. 3 und Art. 51 Abs. 2 VE-DSG auch fahrlässiges Verhalten unter Strafe stellt.

Auch die Höhe der angedrohten Sanktion von Fr. 500'000.-- und von Fr. 250'000.-- bei Fahrlässigkeit halten wir für bedenklich. Das Kernstrafrecht sieht für Bussen einen Höchstbetrag von Fr. 10'000.-- vor (Art. 106 Abs. 1 StGB). Dass dieser Betrag im Rahmen des Datenschutzgesetzes fünfzig Mal höher liegen soll, ist nicht nachvollziehbar. Die Verfasser des Vorentwurfs scheinen vergessen zu haben, dass im Zusammenhang mit Art. 50 und 51 VE-DSG praktisch jedermann als Täter in Frage kommen kann; die Situation lässt sich damit nicht mit der Finanzmarktgesetzgebung vergleichen. Gewisse Täter wird im Übrigen auch eine Busse von Fr. 500'000.-- nicht davon abschrecken, das Datenschutzgesetz zu verletzen.

b) Verletzung der beruflichen Schweigepflicht (Art. 52 VE-DSG)

Viel zu weit geht für uns auch Art. 52 VE-DSG. Danach wird die Bekanntgabe kommerziell bearbeiteter, geheimer Personendaten unter Strafe stellt. Das bisher nur wenige Berufe erfassende Berufsgeheimnis erfährt auf diese Weise eine erratische, durch nichts gerechtfertigte Ausweitung.

c) Übertretungen in Geschäftsbetrieben (Art. 53 VE-DSG)

Als falsch erachten wir es auch, wenn Umgang von der Ermittlung der strafbaren Person genommen werden und direkt die juristische Person bestraft werden kann, soweit die Busse Fr. 100'000.-- nicht überschreitet und eine Strafverfolgung der verantwortlichen natürlichen Personen unverhältnismässige Untersuchungsmassnahmen bedingen würde (Art. 53 VE-DSG): Die Folgen dieses Vorschlags sind leicht absehbar: Die Staatsanwaltschaft wird einen Strafbefehl gegen die juristische Person erlassen und ihm Gegenzug auf eine Untersuchung verzichten. Zu einer seriösen Abklärung des Vorgefallenen durch ein Gericht wird es in diesem Fall praktisch nie kommen.

Schliesslich erlauben wir darauf hinzuweisen, dass die Vorlage in der aktuellen Form den Grundsatz verletzt, wonach sich niemand selber belasten muss (nemo tenentur). Dies passiert, weil der Vorentwurf die Verantwortlichen verpflichtet, strafrechtlich relevante Verstösse gegen das Datenschutzgesetz dem Datenschutz- und Öffentlichkeitsbeauftragten zu melden und dieser dann den Strafrechtsbehörden Anzeige von den strafbaren Handlungen machen muss (Art. 45 VE-DSG).

Mit freundlichen Grüssen
Schweizerische Gesellschaft für Haftpflicht- und Versicherungsrecht

Felix Schöbi, PD Dr. iur.
Vizepräsident

Stephan Fuhrer, Prof. Dr. iur.
Präsident

Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Bundesamt für Justiz
Herr Jonas Amstutz
Bundesrain 20
3003 Bern

jonas.amstutz@bj.admin.ch

Bern, 3. April 2017 sgv-Kl/is

Vernehmlassung:

Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz.

Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen.

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

Sehr geehrte Damen und Herren

Der Schweizerische Gewerbeverband sgv, die Nummer 1 der Schweizer KMU-Wirtschaft, vertritt 250 Verbände und gegen 300‘000 Unternehmen. Im Interesse der Schweizer KMU setzt sich der grösste Dachverband der Schweizer Wirtschaft für optimale wirtschaftliche und politische Rahmenbedingungen sowie für ein unternehmensfreundliches Umfeld ein.

Mit Schreiben vom 21. Dezember 2016 unterbreitete das Eidgenössische Justiz- und Polizeidepartement EJPD den Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, zum Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen und zum Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Der Schweizerische Gewerbeverband dankt für die Möglichkeit zur Stellungnahme. Gestützt auf die zahlreichen und teils umfangreichen Rückmeldungen der Mitglieder des sgv nehmen wir wie folgt Stellung.

Generelle Bemerkungen

Mit der Revision des Datenschutzgesetzes (DSG) will der Bundesrat die Transparenz der Bearbeitung und die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten verbessern. Was auf den ersten Blick gut tönt, geht in Tat und Wahrheit einseitig zu Lasten der Wirtschaft. Für Unternehmen sollen verschiedene neue Verpflichtungen eingeführt werden. Informationspflichten der Unternehmen, die zwangsläufig Daten verarbeiten, sollen ausgeweitet werden. Eine Pflicht zur Mitteilung von Berichtigung oder Löschung von Daten von Personen ist vorgesehen. Damit verbunden sind Auskunftsrechte und ein kostenloses Klagerecht der Betroffenen. Unternehmen werden verpflichtet, eine Datenschutz-

Folgeabschätzung vorzunehmen. Weiter wird eine Pflicht zur Meldung von Verletzungen des Datenschutzgesetzes oder Datenverlust an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eingeführt. Dieser Ausbau von Dokumentations- und Meldepflichten ist unverhältnismässig. Es ist mit einer überschiessenden Informationsflut zu rechnen. Der Revisionsentwurf des Bundesrates orientiert sich einseitig an den potentiellen Risiken für die betroffenen Personen. Die Interessen der Wirtschaft und insbesondere der KMU spielen keine Rolle. Zu weitgehende, nicht praktikable Bestimmungen finden aber keine Akzeptanz in der KMU Wirtschaft. Da alle Unternehmen – insbesondere auch die KMU - dem DSG unterstehen, wird die Gesetzesrevision zusätzliche, hohe Regulierungskosten verursachen. Der vorliegende Entwurf führt insgesamt zu einem übermässigen administrativen Aufwand für die Unternehmen und ist nur schon aus diesem Grund abzulehnen.

Unpräzise Begriffe

Die Vernehmlassungsvorlage verwendet diverse Begriffe, die unpräzise sind und ungenügend definiert bzw. von anderen Begriffen abgegrenzt werden (wie z.B. «Dritte», «Empfänger» uam.). Im Entwurf wird wahlweise von Dritten und Empfängern gesprochen, ohne dass diese Begriffe in Art. 3 VE-DSG definiert werden. Auch werden Begriffe verwendet wie «möglicherweise» (Art. 24 Abs. 2 VE-DSG), was der Rechtssicherheit nicht förderlich ist, oder unnötige, im Kontext eher verwirrende Begriffe wie «klar festgelegte Aufgabe» (Art. 27 Abs. 2 VE-DSG).

Legiferierung über den europäischen Standard hinaus unnötig

Ein Grund für die Revision des DSG ist die Entwicklung des Datenschutzes im europäischen Raum. Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) EuDSGVO in Kraft. Zudem gilt die EU-Richtlinie 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen. Die DSG-Revision soll die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern, wie in der Botschaft des Bundesrates dargelegt wird. Die Annäherung würde gemäss Bundesrat zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür bilden, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht. Die Revision des Schweizer DSG geht aber in mehreren Fällen über das Schutzniveau der EU hinaus, was nicht nachvollziehbar ist. Beispiele für diesen Swiss Finish sind:

- Art. 13 Abs. 3 und 4 VE-DSG sehen eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister) sowie bei der Weitergabe von jeglichen Personendaten vor. Für den Adressaten führt dies zu einer Informationsflut. Nicht einmal die EU-Richtlinie 680/2016 vom 27. April 2016 sieht diesen Detaillierungsgrad vor.
- Art. 16 Abs. 3 VE-DSG sieht eine Informationspflicht des Datenschutzbeauftragten über die Datenschutz-Folgeabschätzungen in jedem Fall vor. Die EU-Richtlinie 680/2016 hingegen fordert in Art. 27 und 28 das nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen.
- Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung (Art. 25). Diese besagt, dass *gewisse* Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen.
- Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EuDSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell.
- Auch der Ansatz des VE-DSG betreffend Profiling geht über die Bestimmungen der EuDSGVO und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der EuDSGVO noch der Konvention. Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung

von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren. Die Bedingung einer vorgängigen ausdrücklichen Einwilligung bei *jeder Art* von Profiling schiesst über das Ziel hinaus. Profiling soll nicht bereits bei dessen Erstellung schutzrelevant werden.

- Überschiessende Informationspflichten (z.B. Art. 6 Abs. 2 oder Art. 13 Abs. 5 VE-DSG), die Geschäftsgeheimnisse betreffen können (gemäss Art. 6 Abs. 2: der EDÖB über heikle Verfahren und (Geschäfts-)Geheimnisse informiert, ohne dass ein (datenschutzrechtlicher) Grund dafür vorliegen würde. Zudem ist diese Pflicht dem EU Recht (inkl. E-SEV 108) fremd und somit ein Swiss Finish. Ebenfalls Swiss Finish ist Art. 13 Abs. 5 VE-DSG.

Insgesamt lehnt der sgv Bestimmungen, die über das Mass der europäischen Regelungen hinausgehen, ab. Es besteht keine Notwendigkeit für einen «Swiss Finish».

Fehlende verfassungskonforme Regulierungskostenfolgeabschätzung (RFA)

Gemäss Art. 170 der Bundesverfassung sorgt die Bundesversammlung dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden. Art. 141 Abs. 2 Bst. f) ParlG verpflichtet den Bundesrat, in den Botschaften ans Parlament eine Kosten-Nutzen Abschätzung vorzunehmen sowie nach Bst. g) die Folgen für die Wirtschaft und die Gesellschaft zu erläutern. Dieser Auftrag wird in der vorliegenden Botschaft zur Totalrevision des Datenschutzgesetzes nicht umgesetzt. Zwar wird auf den Seiten 22 und 23 die RFA als Instrument erwähnt sowie auf eine Studie von PwC verwiesen, die Regulierungskosten werden jedoch als «unbedeutend» eingestuft, was weder plausibel ist noch der Realität entsprechen dürfte. Im Rahmen der zunehmenden Digitalisierung in allen Bereichen und Branchen der KMU-Wirtschaft werden die Unternehmen in den kommenden Jahren viel stärker von Daten aller Art betroffen bzw. abhängig sein. Dies wird auch die Regulierungskosten für die Unternehmen in die Höhe treiben. Die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG wird vom sgv hinterfragt. Die auf Seite 23 der Botschaft vermerkte Unternehmensbefragung basiert auf einer Nettostichprobe von nicht einmal 100 Unternehmen (vgl. S. 25 der Studie «RFA DSG - Regulierungsfolgenabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG) vom 11. Juli 2016, Schlussbericht»). In Anbetracht von rund 300'000 Firmen in der Schweiz ist dies eine klar ungenügende Basis, um neue, weitreichende Verpflichtungen und Regulierungen abzustützen. Weiter stellt die Studie fest, dass «kein Unternehmen den Fragebogen vollständig beantwortet hat; die Qualität des Rücklaufs ist bei den einleitenden, generellen Fragen zum Unternehmen die höchste. Je grösser der Fortschritt bei der Bearbeitung des Fragebogens, desto geringer die Qualität der Antworten (überwiegend sind gegen Ende des Fragebogens keine Antworten mehr gegeben worden).» Die Verfasser Studie stellen fest, dass «die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten sowohl in Bezug auf Quantität als auch Qualität unzureichend waren; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands.» (vgl. S. 9 des Berichts).

Aufgrund eines solchen Befunds kann keine abgestützte Aussage gemacht werden. Das vom EJPD im Erläuterungsbericht präsentierte Ergebnis, die zu erwartenden Regulierungskostenfolgen seien unbedeutend, kann nicht zum Massstab für eine Entscheidung in einer derart wichtigen Angelegenheit genommen werden. Im Ergebnis ist festzuhalten, dass die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt werden konnte.

Auch in Bezug auf die Methodik sind Fragen angebracht. Die Studie (vgl. S. 6) unterscheidet drei Segmente von Unternehmen und suggeriert, dass die Mehrheit der Betriebe der KMU-Wirtschaft über eine „geringe datenschutzrechtliche Exponierung“ verfügt. In Anbetracht der fortschreitenden Digitalisierung der KMU-Wirtschaft muss diesem Befund entschieden widersprochen werden. Auch ein Coiffeursalon oder eine Papeterie verfügt über Kundendaten. Zudem nimmt der online-Verkauf (gerade in Papeterien) stetig zu. Jedes Unternehmen und zunehmend Klein- und Mittelbetriebe setzen moderne Informatikmittel ein, betreiben Internetseiten und Social Media-Profile und bearbeiten damit Personendaten. Kleine Unternehmen nutzen überdurchschnittlich viel cloudbasierte Internetapplikationen oder beziehen ihre Geschäftssoftware aus der Cloud mit Datenspeicherungen im Ausland (z.B. in den USA).

In der Botschaft fehlen Angaben über die Folgekosten. In der Studie von PwC werden zumindest einige Schätzungen vorgenommen. Die Handlungspflicht wird allerdings als «nicht besonders kostentreibend» (S. 29) eingeschätzt. Dieser Einschätzung widerspricht der sgv. Gerade in der KMU-Wirtschaft bei teils sehr geringen Margen gibt es keine zusätzlichen personellen Kapazitäten, diese Handlungs- und Informationspflichten in der Praxis auch zu erfüllen.

Nur schon durch den Zusammenzug der in der PwC-Studie vorhandenen, groben Kostenschätzungen, wird der riesige Umsetzungsaufwand sichtbar. Dass die Botschaft des Bundesrates die Folgekosten mit keinem Wort erwähnt, geschweige denn einen Versuch unternimmt, diese auszuweisen, ist enttäuschend.

Handlungspflichten nach VE-DSG	**Einmalig**	**Wiederkehrend**	**Kosten CHF**
Informationspflichten			
Pflicht zur Information der betroffenen Person	60 – 100 Stunden	30 Stunden	3'000 – 40'000
Auskunft über Aufbau der Datenbearbeitung	4- 12 Stunden	1.6 h – 3 Tage pro Fall	Keine Angabe
Informationspflicht Automatisierte Entscheidungen	30 – 50 Stunden	3 Stunden pro Fall	10'000
Meldung Data Breach	5 – 20 Stunden	2 – 5 Stunden pro Fall	5'000 – 10'000
Datenherrschaft			
Mitteilung, Löschung, Beschränkung	14 – 20 Stunden	3 Stunden pro Fall	100 – 5'000
Pflichten auf Datenübertragbarkeit	12 Stunden	2 Stunden pro Fall	7'500
Unternehmensinterne Datenschutzorganisation			
Datenschutz-Folgeabschätzung[1]		20 – 160 h pro Fall	5'000 – 30'000
Privacy by Default	1 – 40 Stunden		500 – 5'000
Betriebliche Datenschutzbeauftragter		500 – 2'000 h pro Jahr	
Grenzüberschreitender Datenverkehr			
Genehmigung Standard Datentransfervereinbarung	50 Stunden		5'000

Wenn die Aufgaben in Betracht gezogen werden, die alle Unternehmen beachten müssen und als Basis Minimalschätzungen als Grundlage für eine Hochrechnung angenommen werden, können sich im Durchschnitt mehrere Tausend Franken Regulierungskosten pro Unternehmen ergeben.

Aufgrund der methodischen Fehlbeurteilung wird in Verbindung mit der mangelhaften Datenerhebung bei den Unternehmen sichtbar, dass einerseits die Regulierungsfolgenabschätzung nicht korrekt durchgeführt wurde und andererseits die Regulierung für die gesamte Wirtschaft massiv höhere Kosten zur Folge hat.

Keine Ausweitung der Kompetenzen für den EDÖB

Ebenfalls Gegenstand der Gesetzesrevision sind erheblich ausgeweitete Untersuchungs- und Aufsichtsbefugnisse des EDÖB, die der sgv ablehnt.

[1] In einer Studie der Europäischen Union zur Datenschutz-Folgeabschätzung (Privat Impact Analysis) wurden die Kosten pro Durchführung auf € 14'000 – 149'000 geschätzt. Quelle: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, Seite 70.

Völlig überschiessende Strafbestimmungen

Was in den vergangenen Jahren im Rahmen von Volksinitiativen mehrfach kritisiert worden ist (z.B. «Pädophile sollen nicht mehr mit Kindern arbeiten dürfen», «Unverjährbarkeit pornografischer Straftaten an Kindern» oder «Lebenslange Verwahrung für nicht therapierbare, extrem gefährliche Sexual- und Gewaltstraftäter» macht der Bundesrat jetzt selbst, in dem er mit seinen Anträgen auf völlig unverhältnismässig hohe Strafen das Strafnormgefüge insgesamt durcheinander zu bringen droht. Strafverschärfungen wie Bussen bis 500'000.- oder Freiheitsentzug bis 3 Jahre für Widerhandlungen im DSG schiessen weit übers Ziel hinaus. Auch sind die Straftatbestände nicht klar abgefasst. Die Totalrevision des Datenschutzgesetzes darf nicht in eine Kriminalisierung der Unternehmen bzw. verantwortlicher Privatpersonen münden. Keinesfalls dürfen Verstösse gegen Dokumentations- oder Meldepflichten an den Beauftragten sanktioniert werden.

Die Schweiz als digitaler Datentresor

Der Bundesrat hat unlängst eine Strategie «Digitale Schweiz» verabschiedet, die den Nutzen der Digitalisierung und der Daten betont, was Unternehmen aber auch Konsumenten neue Perspektiven eröffnet. Das Datenschutzgesetz darf diesem Geist nicht widersprechen. Entwicklung und Innovation dürfen durch den Datenschutz ebenso wenig behindert wie durch das Datenschutzgesetz nur die Risiken betont werden. Eine Kultur der Verbote und des Bestrafens ist ein falscher Ansatz. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten. Ebenso ist eine Flut von Meldungen und Dokumentationspflichten zu unterbinden.

Gesamtwürdigung

Effektiver Nutzen, praktikabel, darf die Unternehmen nicht mit einem übermässigen administrativen Aufwand belasten Insgesamt fehlt eine vernünftige Anwendbarkeit für alle. Der Entwurf schadet der Wettbewerbsfähigkeit der Unternehmen. Insgesamt lehnt der sgv die Totalrevision des DSG in der vorliegenden Form, wie sie in die Vernehmlassung geschickt worden ist, ab. Die Revision hat mit Forderungen wie Informations- und Handlungspflichten für Firmen zu viele negative Auswirkungen auf die Unternehmen. Mit der Revision ist ein erneuter Bürokratieschub zu erwarten, unter welchem vor allem das Gewerbe leiden wird.

Der Schweizerische Gewerbeverband sgv hat im Rahmen dieser Vernehmlassung ausserordentlich viele Zuschriften und Stellungnahmen von Mitgliedverbänden und anderen Organisationen erhalten, die allesamt kritisch zum vorliegenden Revisionsentwurf Stellung nehmen. Die einzelnen Stellungnahmen umfassen zusätzlich branchenspezifische Besonderheiten, die der sgv in der Gesamtheit in seiner Stellungnahme nicht abbilden kann. Der sgv unterstützt die Stellungnahmen folgender Verbände:

AM Suisse, Schweizerischer Baumeisterverband SBV, Schweizerischer Verband Creditreform SVC, hotelleriesuisse, Verband der Kantonalbanken, UPC Cablecom, Verband Schweizerischer Inkassotreuhand-Institute vsi, Verband Schweizerischer Vermögensverwalter (VSV).

Zu den einzelnen Bestimmungen nehmen wir in der beiliegenden Übersicht Stellung.

Wir danken für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Schweizerischer Gewerbeverband sgv

Hans-Ulrich Bigler
Direktor, Nationalrat

Dieter Kläy
Ressortleiter

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schweizerischer Gewerbeverband sgv

Abkürzung der Firma / Organisation : sgv

Adresse : Schwarztorstrasse 26, 3001 Bern

Kontaktperson : Dieter Kläy

Telefon : 031 380 14 45

E-Mail : d.klaey@sgv-usam.ch

Datum : 3. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
sgv	Vgl. Begleitschreiben zu dieser Tabelle

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Zweck, Geltungsbereich und Begriffe	DSG	1			Nicht nur die juristischen Personen, sondern auch die im HR eingetragenen Einzelunternehmen und Mitglieder von Personengesellschaften sind vom Schutz auszunehmen, den das DSG für von einer Datenbearbeitung betroffene Personen vorsieht. Die Abgrenzung der geschützten von den nicht geschützten Personenkategorien ist in dieser Form nicht sachgerecht. Im HR eingetragene Einzelfirmen oder Mitglieder von Personengesellschaften wären datenschutzrechtlich vielmehr gleich zu behandeln wie juristische Personen. Die strafrechtlichen Bestimmungen über den Schutz der Ehre und das Verbot des wirtschaftlichen Nachrichtendienstes sowie der Persönlichkeitsschutz gemäss Art. 28ff. ZGB (die für diese Kategorien auch weiterhin gelten würden), wären aus Sicht des sgv ausreichend.
sgv	DSG	2	2	lit. c	Bei hängigen Verfahren soll das DSG – wie im geltenden Recht – nicht anwendbar sein. «Dieses Gesetz ist nicht anwendbar sein auf hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren». Der Entwurf will in Art. 2 Abs. 2 lit. c nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung nicht mehr gelten. Dies öffnet Missbräuchen Tür und Tor (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).
sgv	DSG	3		lit. c. Ziff. 3 und 4	Die Begriffe «genetische Daten» und «biometrische Daten» sollen insoweit präzisiert werden, als dass nur jene biometrischen bzw. genetischen Daten besonders schützenswert sollen sein, die zum Zweck der Identifizierung bearbeitet werden. Die Forschung hingegen soll nicht tangiert werden. Es muss möglich sein, durch die Untersuchung von genetischen Daten Mechanismen zu erforschen. Die

					Identität der DNA-Spender ist dabei nicht von Interesse und deren Identifizierung wird nicht bezweckt.
sgv	DSG	3		lit. c. Ziff. 5	Die Bestimmung ist in dieser allgemeinen Form ist nicht praktikabel. Ein künftiger Vertragspartner, z.B. ein Arbeitgeber, muss – wenn es arbeitsrelevant ist – Kenntnis über verwaltungs- und strafrechtliche Sanktionen erhalten können (z.B. Lastwagenchauffeur, dem der Führerausweis entzogen worden ist.
sgv	DSG	3		lit. f.	Bestimmung f ist ersatzlos zu streichen. Am heute gültigen Begriff «Persönlichkeitsprofil» soll festgehalten werden. Der im Gesetzesentwurf vorgeschlagene Begriff des "Profiling" weitet den Geltungsbereich übermässig aus. Jegliche Art von Voraussage soll unmöglich gemacht werden, was ein massiver Eingriff in die Wirtschaftsfreiheit ist. Auswertungen vornehmen und Prognosen abgeben liegen in der Natur der modernen Werbewirtschaft und ist notwendig, ein auf die Kundschaft zugeschnittenes Angebot zu machen. Mit den verbundenen Einschränkungen im Rahmen des Profilings droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem heute gültigen DSG weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind. Dazu gehören z.B. wirtschaftliche Verhältnisse, die Solvenz, das Zahlungsverhalten etc., Daten, die vor Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden (vgl. Botschaft des Bundesrates vom 23. März 1988, S. 446). Sowohl für die betroffenen Firmen im Einzelnen wie auch volkswirtschaftlich wäre eine Ausweitung eines Verbotes schädlich. Die Wirtschaft benötigt verlässliche Daten für die Befriedigung der Kundenwünsche. Die vorgeschlagene Revision und Anpassung des Begriffs schiesst weit über das Ziel hinaus. Der "Profiling" Begriff ist zu unbestimmt und gefährdet dadurch die Rechtssicherheit. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem "Persönlichkeitsprofil" des geltenden Rechts abzulehnen.
sgv	DSG	Art. 3		lit. h	Statt vom «Inhaber der Datensammlung» ist nun vom «Verantwortlichen» die Rede. Als Verantwortlicher gilt die private Person oder das Bundesorgan, das über den Zweck, die Mittel und den Umfang der Datenbearbeitung entscheidet. Gemäss erläuterndem Bericht müssen daher zwei Kriterien erfüllt sein: Verantwortlicher ist, wer einerseits festlegt, zu welchen Zwecken die Daten bearbeitet werden und andererseits, mit welchen Mitteln dies erfolgt. Das entscheidende Kriterium ist somit, wer über die Mittel zur beabsichtigten Datenbearbeitung bestimmt. Dies kann insbesondere im

					Zusammenhang mit der Auftragsdatenbearbeitung zu Abgrenzungsschwierigkeiten führen. Wenn das outsourcende Unternehmen keinen Einfluss auf die konkreten Mittel hat, mit denen der Outsourcingnehmer die Daten bearbeitet (was insbesondere bei grossen international tätigen Dienstleistern der Fall sein wird), dann wird sich aufgrund dieser Bestimmung die Frage stellen, wer als Verantwortlicher zu gelten hat und welche Rechtsfolgen damit verbunden sind. Die bisherige Terminologie (einschliesslich der "Datensammlung") sollte beibehalten werden. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu unklaren - teilweise unsinnigen - Aufteilungen der Verantwortung und Doppelspurigkeiten. Offenbar wird zudem übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen kann. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Daten-schutz-Folgeabschätzung (für den "Verantwortlichen"?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den "Verantwortlichen?") geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den "Verantwortlichen"?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht. Unklar ist auch, ob Arbeitnehmer unter den Begriff des "Auftragsbearbeiters" fallen können, was dem Wortlaut und der Systematik entspräche, aber offensichtlich zu einer völlig ausufernden Verantwortlichkeit führen würde.
Allgemeine Datenschutz-bestimmungen	DSG	Art. 4	Abs. 3		Das Wort "klar" ist zu streichen. Es ist nicht ersichtlich, was für eine Person ein «klar» zu erkennender Beschaffungszweck ist. Die Formulierung schafft Rechtsunsicherheiten und die Frage, was klar ist bzw. welches die Voraussetzungen für diese Klarheit bestehen sollen.
sgv	DSG	Art. 4	Abs. 4		Der Passus, wonach «Personendaten nur solange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt», ist ersatzlos zu streichen. Diese Bestimmung würde eine Pflicht zur Löschung beinhalten in dem Moment, als der Zweck der Bearbeitung nicht mehr gegeben ist. Diese Forderung ist unklar. Zudem hätte ihre Umsetzung einen grossen administrativen Aufwand zur Folge.
sgv	DSG	Art. 4	Abs. 5		Es ist das bisherige Wording gemäss Art. 5 Abs. 1 des geltenden DSG zu verwenden, da es klarer ist: «Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im

					Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.»
sgv	DSG	Art. 4	Abs. 6		Neu schreibt das DSG vor, dass eine gültige Einwilligung eindeutig zu erfolgen hat. Was dies genau bedeutet, wird im erläuternden Bericht nicht erklärt. Die Bestimmung ist zu streichen. Eine Einwilligung soll sich auf die besonders schützenswerten Personendaten beschränken.
	DSG	Art. 5	Abs. 2		Die Bestimmungen in Abs. 2 und 3 sind unklar. Daten sollten wohl nur ins Ausland übermittelt werden können, wenn entweder die Voraussetzungen von Abs. 2 (Feststellung des angemessenen Datenschutzes im Zielland durch den Bundesrat) oder eine der Ausnahmen von Abs. 3 vorliegen.
sgv	DSG	Art. 5	Abs. 3	Ziff. d	Personendaten dürfen – kommt Abs. 2 nicht zum Tragen – nur ins Ausland gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch einen völkerrechtlichen Vertrag; spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde und standardisierte Garantien. Diese Genehmigungspflicht verbindlicher Datenschutzvorschriften ist ersatzlos zu streichen. Zudem ist nicht verständlich, was «spezifische» und was «standardisierte» Garantien durch Vertrag» sein sollen.
sgv	DSG	Art. 5	Abs. 4 bis 6		Streichen der Informationspflichten. Eine Frist von sechs Monaten (vgl. Abs. 5), die zudem durch die Nachforderung von Informationen durch den EDÖB verlängerbar ist, macht ein Genehmigungsverfahren nicht praktikabel und führt zu unzumutbaren Verzögerungen bei Auslandstransfers.
sgv	DSG	Art. 6	Abs. 2		Die Verpflichtung, den EDÖB trotz Ausnahmetatbestand zu informieren, ist zu streichen, da die Massnahme unverhältnismässig ist und in zeitkritischen Momenten zur Anwendung kommend dürfte. Damit ist die Massnahme auch nicht praktikabel. Zudem ist es fraglich, ob die Flut der Meldungen durch den EDÖB bewältigt werden kann.
sgv	DSG	Art. 7	Abs. 2		Neu muss sich der Verantwortliche vergewissern, dass der Auftragsbearbeiter sowohl die Datensicherheit als auch die Rechte der betroffenen Person gewährleisten kann. Es ist unklar, welche Pflichten dem Auftragsbearbeiter damit überbunden werden. Zudem kann der Auftragsbearbeiter nicht sämtliche Rechte der betroffenen Personen gewährleisten, weshalb ist diese Bestimmung zu streichen

					ist. Die Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters präzisieren zu können, soll ersatzlos gestrichen werden.
sgv	DSG	Art. 7	Abs. 3		Die Regelung, dass ein Auftragsbearbeiter die Bearbeitung «nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen» übertragen darf ist zu bürokratisch. Es soll die Möglichkeit einer generellen Einwilligung geschaffen werden können. In der DSGVO – auf welche diese Bestimmung offensichtlich Bezug nimmt – wird ausdrücklich klargestellt, dass auch eine generelle Einwilligung möglich ist, die noch keinen Bezug auf bestimmte Unter-Auftragsbearbeiter nimmt. Zu denken ist etwa an eine entsprechende Klausel im Vertrag zwischen Verantwortlichem und Auftraggeber, in welchem die Zustimmung pauschal erteilt würde.
sgv	DSG	Art. 8			Diese Bestimmung ist ersatzlos zu streichen. Es ist nicht die Aufgabe des EDÖB «Empfehlungen der guten Praxis» zu erarbeiten und dazu «interessierte Kreise» beizuziehen. Wenn schon sind Empfehlungen durch die Betroffenen selbst zu machen. Das entspricht auch dem Gedanken der Selbstregulierung. Zudem ist zu bezweifeln, dass der EDÖB aufgrund seiner beschränkten Kapazitäten dieser Erwartung wirklich gerecht werden kann.
sgv	DSG	Art. 9			Streichen als Folge von Art. 8 (vgl. oben).
sgv	DSG	Art. 11	Abs. 2		Streichen. Der Bundesrat soll keine Bestimmungen über die Mindestanforderungen an die Datensicherheit erlassen können. Auf übermässige Regulierung ist zu verzichten.
	DSG	Art. 12			Der Passus ist ersatzlos streichen. Es braucht keine Regelung zur Datenbearbeitung Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Auch der Persönlichkeitsschutz soll mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, reicht das allgemeine Berichtigungs- und Löschungsrecht. Die Umsetzung dieser Regelung wäre mit zu grossen Aufwänden bzw. zu Rechtsunsicherheit verbunden. Dies insbesondere auch, da Abs. 3 der Bestimmung besagt, dass Amts- oder Berufsgeheimnisse nicht geltend gemacht werden können. Streitfälle mit Erben, die gegen oder

					unabhängig von der Erbengemeinschaft vorgehen, sind ebenfalls vorprogrammiert; sie sollen zudem sogar mehr Rechte haben als die betroffene Person selbst. Unklar ist, wie eine verstorbene Person ein "überwiegendes Interesse" geltend machen kann haben?
sgv	DSG	Art. 13	Abs. 1 und 2		Die Informationspflicht wird auf sämtliche Personendaten ausgeweitet, was zu erheblichem Mehraufwand für die Unternehmen führen wird. Unklar ist, was mit bisherigen bzw. früher erarbeiten Daten geschehen soll. Da sie nicht erwähnt sind kann davon ausgegangen werden, dass diese nicht unter das neue DSG fallen und damit altrechtlich zu behandeln sind. Eine generelle Informationspflicht z.B. durch Publikation auf einer Webseite oder in den AGB muss soll explizit vorgesehen werden, andernfalls eine Informationspflicht an alle nicht praktikabel ist und Art. 13 ff. zu streichen ist. Es gibt datenverarbeitende Unternehmen, die aus Natur der Sache keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben bzw. haben können, deren Daten sie verarbeiten. Diese Unternehmen, z.B. Auskunfteien und Inkassounternehmen könnten unter Berufung auf Art. 13 gezwungen werden, Hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. Das ist völlig inakzeptabel. Es muss genügen, dass diese Informationen auf einfache Art und Weise öffentlich zugänglich gemacht werden.
sgv	DSG	Art. 13	Abs. 3 und Abs. 4		Die Begriffe «Dritter» und «Empfängerinnen und Empfänger» sind nicht klar definiert, ebenso wenig wie die Differenzierung zwischen «Beschaffung» und «Bearbeitung». Hier weiter Der gesamte Absatz ist unklar formuliert, was insbesondere die Abgrenzung der Pflichten des Verantwortlichen und des Auftragsdatenbearbeiters betrifft. Der VUD ist daher der Meinung, dass Abs. 3 ersatzlos zu streichen ist. Art. 13 Abs. 4 VE-DSG geht weit über die DSGVO hinaus und ist als «Swiss Finish» abzulehnen. Die Bestimmung, die übrigens ebenfalls unklar formuliert ist, ist zu streichen.

					Dieser Absatz fordert im Falle einer Bekanntgabe von Personendaten an Dritte, dass die Empfänger den betroffenen Personen mitgeteilt werden müssen. Eine voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" lehnt der sgv ab. Wie bis anhin müssen "Kategorien" genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, wo persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger irgendwelcher Informationen zu kennen ist in der Praxis gar nicht handhabbar. Datenbearbeitende Unternehmen würden faktisch zur Offenlegung ihrer Kundenkreise und damit ihrer Geschäftsgeheimnisse gezwungen. Mit in Betracht zu ziehen ist die Tatsache, dass auch innerhalb eines Konzerns Daten weitergegeben würden. Das würde ebenfalls verunmöglicht. Für Absatz 4 soll die Kategorienregelung sinngemäss gelten.
sgv	DSG	Art. 13	Abs. 5		Diese Regelung verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Unmittelbar nach der Beschaffung werden die Daten gespeichert und wohl erst nachher überhaupt gelesen. Deshalb ist der Passus ersatzlos zu streichen, da es sich um einen Swiss Finish handelt, der über die EuDSGVO hinausgeht. Die Forderung, dass wenn Personendaten nicht bei der betroffenen Person beschafft werden, die betroffene Person spätestens bei der Speicherung der Daten informiert werden muss, hat einen unverhältnismässigen administrativen Aufwand zur Folge. Eine allfällige aktive Informationspflicht ist maximal auf die Bearbeitung besonders schützenswerter Daten zu beschränken.
sgv	DSG	Art. 14	Abs. 1		Generelle Bemerkung zu Art. 14: Die Berufung auf ein überwiegendes privates Interesse ist nicht möglich, wenn Daten einem Dritten weitergegeben werden, z.B. wenn Daten innerhalb eines Konzerns verschoben werden (z.B. von der Mutter- an die Tochtergesellschaft oder unter Tochtergesellschaften). (was z.B. auch eine Konzerngesellschaft sein kann). Für diese Einschränkung gibt es keinen Grund und sie sollte gestrichen werden. Sie würde in manchen Fällen und ganz besonders in Konzernverhältnisse zu einem enormen administrativen Mehraufwand, der in der Sache aber nicht zu mehr Transparenz für die Betroffenen führt. Die Fälle, in denen ein überwiegendes privates Interesse in der Regel besteht, sollten analog zu Art. 24 VE-DSG aufgeführt werden (vgl. die Ausführungen zum Auskunftsrecht).

					Absatz 1 soll um den Fall ergänzt werden, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung), in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist.
sgv	DSG	Art. 14	Abs. 2		Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerten Personendaten bearbeitet werden. Auch diese sollen von der Informationspflicht und den Einschränkungen ausgenommen werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten nur schon angesichts der drakonischen Strafen, die der Vernehmlassungsentwurf für Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
sgv	DSG	Art. 14	Abs. 4	lit. a	Das Kriterium der fehlenden Weitergabe von Personendaten an Dritte soll gestrichen werden. Die Weitergabe von Daten innerhalb eines Konzerns würde unnötig erschwert.
sgv	DSG	Art. 15	Abs. 1		Ersatzlos streichen, da es sich um einen zu weitgehenden Vorschlag handelt, Konsumenten vor jedweder Art von automatisierten Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgendeiner Weise argumentierbar sein, und was eine "erhebliche Auswirkung ist, dürfte letztlich von der Sensibilität des Betroffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte Art. 22 DSGVO EU nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstatten vor - eine Abweichung wäre demnach zweifellos auch für die Schweiz zulässig. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Die Formulierung der "Auswirkungen" ist so breit, dass jeder kommerzielle Entscheid - z.B. über eine Lieferung von Ware gegen Rechnung - darunterfallen kann. Auch die Lieferung von Ware gegen

					Rechnung ist in keiner Weise zwingend, und die Verweigerung darf nicht begründungspflichtig werden. Zudem haben wir auch hier wiederum den Fall eines Swiss Finish. Die Informationspflicht muss erfüllt werden, wenn die automatisierte Einzelentscheidung *rechtliche Wirkungen oder erhebliche Auswirkungen* auf die betroffene Person hat. Damit unterscheidet sie sich damit im Wortlaut von Art. 22 DSGVO und Art. 8 Abs. 1 Bst. a der E-SEV 108, wo man von *erheblichen* Auswirkungen ausgeht.
sgv	DSG	Art. 16			Der ganze Artikel ist zu streichen da viel zu breit formuliert «...führt die vorgesehene Datenbearbeitung *voraussichtlich* zu einem erhöhten Risiko…». In der Konsequenz würde jedes Unternehmen verpflichtet, eine "Folgeabschätzung" vorzunehmen, wenn es mehr tut, als die Daten seiner eigenen Kunden zu bearbeiten. Die Frage, ob ein erhöhtes Risiko vorliegen kann, kann unter Umständen erst nach der Durchführung einer Datenschutz-Folgenabschätzung beantwortet werden, was unbefriedigend ist. Eine solche Prüfung wird aber nötig sein, da die Bestimmung unter Androhung einer Strafe gilt. Dies wird dazu führen, dass in der Praxis auch für Bearbeitungen, für die keine formale Datenschutz-Folgeabschätzung erforderlich ist, eine solche durchgeführt werden muss, was nicht Sinn der Sache ist, da es unnötigen Aufwand darstellt und personelle Kräfte bindet. Missbräuche werden kaum verhindert. Die Regulierungsfolgeabschätzung ist für den Bundesrat eine Pflicht. Gleichzeitig werden immer neue Verpflichtungen für die Unternehmungen eingeführt, wie das vorliegende Beispiel der Datenschutzfolgeabschätzung zeigt. Eine Frist von drei Monaten (Abs. 4), innerhalb welcher «der Beauftragte Einwände gegen die vorgesehenen Massnahmen dem Verantwortlichen oder dem Auftraggeber mitteilt, ist viel zulange und für Projekte nicht praxistauglich.
sgv	DSG	Art. 17			Art. 17 beinhaltet eine Selbstanzeige, falls der Verantwortliche Daten verliert oder eine unbefugte Datenbearbeitung vornimmt. Dieser Passus ist ersatzlos zu streichen. Zudem findet er auf jede Datenschutzverletzung Anwendung und geht weiter als die Regelung in der EuDSGVO, die eine Selbstanzeige nur dann fordert, wenn Schutzmassnahmen versagt haben und daraus tatsächlich ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Das «unverzügliche» Vornehmen einer «unbefugten Datenbearbeitung» nach Art. 17 Abs. 1 VE-DSG birgt in sich sehr viel Unklarheit und könnte zu einer Flut von Selbstanzeigen führen, die den Apparat des EDÖB völlig unnötigerweise belasten würde. Die Pflicht zu einer Selbstanzeige ist systemfremd und bricht mit dem Grundsatz, sich nicht selbst

					belasten zu müssen. Die Aufnahme einer solchen Bestimmung hätte Präzedenzcharakter und ist nur schon aus diesem Grund entschieden abzulehnen. Die Informationspflicht des Verantwortlichen gegenüber der betroffenen Person (Art. 17 Abs. 2 VE DSG) auf Geheiss des Datenschutzbeauftragten oder «wenn es zum Schutz der betroffenen Person erforderlich ist» schiesst in der allgemeinen Formulierung über das Ziel hinaus.
sgv	DSG	Art. 18			Die Forderung, «angemessene Massnahmen zu treffen, die … Verletzungen vorbeugen», ist bereits durch die Prinzipien der Richtigkeit, Verhältnismässigkeit und Zweckbindung abgedeckt und kann deshalb ersatzlos gestrichen werden.
sgv	DSG	Art. 19			Die «weiteren Pflichten», die «Datenbearbeitung zu dokumentieren» und «die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung, oder Vernichtung von Daten, über Verletzung des Datenschutzes.... zu informieren» sind in der Praxis nicht oder nur mit unverhältnismässigem Aufwand umsetzbar, sondern ergeben auch gegenüber dem Betroffenen keinen Sinn, da ständig Korrekturen, Löschungen, etc. vorgenommen werden und der Empfänger mit Mitteilungen geflutet werden könnte. Besonders die Informationspflicht gemäss lit. b. ist nicht umsetzbar. Es kann z.B. nicht sein, dass der Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben. Der Passus schafft vor allem Rechtsunsicherheit und könnte Millionen von unnötigen Mitteilungen auslösen. Der Nutzen einer solchen Regelung ist völlig unklar. Art. 19 VE DSG ist deshalb ersatzlos zu streichen.
	DSG	Art. 20			Bezüglich Auskunftsrecht fehlt eine wirksame Klausel, die den Missbrauch verhindern kann. Zweckentfremdete bzw. datenschutzfremde Nutzung zur Beweismittelausforschung darf unter dem Deckmantel des Datenschutzes nicht Einzug halten. Im Auskunftsrecht ist neu eine Pflicht zur Begründung jeglicher Entscheide versteckt, welche auf einer Bearbeitung von Personendaten basieren, was ein Eingriff in Freiheit des Unternehmens ist und über die EuDSGVO hinausgeht.
Rechte der betroffenen Person	DSG	Art. 20	Abs. 2	lit. e	lit e) kann gestrichen werden, da in aller Regel das Vorliegen einer automatisierten Einzelentscheidung (z.B. im Online-Handel) sowieso ersichtlich ist.

sgv	DSG	Art. 20	Abs. 2	lit. f	Diese Bestimmung kann die Preisgabe von Geschäftsgeheimnissen zur Folge haben und ist ersatzlos zu streichen.
sgv	DSG	Art. 20	Abs. 3		Art. 20 Abs. 3 ist zu streichen. Die Information über eine automatisierte Einzelentscheidung wird durch das Zustandekommen eines Vertrags (oder die Ablehnung) z.B. im Online-Handel bereits mitgeteilt.
Besondere Bestimmungen für die Datenbearbeitung durch private Personen	DSG	Art. 23	Abs. 2	lit. d	„Profiling ohne ausdrückliche Einwilligung der betroffenen Person“ ist ersatzlos zu streichen. Diese Anforderung ist unbegründet.
Rechtfertigungs-gründe	DSG	Art. 24	Abs. 2		Statt „ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben“ besser „ein…. wird vermutet“.
sgv	DSG	Art. 24	Abs. 2	lit. a	Das Wort „unmittelbar“ ist zu streichen.
sgv	DSG	Art. 24	Abs. 2	lit. c Ziff. 3	Da die Volljährigkeit häufig weder bekannt noch eruierbar ist, ist der Passus zu streichen.
Rechtsansprüche	DSG	Art. 25	Abs. 2		Die Pflicht zur Anbringung eines "Bestreitungsvermerks" ist zu streichen.
sgv	DSG	Art. 25	Abs. 3		Die Pflicht zu einer Mitteilung von Urteilen an Dritte oder zur Publikation ist ersatzlos zu streichen. Nicht einmal die EuDSGVO kennt diese Verpflichtung
	DSG	Art. 27			Diese Bestimmung ist zu überarbeiten. Da die Bestimmung neu eine Grundlage in einem formellen Gesetz verlangt, wenn ein automatisierter Einzelfallentscheid erfolgen soll, werden Bundesorgane künftig ihre Prozesse nicht mehr automatisieren dürfen, selbst wenn dies aus Gründen der Effizienz sachgerecht ist, da die erwähnten Grundlagen regelmässig fehlen und auch im Vorentwurf nicht

					vorgesehenen sind. Ein Beispiel ist die heute bei einigen Krankenkassen weitgehend automatisierte Beurteilung von Rückerstattungsanträgen bei der gesetzlichen Krankenversicherung. Diese werden wieder manuell abgewickelt werden müssen, was zu deutlichen Mehrkosten führen wird.
Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen	DSG	Art. 28	Abs. 1 und Abs. 2		Der Bundesrat kann gemäss dieser Vorschrift vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling unter gewissen Voraussetzungen bewilligen. Diese Regel ist entweder für alle zu ermöglichen oder ganz zu streichen, aber nicht einseitig zugunsten des Staats auszugestalten.
EDÖ	DSG	Art. 37	Abs. 1		Das Parlament soll gemäss Pa. Iv. (16.409) die Kompetenz erhalten, den EDÖB zu wählen. Der Bundesrat hat lediglich ein Vorschlagsrecht.
sgv	DSG	Art. 37	Abs. 4		Das Budget des EDÖB ist durch das Parlament zu genehmigen.
sgv	DSG	Art. 38	Abs. 2		Der Passus, wonach der Bundesrat «nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlichen Gründen die Nichtwiederwahl verfügt, der Beauftragte wiedergewählt ist», ist ersatzlos zu streichen. Die zweimalige Wiederwahl soll durch das Parlament erfolgen.
sgv	DSG	Art. 39	Abs. 2		Nach Abs. 2 bewilligte Nebenbeschäftigungen müssen offengelegt werden.
sgv	DSG	Art. 41	Abs. 4		Dass ausserhalb eines Untersuchungsverfahrens der EDÖB überprüfen können soll, ob private Personen die Datenschutzvorschriften einhalten, lehnt der sgv ab. Ohne konkreten Anlass soll es keine Überprüfung Privater geben können. Der Passus ist auf die Beraterfunktion zu reduzieren.
sgv	DSG	Art. 42			Art. 42 betreffend vorsorglicher Massnahmen und Beizug der Polizei für ihre Vollstreckung ist ersatzlos zu streichen. Der sgv lehnt eine Datenschutzpolizei ab. Es ist rechtsstaatlich verwerflich, einer einzigen Amtsperson derartige Kompetenzen zuzuschreiben. Vorsorgliche Massnahmen werden zudem von Gerichten angeordnet.

sgv	DSG	Art. 43	Abs. 1		Abs. 1 von Art. 43 über Verwaltungsmassnahmen ist ersatzlos zu streichen. Es ist nicht nachvollziehbar, weshalb der EDÖB derartige Kompetenzen wie z.B. die Anordnung der Vernichtung von Daten erhalten soll.
sgv	DSG	Art. 44	Abs. 3		Der Entzug aufschiebender Wirkung soll durch eine gerichtliche Instanz angeordnet werden, nicht durch den EDÖB selbst. Vorsorgliche Massnahmen im Bereich der Datenbearbeitung können massive Konsequenzen für Unternehmen haben, ja können einen Betrieb lahmlegen. Die Erfahrungen haben gezeigt, dass der EDÖB vorsorgliche Massnahmen auch ohne vertieftes Abwägen der Folgen solcher verlangt. Eine unabhängige Überprüfungsmöglichkeit ist daher entscheidend, und bis diese stattfindet, muss eine aufschiebende Wirkung bestehen.
sgv	DSG	45			Die Anzeigepflicht durch den EDÖB ist ersatzlos zu streichen. Der EDÖB soll ein Recht haben, Anzeige zu erstatten.
sgv	DSG	49			Die «weiteren Aufgaben» des EDÖB hätten einen markanten Personalausbau zur Folge, sollten sie alles seriös umgesetzt werden. Für einen Ausbau fehlen allerdings die finanziellen Mittel, weshalb Art. 49 ersatzlos zu streichen ist.
Strafbestim-mungen	DSG	Art. 50			Art. 50 ist in der vorliegenden Form zu streichen. Bussen «bis 500'000.-» für private Personen sind völlig überrissen und unverhältnismässig. Die Verwaltung soll offensichtlich nicht behelligt werden, untersteht aber ebenfalls dem Datenschutzgesetz. Mit solchen Massnahmen wird die Verhältnismässigkeit im strafrechtlichen Gefüge ignoriert. Sie führen auch zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden. Die Folge davon wird sein, dass gesetzlich gewollte Spielräume bei der Datenbearbeitung aus Angst vor persönlicher Bestrafung nicht ausgeschöpft oder mit sehr viel mehr Bürokratie betrieben werden, als notwendig. Bei Vorsatz sind Bussen bis 10'000.- angemessen, bei Fahrlässigkeit maximal 5'000.-. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen angepasst, sicher nicht Beträge bis 500'000.-. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.00 für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Rahmen. Bussenbeträge über 100'000.- sind nicht bekannt. Bei Steuervergehen sind im Gesetz über die direkte Bundessteuer Bussen bis 50'000.-

					vorgesehen.
	DSG	Art. 51			Art. 51 ist in der vorliegenden Art zu streichen. Für die Verletzung von Sorgfaltspflichten sollen Bussen bis 500'000.- ausgesprochen werden können, was mit Blick auf das Strafgefüge von Bussen völlig überrissen ist.
sgv	DSG	Art. 52			Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist ebenfalls völlig unverhältnismässig. Es ist nicht nachvollziehbar, wieso eine derartige Kriminalisierung der Fehlbaren gerechtfertigt wäre. Art. 52 ist deshalb ersatzlos zu streichen. Zudem ist unklar, was unter "geheimen Personendaten" zu verstehen ist.
sgv	DSG	Art. 54			Die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet und nicht auf die Kantone abgewälzt werden.
sgv	DSG	Art. 55			Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109)
sgv	DSG	Art. 56			Nach dem Abschluss von Staatsverträgen durch den Bundesrat ist die Zustimmung des Parlaments einzuholen.
	DSG	Art. 59			Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen und diese nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken.
	StGB	Art. 179novies			Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe bestrafen zu wollen ist völlig überrissen. Zumindest müsste klargestellt werden, dass diese Strafe nachweisbar gegen den Willen der betroffenen Person erfolgt. Der Passus ist zu streichen.
sgv	ZPO	Art. 20 Bst. d, Art. 99 ABs. 3			Die zivilprozessualen Bestimmungen in den erwähnten Artikel sind zu streichen. Das Datenschutzrecht braucht keine speziellen prozessualen Regeln. Wo das Gesetz in Abweichung von den normalen Regeln von der Erhebung von Gerichtskosten absieht, geht es üblicherweise um Vertragsstreitigkeiten (Miete, Arbeitsvertrag, uam.). Wegleitend ist dabei die Annahme des Gesetzgebers, dass eine Partei

		Bst. d, Art. 113 Abs. 2 Bst. g, Art. 114 Bst. f, Art. 243 Abs. 2 Bst. d			besonders geschützt werden muss, weil sie in einem Abhängigkeitsverhältnis zur anderen steht. Im Datenschutzbereich werden oft keinerlei vertragliche oder persönliche Beziehungen zwischen dem Datenbearbeiter und dem Betroffenem bestehen. In dieser Konstellation ist nachgerade mit einer Flut von - durchaus auch mutwilligen - Klagen zu rechnen, wenn das Prozessieren kostenlos ist. Es gibt keinen Grund, einer Populärbeschwerde Vorschub zu leisten. Wie auf anderen Rechtsgebieten soll einem bedürftigen Kläger die unentgeltliche Prozessführung zur Verfügung stehen. Der solvente Kläger soll, wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist, seine Kostenrisiken abwägen müssen. Ebenso wenig gibt es einen Grund für vereinfachte Verfahren. Auch das leistet der Populärbeschwerde Vorschub. Zudem beschneidet das vereinfachte Verfahren die beklagte Partei in ihren Verfahrensrechten.
sgv					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
sgv	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
sgv	Der sgv kritisiert die Ausdehnung des Anwendungsbereichs der Konvention 108, die hier quasi durch die Hintertür vorgenommen wird. Bisher beschränkte sich die Konvention 108 auf die automatisierte Bearbeitung von Personendaten, während der Entwurf jede Art der Bearbeitung von Personendaten avisiert. Nachdem der VE DSG bereits stark auf das europäische Datenschutzrecht ausgerichtet ist, scheint der Abschluss eines zusätzlichen Übereinkommens - das zwangsläufig zu Überschneidungen, Redundanzen und vermeidbaren Rechtsunsicherheiten führt - von vornherein überflüssig. Nachstehend wird auf einige Bestimmungen hingewiesen, bei denen der VE DSG weitergeht, als er dies aufgrund des Entwurfstextes tun müsste:
Art. 5 Abs. 4 lit. d)	Die schrankenlose Nachführungspflicht, die der VE DSG einführen will, ist im Text des Konventionsentwurfs explizit relativiert ("wenn nötig").
Art. 8 Abs. 21 lit a) und Abs. 2	Der Entwurf würde explizit die Möglichkeit offenlassen, auf die impraktikablen Bestimmungen über die Informations- und Anhörungspflichten bei automatisierten Entscheidungen gemäss Art. 15 VE DSG zu verzichten. Insofern ist nicht einzusehen, wieso diese Bestimmung trotzdem in den VE aufgenommen werden musste. Der Schutz, den schon das geltende DSG für die von einer Datenbearbeitung Betroffenen vorsieht, würde auch für diese Fälle ausreichen.
sgv	Die Rechte und Freiheiten Dritter werden ausdrücklich als mögliche Gründe für eine Abweichung von bestimmten Kautelen der Konvention aufgeführt. Der VE DSG widerspiegelt dies nicht; die auf der Hand liegende Erkenntnis, dass - nicht nur, aber insbesondere - die umfassenden Informations- und Auskunftspflichten des VE DSG zu einem übermässigen Eingriff in die Rechte Dritter führen können, scheint nicht bis zu den Redigierenden des VE DSG vorgedrungen zu sein.
Art. 12 Abs. 5 und 6:	Es ist nicht zwingend, den Beauftragten über vertragliche Garantien zu informieren, die im grenzüberschreitenden Verkehr auszuhandeln sind, wenn das Bestimmungsland kein "angemessenes Datenschutzniveau" aufweist. Gemäss Art. 12bis Abs. 2 lit. b i.V. mit Art. 9 Abs. 3 ist auch die Einholung

	entsprechender Genehmigungen nicht zwingend.
Art. 12bis Abs. 2 lit. a - d, insb. lit. c)	Art. 9 Abs. 3 des Konventionsentwurfs ermöglicht den einzelnen Staaten ausdrücklich, die Befugnisse des Beauftragten eigenständig zu regeln. Insbesondere ist keine Verfügungskompetenz erforderlich. Die Kompetenzzuweisungen des geltenden Rechts hätten auch insofern problemlos beibehalten werden können.
sgv	

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
sgv		

simsa, Heinrichstrasse 235, 8005 Zürich

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

per E-Mail: Jonas.amstutz@bj.admin.ch

Zürich, 31. März 2017

Stellungnahme der simsa – Swiss Internet Industry Association zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Die simsa – Swiss Internet Industry Association ("simsa") ist der Interessenverband der Schweizer Internet-Dienstleistungsunternehmen. Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Vorentwurf des Datenschutzgesetzes ("VE-DSG"). In unserer Stellungnahme gehen wir exemplarisch und ohne Anspruch auf Vollständigkeit auf diejenigen Vorschläge des Vorentwurfs ein, welche für die Internetindustrie in der Schweiz besonders relevant sind.

Das Wichtigste in Kürze:

Starker Datenschutz und Datensicherheit sind wichtige Grundpfeiler für den Erfolg digitaler Geschäftsmodelle in der Schweiz. Der Austausch von Personendaten mit unseren Nachbarländern und anderen wichtigen Handelspartnern muss möglich bleiben, weshalb ein inhaltlich gegenüber der EU gleichwertiger Datenschutz zu erhalten ist. Das Schweizer Datenschutzgesetz (DSG) aus dem Jahr 1992 basiert auf allgemeinen Grundsätzen der Datenbearbeitung, die sich in der Praxis bewährt haben und die sich bisher auch erfolgreich auf digitale Sachverhalte anwenden liessen. Gemäss Beschluss der EU-Kommission vom 26. Juli 2000 verfügt die Schweiz über ein angemessenes Datenschutzniveau. Dieser Beschluss bleibt auch unter der ab 25. Mai 2018 verbindlichen EU Datenschutz-Grundverordnung (Verordnung EU 2016/679; DSGVO) weiterhin gültig. **Eine Teilrevision des DSG genügt, um den Herausforderungen der Digitalisierung zu begegnen und einen gegenüber der EU angemessenen Datenschutz zu erhalten.**

Für die Schweiz **im internationalen Verhältnis direkt verbindlich ist das (revidierte) Übereinkommen des Europarates (SEV 108)** zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener

Daten. Das Übereinkommen bedingt, wenn überhaupt, lediglich wenige Änderungen im DSG. Solange die Schweiz die SEV 108 einhält besteht auch für die EU kein Grund, auf den Angemessenheitsentscheid zurückzukommen und diesen zu revidieren. **Für eine Übernahme der in der DSGVO detailliert geregelten administrativen Pflichten bei der Datenbearbeitung sowie für hohe Bussen besteht in der Schweiz kein Anlass.**

Geradezu unverständlich ist, dass der VE-DSG verschiedene Pflichten der DSGVO nicht nur übernimmt, sondern diese gar noch verschärft. In dieser Stellungnahme weisen wir nur auf die wichtigsten dieser strengeren Regelungen hin, welche die Geschäftstätigkeit von Online-Dienstleistern und Betreibern digitaler Geschäftsmodelle in der Schweiz bedrohen. **Sämtliche Verschärfungen gegenüber den Regelungen der DSGVO sind aus dem VE-DSG zu entfernen.** Vor allem auf überschiessende Neben- und Administrativpflichten ist zu verzichten. Solche Pflichten erhöhen den Aufwand für die Schweizer Anbieter von Kommunikations- und Werbe-Diensten, IT-Beratung, Hosting-, Cloud-Lösungen und anderen Dienstleistern für digitale Geschäftsprozesse. Die Administrativpflichten stärken auch den Persönlichkeitsschutz der betroffenen Personen kaum. Um die Attraktivität des Dienstleistungsstandorts Schweiz zu erhalten, sind Pflichten und Einschränkungen für Schweizer Anbieter zu vermeiden, welche sogar über das von der EU geforderte Mass hinausgehen.

Besonders standortschädlich und abzulehnen ist das vorgeschlagene Sanktionswesen mit neuen Straftatbeständen. Der Verzicht auf drakonische Sanktionen im Stile der DSGVO (Bussen bis zum höheren Betrag von EUR 20 Mio. oder 4% des letzten weltweit erzielten Jahresumsatzes) ist zwar zu begrüssen. Der VE-DSG setzt darauf, die Verletzung von administrativen Nebenpflichten neu als Straftatbestände auszugestalten. Ins Visier geraten damit die natürlichen Personen in der Schweiz, welche für die Datenbearbeitung in Unternehmen verantwortlich sind. Nur wenn sich diese nicht identifizieren lassen, soll subsidiär das Unternehmen mit maximal CHF 100'000.— gebüsst werden. Für global tätige Online-Plattformen ohne Niederlassung in der Schweiz wäre eine solche Busse im Vergleich zu einer Sanktion in der EU ein kleines Übel. Schweizer Unternehmen – besonders KMU – hingegen müssten ihre Mitarbeiter mit grossem Compliance-Aufwand schützen und würden sich im Zweifel für eine konservativere Methode der Datenbearbeitung entscheiden. **Im Ergebnis wäre der VE-DSG gut für Beratungsunternehmen und Anwaltskanzleien, nicht aber für innovative Unternehmen, die in der Schweiz datengestützte Geschäftsmodelle betreiben möchten.**

Im Einzelnen:

Die Auftragsdatenbearbeitung ist nicht unnötig zu erschweren (Art. 7 ff. VE-DSG):

Die Informationspflichten sind auf ein verhältnismässiges Mass zu beschränken. Die vorgesehenen Pflichten sind zu unbestimmt. Die aktive Information muss z.B. alle Angaben umfassen, die für die betroffene Person "erforderlich" sind (Art. 13 Abs. 2 VE-DSG). Längere Datenschutzerklärungen bedeuten nicht automatisch eine bessere Information der betroffenen Person. Daher verfehlt die Informationspflicht das Regelungsziel der Stärkung von Kontrollmöglichkeiten der Betroffenen. Die sehr weit formulierte Informationspflicht widerspricht dem risikobasierten Ansatz, wie sie der Vorentwurf im Rahmen der Transparenzanforderung gemäss Art. 4 VE-DSG vorsieht.

Die Pflicht zur Information über die Identität und Kontaktangaben der Auftragsbearbeiter ist überschiessend (Art. 13 Abs. 4 VE-DSG). Der Verantwortliche müsste die betroffene Person, z.B. bei jedem Wechsel des Kommunikations-, Werbe-, IT-, Hosting- oder Beratungs-Dienstleisters, über die Identität und Adresse des neuen Anbieters informieren. Diese Information erhöht den Datenschutz und die Datensicherheit für die betroffene Person nicht, sondern führt zu einer kontraproduktiven Informationsflut. Die Information ist zudem in einer arbeitsteiligen, digitalen Geschäftswelt nicht praktikabel. Weder die SEV 108 noch die DSGVO verlangen die Angabe der Identität der Auftragsbearbeiter. Es ist nicht einzusehen, weshalb sich die Schweiz freiwillig einen massiven Standortnachteil auferlegen sollte.

Die Pflicht zur permanenten Datenüberprüfung ist in der Praxis nicht erfüllbar (Art. 4 Abs. 5 und Art. 19 Bst. b VE-DSG). Vor allem Auftragsbearbeiter sind von der Datenquelle zu weit entfernt, als dass sie Änderungsbedarf an den von ihnen bearbeiteten Daten erkennen können. Die Tätigkeit des Auftragsbearbeiters erfolgt immer im Auftrag des Verantwortlichen. Daher kann höchstens der Verantwortliche für die Richtigkeit der zur Verfügung gestellten Daten sorgen.

Auf strafrechtlich sanktionierte Informationspflichten des Auftragsbearbeiters gegenüber Datenempfängern ist zu verzichten (Art. 19 Bst. a VE-DSG). Daten werden tagtäglich angepasst, ergänzt oder gelöscht, weil die Daten nicht mehr notwendig sind oder an Relevanz verloren haben. Beispiele dafür sind die Archivbereinigung, der Abschluss der Leistungserbringung, die Begleichung der offenen Forderung durch den Kunden oder die Auflösung einer Geschäftsbeziehung. Es ist unverhältnismässig, wenn der Verantwortliche und der Auftragsbearbeiter in allen Fällen einer Berichtigung, Löschung oder Vernichtung von Daten alle Datenempfänger nachinformieren müssen. Die Informationspflicht ist auf Fälle zu begrenzen, in welchen die betroffene Person ein Begehren um Datenanpassung aufgrund schutzwürdiger Interessen gestellt hat. Die Mitteilung an Dritte soll höchstens dann erfolgen, wenn die betroffene Person dies aus berechtigten Gründen verlangt. Der Verantwortliche entscheidet über Zweck, Mittel und Umfang der Bearbeitung und ist damit auch in der Position, über den Bedarf für eine Datenanpassung zu befinden. Aus diesem Grund soll der Verantwortliche und nicht der Auftragsbearbeiter für die Mitteilung zuständig sein. So sieht es auch die EU vor (Art. 19 DSGVO).

Datenschutz-Folgenabschätzung, Privacy by Design und Privacy by Default sind keine Aufgaben des Auftragsbearbeiters (Art. 16 und 18 VE-DSG). Der Verantwortliche entscheidet über eine bestimmte Geschäftsaktivität und die damit zusammenhängende Datenbearbeitung. Die Pflichten zur Datenschutz-Folgenabschätzung, zur Sicherstellung des Datenschutzes durch Technik (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) setzen zu einem frühen Zeitpunkt in der

Planung an. Der Auftragsbearbeiter ist in diese Entscheidungsprozesse meist nicht involviert. Hat der Auftragsbearbeiter einen entsprechenden Auftrag vom Verantwortlichen erhalten, verfügt er meist trotzdem nicht über alle relevanten Informationen. Die genannten Pflichten sind für den Auftragsbearbeiter daher kaum umsetzbar. Gleichzeitig stellen die Sanktionsdrohungen für den Auftragsbearbeiter unverhältnismässig hohe Risiken dar. Auch die EU beschränkt die genannten Pflichten auf den Verantwortlichen (Art. 25 und 35 DSGVO). Die Schweiz sollte die in der Schweiz ansässigen Dienstleister nicht gegenüber den EU-Anbietern benachteiligen. Sofern der Verantwortliche Schutzmassnahmen festlegt, wird er diese zudem auch vertraglich auf den Auftragsbearbeiter überbinden, soweit sie die Auftragsbearbeitung betreffen.

Die Einwilligungsvoraussetzung für eine Unterbeauftragung ist nicht praktikabel (Art. 7 Abs. 3 VE-DSG). In einer arbeitsteiligen Welt muss der Auftragsbearbeiter flexibel und zeitnah Unteraufträge vergeben können (z.B. eine Marketingagentur für die verschiedenen Elemente und Teilleistungen einer online Kampagne, ein Registrar und Hosting-Anbieter für verschiedene Elemente seines Domain- und Hosting-Geschäfts oder ein IT-Beratungsunternehmen für die verschiedenen Teilleistungen eines Mandates wie Softwareentwicklung, Datenauswertungen etc.). Er gewährleistet dabei gegenüber seinem Auftraggeber die Einhaltung der Pflichten durch die Unterauftragnehmer. Eine Pflicht zur vorgängigen Einholung der Einwilligung durch den Verantwortlichen ist praxisfern und nicht notwendig.

Der Auslandtransfer ist nicht unnötig zu verzögern und zu erschweren (Art. 5-6 VE-DSG):

Die zahlreichen Melde- und Genehmigungspflichten für die Bekanntgabe ins Ausland sind unverhältnismässig und fördern den Datenschutz nicht. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) würde zahlreiche für ihn kaum relevante Meldungen erhalten. Solche Mitteilungen bewirken für die betroffenen Personen keinen stärkeren Schutz. Die verpflichteten Verantwortlichen und Auftragsbearbeiter müssten in ihren Meldungen an den EDÖB unnötigerweise Geschäftsgeheimnisse offenbaren (z.B. betreffend hängiger ausländischer Verfahren). Für die Verpflichteten bestehen dabei unverhältnismässige Risiken, da die übermittelten Informationen dem Öffentlichkeitsgesetz unterliegen können. Ein Auftragsbearbeiter wird zudem nur auf Auftrag und Instruktion des Verantwortlichen tätig. Es ist der Verantwortliche, welcher die beauftragten Bearbeitungen als Teil seiner Geschäftsaktivität plant und über die erforderlichen Informationen verfügt. Es macht für eine zeitnahe Benachrichtigung und Aktivierung des EDÖB keinen Sinn den Auftragsbearbeiter für Praktiken in die Pflicht zu nehmen, die der Verantwortliche alleine bestimmt. Für einen Schweizer Kommunikations- oder Werbe-Dienstleister, Web-Designer oder Cloud-Anbieter, der von seiner Kundin ausserhalb Europas Daten erhält und speichert bzw. bearbeitet, ist unter der vorgeschlagenen Regelung zudem nicht klar, ob er für den Re-Export der Daten in das Land der Kundin eine neue vertragliche Grundlage (im Sinne von Abs. 3) benötigt. Die Bussendrohung stellt für den Auftragsbearbeiter eine unzumutbare Unsicherheit dar. Die strafrechtlich sanktionierten Melde- und Genehmigungspflichten sind insbesondere für Auftragsbearbeiter zu löschen.

Die vorgesehene Frist von sechs Monaten (anstelle der bis anhin 30 Tage) zur Prüfung von standardisierten Garantien und unternehmensinternen verbindlichen Vorschriften ist kontraproduktiv. Viele Anbieter können nicht so lange auf einen Bescheid warten und werden sich auf eine andere Basis für den Auslandtransfer stützen oder die geplante Aktivität aufgeben. Diese Frist ist für den EDÖB nicht einmal verbindlich, was zu einer unzumutbaren Rechtsunsicherheit und einem Nachteil für Schweizer Anbieter führt. Es ist zudem nicht einzusehen, warum bei spezifischen Garantien der EDÖB nur informiert werden muss, bei standardisierten Garantien aber eine langwierige Vorprüfung vorgeschrieben ist. Gerade standardisierte Garantien sowie unternehmensinterne verbindliche Vorschriften haben das Potential zur Entwicklung von wichtigen Best

Practices. Davon profitieren wiederum die betroffenen Personen. Vorbildliche Anbieter, die für ihre Branche solche Standards durch regen Gebrauch etablieren möchten, sollen nicht durch unverhältnismässig lange Prüffristen des EDÖB blockiert werden.

Das DSG soll die Datenbekanntgabe auch im Zusammenhang mit einem Vertrag im Interesse der betroffenen Person erlauben. Die Bekanntgabe ins Ausland ist ausnahmsweise erlaubt, wenn die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten des Vertragspartners handelt. Unter der DSGVO ist die Bekanntgabe auch für den Abschluss oder die Erfüllung eines bloss im Interesse der betroffenen Person geschlossenen Vertrages möglich (Art. 49 Abs. 1 Bst. c DSGVO). Die Schweiz soll diese erweiterte Ausnahme den eigenen Anbietern nicht vorenthalten.

Missbrauchspotential beim Auskunftsanspruch ist zu vermeiden (Art. 20 VE-DSG):

Der Auskunftsanspruch ist auf ein verhältnismässiges Mass an Daten zu beschränken. Die vorgesehene Auskunftspflicht umfasst alle Angaben zur Aufbewahrungsdauer, die Identität und Kontaktdaten aller Auftragsbearbeiter, das Ergebnis, Zustandekommen und die Auswirkungen von Entscheidungen, die auf irgendeiner Art von Datenbearbeitung beruhen. Dieser sehr weit gefasste Anspruch eröffnet Missbrauchspotential: Querulatorische Gesuche oder Anfragen zu datenschutzfremden Zwecken werden zunehmen. Das vorgeschlagene Auskunftsrecht geht weit über das verhältnismässige Mass und die Regelung der DSGVO hinaus. Die DSGVO beschränkt z.B. den zusätzlichen Anspruch auf Auskunft bei automatisierten Einzelfallentscheiden auf Fälle, in denen besonders schützenswerte Personendaten bearbeitet werden oder der Entscheid eine rechtliche Wirkung oder andere erhebliche Beeinträchtigung für die betroffene Person hat. Der ufer- und voraussetzungslose Auskunftsanspruch im VE-DSG steht in einem Missverhältnis zur Belastung der Auskunftspflichtigen. Aufgrund der vorgesehenen Bussendrohung, können Bearbeiter auch missbräuchliche Anfragen faktisch nicht mehr zurückweisen.

Für Auskunftsansprüche ist ein Kostenersatz vorzusehen. Ohne den Ausschluss des DSG in hängigen Zivilprozessen und laufenden Strafverfahren (Art. 2 Abs. 2 VE-DSG) eröffnet der Vorentwurf weiteres Missbrauchspotential: Mittels Auskunftsbegehren kann eine Verfahrenspartei kostenlos umfangreiches Beweismaterial für datenschutzfremde Zwecke beschaffen. Damit lassen sich z.B. die im Zivilprozess bestehenden Anforderungen für Editionsbegehren umgehen. Querulatorische oder wiederholte Anfragen können grosse Ressourcen binden. Ohne Kostenersatz geht das Risiko einseitig zu Lasten der Auskunftspflichtigen. Staatliche Behörden können bei einer Auskunft nach dem Öffentlichkeitsgesetz einen Kostenbeitrag verlangen. Selbst die DSGVO sieht zumindest bei wiederholten Anfragen den Kostenersatz vor (Art. 15 Abs. 3 DSGVO).

Auf unverhältnismässige Anforderungen an das Profiling ist zu verzichten (Art. 3 Bst. F und Art. 23 Abs. 2 Bst. d VE-DSG):

Informations- und Anhörungspflichten sollen auf automatisierte Entscheide mit erheblichen Auswirkungen beschränkt werden. In einem ersten Schritt ist der Begriff des Profiling einzuschränken auf die automatisierte Auswertung von personenbezogenen Daten, deren Ergebnis wiederum Personendaten sind. Dies sieht auch die DSGVO vor (Art. 4 Abs. 4 DSGVO). Profiling an sich hat für die betroffene Person kaum direkte Auswirkungen. Rechtliche Anforderungen sollen daher, wenn überhaupt, nur an die Verwendung der Ergebnisse anknüpfen, z.B. für automatisierte Entscheide. Erfasst wären aber potentiell sehr viele Routineverfahren, die im Rahmen der fortschreitenden Digitalisierung aus Effizienzgründen automatisiert werden, z.B. Prozesse zur Vertragsabwicklung. Die zusätzlichen administrativen Hürden für die Verpflichteten

sollen in einem angemessenen Verhältnis zum Schutzbedürfnis der betroffenen Personen stehen. Die Pflichten bei automatisierten Einzelfallentscheiden sind daher in einem zweiten Schritt auf Entscheide zu beschränken, welche unmittelbare und erhebliche Auswirkungen auf die Persönlichkeitsrechte der betroffenen Person haben. Das DSG soll zudem weitere Ausnahmen von den Pflichten bei automatisierten Einzelfallentscheiden aufnehmen, wie dies auch die EU vorsieht (Art. 22 DSGVO). Darunter fallen z.B. Entscheidungen, die für den Abschluss oder die Erfüllung von Verträgen mit der betroffenen Person erforderlich sind.

Der Geheimnisschutz ist auf Berufe mit spezialgesetzlicher Schweigepflicht und eine berechtigte Geheimniserwartung einzuschränken (Art. 52 VE-DSG):

Eine Geheimhaltungspflicht soll nur greifen bei beruflichen Schweigepflichten, die unabhängig von Art. 52 VE-DSG bestehen. In den spezialgesetzlich erfassten Berufszweigen (z.B. Arzt, Anwalt) ist für alle Beteiligten klar, dass eine besondere Vertraulichkeit notwendig ist, z.B. für Patientendaten. Für viele andere Geschäftsfelder, die standardmässig Personendaten erfassen und bearbeiten (z.B. Online-Händler, Werbe-Dienstleister etc.), ist dies nicht der Fall. Früher oder später können praktisch alle Berufszweige mit geheimen Personendaten in Berührung kommen. Die vorgeschlagene Regel schliesst Anbieter damit weitgehend von jeglicher Nutzung der beschafften Daten aus. Die Bussendrohung für derart weit gefasste Pflichten ist unverhältnismässig. Sie ist zu beschränken auf berufliche Schweigepflichten, die ein anderes Gesetz vorschreibt. Wie bei anderen beruflichen Geheimnispflichten, muss eine Befreiung durch die Aufsichtsbehörde möglich sein.

Die Ausweitung des Geheimnisschutzes auf alle Personen, welche geheime Daten kommerziell bearbeiten ist überschiessend. Nicht einmal die EU sieht eine derart strenge Regelung vor. Dienstleister in den Bereichen der datengestützten Beratung und der personalisierten Online-Werbung (z.B. Betreiber von Werbenetzwerken, Dienstleister im Bereich digitales Marketing), aber auch Hosting- und Cloud-Anbieter könnten solche Dienstleistungen kaum mehr in der Schweiz anbieten. Die Sanktionsdrohung wäre ein weiterer massiver Standortnachteil für die Schweiz.

Nur diejenigen geheimen Daten sind zu schützen, für die der Geheimnisherr auch eine berechtigte Erwartung an die Geheimhaltung hat. Sofern zwischen dem Geheimnisherrn (d.h. der betroffenen Person) und dem Bearbeiter als Geheimnisträger z.B. eine vertragliche Grundlage für die Bearbeitung besteht, soll auch die Bearbeitung und entsprechende Offenlegung möglich sein.

Selbstregulierung ist zu fördern und nicht zu verordnen (Art. 8-9 VE-DSG):

Nur Empfehlungen der guten Praxis aus der jeweiligen Branche selbst sind zielführend. Das DSG soll die Selbstregulierung in Eigeninitiative der jeweiligen Branchen fördern. Die Kompetenz dazu muss bei den interessierten Kreisen liegen, nicht beim EDÖB. Die Befugnisse des EDÖB zur Ausarbeitung und Genehmigung von Empfehlungen sind zu weitgehend und können zu praxisfernen Alleingängen führen. Nicht praktikable Empfehlungen schwächen den Datenschutz eher, als dass sie die Persönlichkeitsrechte der betroffenen Personen wirksam schützen. Erfahrungen mit Schweizer Selbstregulierungen haben gezeigt, dass echte Brancheninitiativen am wirksamsten sind. Auch der erläuternde Bericht nennte als Erfolgsbeispiele (S. 53) die Verhaltenskodizes der Brancheninitiative des Schweizerischen Verbandes der Telekommunikation für verbesserten Jugendmedienschutz in den neuen Medien und zur Förderung der Medienkompetenz in der Gesellschaft sowie den Code of Conduct Hosting unserer Organisation.

Die freiwillige Benennung eines betrieblichen Datenschutzbeauftragten zeigt die Erfüllung der Sorgfaltspflichten des Unternehmens. Es ist richtig, dass die Schweiz auf die zwingende Benennung eines

betrieblichen Datenschutzbeauftragten verzichtet. Das DSG soll aber Unternehmen, die freiwillig eine solche Sorgfaltsmassnahme ergreifen, von gewissen Pflichten entbinden. Die mit der Einsetzung eines betrieblichen Datenschutzbeauftragten gezeigte Sorgfalt ist zudem bei allfälligen Sanktionsbemessungen zu berücksichtigen.

Meldepflicht bei Datenschutzverletzungen muss verhältnismässig sein (Art. 17 VE-DSG):

Die Meldepflicht ist auf Datenschutzverletzungen mit erhöhtem Risiko für eine Vielzahl von Personen zu beschränken. Anders als in der EU, stellt der Wortlaut des Schweizer Vorentwurfs alle unbefugten Datenschutzbearbeitungen unter die Meldepflicht. Aus Gründen der Verhältnismässigkeit soll die Meldepflicht nur in Fällen eines Datenverlusts, einer unbefugten Offenlegung oder eines unbefugten Datenzugangs mit erhöhtem Risiko für die Persönlichkeitsrechte einer grösseren Zahl von betroffenen Personen greifen. Andernfalls rechtfertigen sich das Einschalten und Aktivwerden des EDÖB nicht. Die Verpflichteten sollen die dazu nötige Einschätzung der Risiken und Anzahl Betroffener nach sorgfältigen Massstäben aber in eigenem Ermessen durchführen können. Eine Meldung soll ohne unnötige Verzögerung erfolgen, wobei sachliche Gründe (z.B. Massnahmen zur Schliessung des Lecks, zur technischen Untersuchung etc.) eine Verzögerung rechtfertigen können.

Zu weitgehend ist auch die Meldepflicht an Dritte. Der Vorentwurf enthält die Schweizer Besonderheit, wonach jeder Verantwortliche und Auftragsbearbeiter allfällige Drittempfänger der Daten über Verletzungen des Datenschutzes informieren muss. Diese Mitteilung hat unabhängig davon zu erfolgen, ob eine Meldung an den EDÖB oder an die betroffene Person notwendig ist. Die EU sieht keine solche Pflicht vor (Art. 19 DSGVO). Diese Mitteilung beinhaltet ein enormes Potential zur Rufschädigung. Es ist nicht einzusehen, weshalb die Schweiz derartige Verschärfungen einführen soll, die keine Erhöhung des Datenschutzes aber massive administrative Aufwendungen für Verantwortliche und Auftragsbearbeiter bewirken.

Auf unverhältnismässige Sanktionen einseitig zulasten der Schweizer Anbieter ist zu verzichten (Art. 50-53 VE-DSG):

Der Verzicht auf hohe Bussen führt nicht zum Verlust des Angemessenheitsbeschlusses der EU. Das SEV 108 verlangt lediglich die "wirksame" Umsetzung (Art. 4 Abs. 1 und 3 Bst. a SEV 108) und "geeignete" Sanktionen (Art. 10 SEV 108). Das DSG muss keine hohen Bussen für Administrativpflichten vorsehen, um diesen Anforderungen gerecht zu werden. Die Verfügungskompetenz des EDÖB und die Sanktion bei Widerhandlungen gegen rechtskräftige Verfügungen (Art. 292 StGB) reichen als wirksame Durchsetzungsmassnahmen aus.

Die selbständige Sanktionierung von Administrativpflichten stärkt den Datenschutz nicht und ist unverhältnismässig. Die zahlreichen selbständig sanktionierten, administrativen Pflichten (Art. 50 und 51 VE-DSG) erhöhen den administrativen Aufwand und das finanzielle Risiko für Schweizer Anbieter. Diese Pflichten bleiben aber weitgehend ohne direkte Wirkung für den Schutz der Persönlichkeitsrechte der betroffenen Personen.

Hohe Schweizer Bussen bedrohen einseitig Schweizer Anbieter. Die vorgeschlagene Sanktionsregelung bedeutet für in der Schweiz ansässige KMU eine stärkere finanzielle Belastung, als für grosse, internationale Konzerne: Für internationale Anbieter ohne Schweizer Niederlassung ist der Anreiz grösser, die natürliche Person nicht identifizierbar zu halten. Für Schweizer Anbieter liesse sich demgegenüber regelmässig leichter feststellen, wer als natürliche Person zur Verantwortung gezogen werden kann. Damit sind die Risiken gerade für Geschäftsführer und leitende Angestellte von Schweizer Unternehmen grösser als für

internationale Konkurrenten. Eine grosse Rechtsunsicherheit für die verpflichteten Unternehmen besteht zudem aufgrund fehlender Harmonisierung und sehr unterschiedlicher datenschutzrechtlicher Erfahrung der zuständigen kantonalen Strafbehörden.

Die Ausweitung des Strafkatalogs widerspricht der Schweizer Rechtstradition. Unter dem geltenden DSG sollen Datenschutzverstösse nur ausnahmsweise mit strafrechtlichen Sanktionen geahndet werden (Botschaft des Bundesrates vom 23. März 1988 zum DSG, BBl 1988 II 413, 484). In der Schweizer Rechtstradition ist nicht zwingend eine Androhung von Strafen notwendig, damit gesetzliche Verpflichtungen als verbindlich aufgefasst werden. Den Verpflichteten drohen bei Nichtbefolgen der Administrativpflichten an sich bereits regelmässig Rechtsnachteile, z.B. wegen fehlender Nachweise in einem Verfahren. Zudem sind die administrativen Pflichten im Vorentwurf sehr unbestimmt (z.B. die Dokumentationspflicht), was eine Bestrafung rechtsstaatlich problematisch macht. Die Ausweitung des Sanktionskatalogs für Administrativpflichten schadet auch dem offenen und zielgerichteten Dialog zwischen Datenbearbeitern und dem EDÖB.

Für die Berücksichtigung der Anliegen der Internetindustrie zur Schaffung einer verhältnismässigen und praxistauglichen Datenschutzregulierung danken wir Ihnen im Voraus und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

simsa – Swiss Internet Industry Association

Andrej Vckovski — Präsident

Rolf Auf der Maur — Vizepräsident

Amstutz Jonas BJ

Von: Thomi Cécile <c.thomi@konsumentenschutz.ch>
Gesendet: Mittwoch, 22. März 2017 15:19
An: Amstutz Jonas BJ
Betreff: Revision DSG: Stellungnahme SKS
Anlagen: 17_03_Revision_DSG_Stellungnahme_SKS.docx

Sehr geehrter Herr Amstutz

In der Beilage lasse ich Ihnen die Stellungnahme der Stiftung für Konsumentenschutz in Sachen Revision DSG zukommen.

Bei Fragen oder Unklarheiten stehe ich Ihnen gerne zur Verfügung.

Freundliche Grüsse

Cécile Thomi
Leiterin Recht

Stiftung für Konsumentenschutz SKS
Monbijoustrasse 61, Postfach
3001 Bern
Geschäftsstelle +41 31 370 24 24
Direkt +41 31 370 24 29
c.thomi@konsumentenschutz.ch
www.konsumentenschutz.ch

Stopp Hochpreisinsel – unterschreiben Sie jetzt die Fair-Preis-Initiative:
https://wecollect.ch/de/campaign/fairpreisinitiative/

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Stiftung für Konsumentenschutz

Abkürzung der Firma / Organisation : SKS

Adresse : Monbijoustrasse 61, Postfach, 3000 Bern 23

Kontaktperson : Cécile Thomi

Telefon : 031 370 24 29

E-Mail : c.thomi@konsumentenschutz.ch

Datum : 22. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SKS	Die Stiftung für Konsumentenschutz SKS unterstützt die Stossrichtung des Revisionsentwurfs. Es ist die dringende Aufgabe des Gesetzgebers sicherzustellen, dass der Einzelne auch in einem digitalen Umfeld die Hoheit über seine Daten grundsätzlich in den eigenen Händen behält und dass die Datenbearbeiter zu Transparenz und Verhältnismässigkeit verpflichtet werden. Der beste Beweis, dass Handlungsbedarf besteht, lieferte im Februar 2017 die Swisscom AG: in einem Informationsschreiben kündigte sie an, Kundendaten an Dritte weiterzuleiten. Kunden, die damit nicht einverstanden waren, mussten aktiv werden und der Datenbearbeitung widersprechen. Dabei reichte jedoch ein einfacher Widerspruch nicht aus. Vielmehr musste über den Kunden-Account in einem komplizierten Opt out-Verfahren in einer verschachtelten und unübersichtlichen Konstruktion an zahllosen Stellen die Datenbearbeitung untersagt werden. Personen mit einer gewissen Vorkenntnis, die sich zudem auch auf englischsprachigen Internetseiten gut zurechtfinden, benötigten dazu im Minimum eine halbe Stunde – Personen, die mit derartigen Fragen weniger vertraut sind, schafften es nicht unter zwei Stunden (und waren dazu keineswegs sicher, alles verstanden zu haben). Für Kunden, die dazu nicht in der Lage waren, bedeutete dies, dass ihre Daten ungehindert an Drittunternehmen – zahlreiche davon im Ausland angesiedelt – weitergeleitet wurden. Ein derartiger Umgang mit Kundendaten darf nicht zulässig sein! Datenbearbeitung hat zwingend den Regeln eines Opt in-Verfahrens zu folgen. Die Person, deren Daten bearbeitet werden sollen, muss ihr Einverständnis dazu geben. Wichtig dabei ist, dass es mit der Erteilung einer Blankovollmacht nicht getan ist. Vielmehr muss sich die Person der Datenbearbeitung zeitlich und inhaltlich bewusst sein.
SKS	Zum Aufbau der Datenschutzgesetzgebung in der Schweiz ist folgendes zu sagen: das Konstrukt ist grundsätzlich falsch. Für die Umsetzung eines modernen Datenschutzgesetzes wäre es notwendig, dass die kantonalen Datenschützer auf kantonaler Ebene für dieselbe Materie zuständig sind wie der Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB auf Bundesebene. Sämtliche kantonalen Datenschützer müssen die Kompetenz haben, das materielle Recht, welches aus dem zu revidierenden DSG fliesst, auf kantonaler Ebene anwenden und durchsetzen zu können- und zwar im Verhältnis kantonale Behörde – Privatperson sowie im Verhältnis unter Privaten (natürliche und juristische Personen). Dies wäre nicht bloss eine Kompetenzerweiterung der kantonalen Datenschützer, sondern wäre in erster Linie als Entlastungsmassnahme für den EDÖB zu betrachten: einerseits, weil konkrete Streitfälle bereits auf kantonaler Ebene erledigt werden könnten, andererseits, weil die vermehrte Rechtsanwendung zu Rechtssicherheit beitragen würde.
SKS	Wichtig ist, dass das DSG keinen zu hohen Detaillierungsgrad aufweist. Die in einem digitalen Umfeld notwendigen Grundsätze zur vollständigen Bewahrung der Hoheit über die eigenen Daten und zum Schutz der Privatsphäre sind klar im Gesetz festzuhalten. Ansonsten ist im Gesetz jedoch ein grosser Auslegungsspielraum für den EDÖB vorzusehen. Hingegen sollten in der Botschaft sowie im Erläuternden Bericht zwecks Verdeutlichung der materiellrechtlichen Bestimmungen jeweils zahlreiche Beispiele enthalten sein.

SKS	Es wird begrüsst, dass der Revisionsentwurf eine Ausdehnung der Kompetenzen des EDÖB vorsieht. Die geplanten neuen Handlungsmöglichkeiten und Aufgaben sind durchaus geeignet, die aus dem Gesetz fliessenden Rechte und Pflichten umzusetzen. Um den neuen Anforderungen gerecht werden zu können, müssen dem EDÖB jedoch auch adäquate Ressourcen zur Verfügung stehen. Notwendig sind dazu in erster Linie ausreichendes Personal sowie ein angepasstes Budget. Ein effizientes Instrument, mit welchem der EDÖB dem materiellrechtlichen Gesetzesinhalt zum Durchbruch verhelfen kann, fehlt jedoch: Er muss die Möglichkeit haben, Stichproben durchzuführen. Ohne Preisgabe seiner Identität muss er beispielsweise den Ablauf der Datenbearbeitung und die Einhaltung der datenschutzrechtlichen Vorgaben in einem Unternehmen überprüfen können. Dazu braucht es jedoch eine ausreichende gesetzliche Grundlage im DSG.
SKS	Zwei der materiellrechtlichen Highlights der EU-Datenschutzgrundverordnung, nämlich das Recht auf Datenportabilität sowie das Recht auf Vergessen werden im vorliegenden Revisionsentwurf vollständig ausgeblendet. Diese beiden Aspekte bilden jedoch einen wichtigen Bestandteil des Anspruchs, die Hoheit über die eigenen Daten zu behalten bzw. wieder zu erlangen. Das Recht auf Datenportabilität ist gleichzeitig ein Recht auf Kopie (der bei einem Anbieter gespeicherten eigenen Daten) und stellt eine moderne Form des Einsichtsrechts dar. Die den Kunden betreffenden Daten können neu von Firma A zur konkurrierenden Firma B übertragen werden. Die Anbieter sind verpflichtet, die Daten in maschinenlesbarer Form in einem einheitlichen Datenformat in einem einfachen und unkomplizierten Verfahren zur Verfügung zu stellen. Mit der Datenportabilität wird zum einen die Stellung des Betroffenen gestärkt – er wird vom Datenobjekt zum Datensubjekt, in dem er die Verfügungsgewalt über seine eigenen Daten inne hat. Zum andere wird der Wettbewerb angeregt, da ein Anbieterwechsel einfacher von Statten geht. Seit dem EuGH-Urteil Gonzales aus dem Jahre 2014 ist das Recht auf Vergessen höchstrichterlich verankert. Es darf nicht sein, dass die Öffentlichkeit Kenntnis erhält von Ereignissen, die unter Umständen weit zurückliegen und sich belastend auf das private oder berufliche Leben des Betroffenen auswirken. Die Privatsphäre muss auch im Internet geschützt werden. Die Suchmachschinenbetreiber Google&Co. sind somit auch in der Schweiz zu verpflichten, unter bestimmten Voraussetzungen Links auf Seiten, die nach bestimmten Suchanfragen erscheinen, zu löschen. Diese beiden Rechte sind an geeigneter Stelle im Revisionsentwurf einzufügen.
SKS	Die Wirksamkeit des materiellrechtlichen Inhalts von Normen hängt im Wesentlichen davon ab, wie leicht deren Einhaltung auf dem Klageweg eingefordert werden kann. Auf Grund der Komplexität und auch Undurchsichtigkeit der modernen Datenbearbeitung (vor allem auch im Internet) ist es den Betroffenen jedoch oftmals gar nicht möglich, nachzuweisen, dass eine widerrechtliche Datenbearbeitung stattgefunden hat. Eine einfache und effiziente Lösung, wie dem Recht trotzdem zum Durchbruch verholfen werden kann, ist die Umkehr der Beweislast. Der Datenbearbeiter hat die Konformität seiner Datenbearbeitung nachzuweisen. Da dem Datenbearbeiter gestützt auf Art. 19 des Entwurfs ohnehin eine Dokumentationspflicht zukommt, entsteht ihm durch dieses prozessuale Instrument auch keine Mehrbelastung.

	Eine passende Bestimmung ist entweder in den vorliegenden Revisionsentwurf oder in die zu revidierende ZPO aufzunehmen.
SKS	Entscheidend ist, dass auch im grenzüberschreitenden Datenverkehr ein ausreichender Rechtsschutz gewährt bleibt. Insbesondere ist sicherzustellen, dass Anbieter aus der EU, für welche bei ihren Tätigkeiten in der Schweiz die EU-Datenschutzgesetzgebung nicht gilt, von den Rechten und Pflichten des DSG erfasst werden. Es darf nicht sein, dass die Schweiz für ausländische Anbieter ein datenschutz-freies Eldorado wird.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SKS	DSG	4	2		Die Forderung nach einer verhältnismässigen Datenbearbeitung ist zentral und wird unterstützt. Das Prinzip der Datensparsamkeit lässt nur eine Bearbeitung von so vielen und derjenigen Daten zu, wie dies für den beabsichtigten Zweck notwendig ist.
SKS	DSG	4	3		Die Formulierung von Abs. 3 gewährt keinen ausreichenden Schutz. Es reicht nicht, wenn der Zweck der Datenbeschaffung *klar erkennbar* ist. Entscheidend ist, dass der Betroffene zum Zeitpunkt der Datenbeschaffung explizit informiert wird. Gemäss dem Erfordernis der Transparenz muss zum einen mitgeteilt werden, *dass* eine Datenbeschaffung stattfindet. Zum anderen muss der Betroffene sich darüber im Klaren sein, *zu welchem Zweck* die Datenbeschaffung geschieht. Vorschlag: *Personendaten dürfen nur zu einem bestimmten und der Person mitgeteilten Zweck beschafft werden; […].* Die Formulierung, wonach die Daten nur so weit bearbeitet werden dürfen, *dass dies mit dem Zweck zu vereinbaren ist*, ist abzulehnen. Diese zu offene Formulierung macht die Zweckbindung auslegungsfähig und interpretierbar. Vorschlag: *sie dürfen nur so bearbeitet werden, soweit die dem Zweck entspricht.*
SKS	DSG	4	6		Zum Inhalt von Abs. 6 ist zu bemerken, dass grundsätzlich für jede Datenbearbeitung, die in den Anwendungsbereich des DSG fällt, eine Einwilligung erforderlich ist. Dies sieht auch der im Erläuternden Bericht vom 21. Dezember 2016 (EB) erwähnte Art. 5 Abs. 2 E-SEV 108 so vor. Die Formulierung *Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, […].* ist daher irreführend. Der Begriff der *angemessenen* Information genügt den Anforderungen grundsätzlich nicht, da er einen zu grossen Interpretationsspielraum offen lässt. Jedoch lässt sich dieses Manko beheben, indem auf die Unterscheidung zwischen *eindeutiger* und *ausdrücklicher* Einwilligung verzichtet wird. Die im Gesetzesentwurf vorgenommene Unterscheidung zwischen eindeutig und ausdrücklich

					wiederspiegelt eine der Kernforderungen einer modernen Datenschutzgesetzgebung: die Digitalisierung unseres Alltags führt dazu, dass eine ständige Datenbearbeitung (sammeln, analysieren, auswerten weitergeben etc.) stattfindet. Mehrheitlich ist sich der Einzelne dieser Datenbearbeitung gar nicht bewusst. Um sicherzustellen, dass das Bewusstsein und die Zustimmung zur Datenbearbeitung gegeben sind, braucht es daher zwingend eine *ausdrückliche* Zustimmung – das Prinzip des sogenannten *Opt in.* Eine *eindeutige* Einwilligung, so wie sie im Gesetz vorgesehen ist, stellt nicht sicher, dass das Bewusstsein für die Datenbearbeitung tatsächlich vorhanden ist. Eine eindeutige Einwilligung soll gemäss EB, S. 47, wie bereits bis anhin, auch durch blosses konkludentes Handeln und ohne Formvorschriften angenommen werden. Genau hier liegt jedoch eines der Hauptprobleme: konkludentes Handeln kann unter diesen Vorzeichen z.B. angenommen werden, wenn ein Nutzer eine Dienstleistung weiter nutzt, ohne dass er aber von den Änderungen in den Datenschutzbestimmungen, die ihm beispielsweise per Email mitgeteilt worden sind, effektiv zur Kenntnis genommen hat. Daher ist es notwendig, dass der Betroffene sich ausdrücklich zur Datenbearbeitung äussern und sich damit einverstanden erklären muss. Beispielsweise, in dem er eine ausdrückliche Annahmeerklärung abgeben muss, wenn ein Teil der Nutzungsbedingungen geändert worden ist. Die Dienstleistung sollte nicht weiter nutzbar sein, solange diese ausdrückliche Einwilligung nicht stattgefunden hat. Auf diese Weise ist gleichzeitig sichergestellt, dass keine Blankovollmachten erteilt werden, in dem Sinne, dass gestützt auf eine einmalige Einwilligung zur Datenbearbeitung alle nachfolgenden Neuerungen, Änderungen etc. legitimiert sind. Wichtig ist dabei, dass dem Nutzer Änderungen dergestalt mitgeteilt werden, dass er diese auch tatsächlich zur Kenntnis nimmt. Sicherlich nicht zielführend ist es, dem Nutzer vorgängig zu einer konkreten Nutzung (z.B. Anfrage bei einer Suchmaschine) eine mehrseitige Erklärung zukommen zu lassen, mit der Absicht, dass ihn diese Informationsflut abschreckt, er sie nicht durchliest und die Änderung unbesehen akzeptiert. Dadurch erledigt sich die Frage, was eine angemessene Information darstellt, von selbst, da eine Datenbearbeitung ohnehin nur erfolgen darf, wenn eine ausdrückliche Einwilligung dazu vorliegt. Die Voraussetzung der Freiwilligkeit wird unterstützt. Dazu ist auszuführen, dass der Begriff der Freiwilligkeit so zu verstehen ist, dass damit auch ein Koppelungsverbot verbunden sein muss. Der Nutzer darf nicht gezwungen sein, einer Datenbearbeitung zuzustimmen, wenn er beispielsweise eine Dienstleistung in Anspruch nehmen will. Oder umgekehrt: Ein Vertragsabschluss muss möglich sein, auch wenn einer Datenbearbeitung nicht zugestimmt wird. Allenfalls wäre denkbar, dass bei einer nur beschränkten

					Datenbearbeitungseinwilligung ein bestimmtes Angebot auch nur in einem beschränkten Umfang genutzt werden kann.
SKS	DSG	5	1		Gemäss Abs. 1 dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen *schwerwiegend* gefährdet würde. Diese Einschränkung, wonach eine Datenweitergabe nur bei Gefahr von schwerwiegenden Persönlichkeitsverletzungen unzulässig ist, wird vehement abgelehnt. Die Einschränkung widerspricht zudem der weiteren Regelung von Art. 5. Dieser versucht, ein Regime auf die Beine zu stellen, mit welchem der Schutz der Daten auch bei Bekanntgabe ins Ausland sichergestellt ist. Es ist z.B. kaum davon auszugehen, dass der Bundesrat gemäss Abs. 2 das Vorliegen eines *angemessen* Schutzes im ausländischen Staat annimmt oder der in Abs. 3 lit. a. erwähnte völkerrechtliche Vertrag, bei dessen Vorliegen ein *geeigneter* Schutz angenommen wird, als geeignet erachtet wird, wenn damit bloss *schwerwiegende* Persönlichkeitsverletzungen ausgeschlossen werden.
SKS	DSG	5	2		Entscheidend wird sein, welche Kriterien zum Einsatz kommen werden, gemäss welchen der Bundesrat einen Staat auf die Liste derjenigen Länder setzt, die einen angemessenen Datenschutz garantieren. Grundsätzlich wird hier das in Schweiz geltende Datenschutzniveau zur Anwendung kommen müssen. Es gibt keine Gründe für die Anwendung von lockereren Vorschriften als bei einer Datenbearbeitung in der Schweiz; im Gegenteil: geht die Datenhoheit durch die Weitergabe der Daten ins Ausland verloren, so sind umso strengere Voraussetzungen zu erfüllen, um den notwendigen Schutz weiterhin zu garantieren.
SKS	DSG	6	1	e	Gemäss lit. e. soll eine Datenbekanntgabe ins Ausland zulässig sein, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Das digitalisierte Umfeld stellt höhere Anforderungen an diesen Legitimationsgrund. Daten werden heutzutage in mannigfacher Hinsicht zugänglich gemacht, beispielsweise über soziale Netzwerke. Hier ist es schwierig zu bestimmen, ob bzw. ab welchem Zeitpunkt Daten *allgemein zugänglich* gemacht werden. Welche Datenschutzeinstellungen, die ein soziales Netzwerk bietet, führen zur Annahme, dass die betroffene Person die Daten *allgemein* zugänglich gemacht hat oder eben nicht? Ein einfacher Weg, um hier mehr Klarheit zu schaffen, wäre die Ersetzung des Begriffs *allgemein* mit dem Begriff *öffentlich*. Mit diesem Begriff wird sichergestellt, dass es der Wille der betroffenen Person war, dass die betroffenen Daten für jedermann – also für die Öffentlichkeit – frei zugänglich sind.

					Als kumulatives Element ist erforderlich, dass die betroffene Person die Bearbeitung der zugänglich gemachten Daten nicht ausdrücklich untersagt hat. Dieses Element widerspricht einem fundamentalen Erfordernis, dem eine moderner Datenschutzgesetzgebung zu genügen hat – dem Prinzip Opt in: die betroffene Person muss aktiv zustimmen, wenn sie eine bestimmte Datenbearbeitung zulassen will. Dies gilt umso mehr, wenn es um die heikle Frage der Bekanntgabe von Daten ins Ausland geht. Die vorgesehene Regelung sieht jedoch ein sogenanntes Opt out vor. Die betroffene Person soll aktiv widersprechen müssen, wenn sie mit einer Datenbearbeitung nicht einverstanden ist. Eine derartige Regelung lehnen wir ausdrücklich ab. Zudem muss ausdrücklich von *Bekanntgabe ins Ausland* die Rede sein, nicht lediglich von *Bearbeitung*. Vorschlag: *die betroffene Person die Daten öffentlich zugänglich gemacht und einer Bekanntgabe ins Ausland ausdrücklich zugestimmt hat*.
SKS	13	1 – 5			Artikel 13 sieht eine grundlegende Informationspflicht bei der Beschaffung von Personendaten gegenüber der betroffenen Person vor. Auch das Beschaffen von Daten stellt bereits eine Datenbearbeitung dar. Wie dargelegt, fordert die SKS eine Beachtung des *Opt in*-Prinzips: Datenbearbeitung darf nur bei Vorliegen einer ausdrücklichen Zustimmung zur Datenbearbeitung erfolgen. Dieses Prinzip ist somit auch bei der in Art. 13 geregelten Datenbeschaffung zu verfolgen und ist in geeigneter Weise in den Artikel einzufügen. Dies gilt umso mehr bei der in Abs. 3 vorgesehenen Weitergabe von Personendaten an Dritte. Abs. 3 spricht zudem von *Empfängerkategorien*. Gemäss der Bestimmung soll es demnach ausreichend sein, wenn die betroffene Person über die Bekanntgabe ihrer Personendaten an eine bestimmte Empfängerkategorie informiert wird. Dies entspricht in keiner Art und Weise dem Schutz von Personendaten, den das revidierte DSG anstreben sollte. Gerade bei der Weitergabe von Personendaten an Dritte muss zwingend eine ausdrückliche Einwilligung der betroffenen Person vorhanden sein. Es reicht nicht, dass die betroffene Person lediglich informiert ist. Zudem muss bekannt sein, an wen genau die Daten geliefert werden.
SKS	14	1			Gemäss dieser Bestimmung soll die Informationspflicht gemäss Art. 13 entfallen, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt. Diese Regelung wird dezidiert abgelehnt. Auf die dahinter stehende grundsätzliche Problematik des Bewusstseins für die Datenbearbeitung wurde bereits mit den Bemerkungen zu Art. 4 Abs. 6 hingewiesen. Dort geht es um eine einmal, zu einem bestimmten

					Zeitpunkt erteilte Einwilligung. Unter Umständen erfolgte die einmalige Information bereits vor langer Zeit. Eine einmal erteilte Information wird auf diese Weise zu einer Blankovollmacht. Bereits nach wenigen Monaten erinnert sich die betroffene Person mit grosser Wahrscheinlichkeit nicht mehr an die erhaltenen Informationen, welche Daten bearbeitet werden, zu welchem Zweck und in welchem Umfang. Zum heutigen Zeitpunkt ist die betroffene Person unter Umständen mit der Datenbearbeitung nicht mehr einverstanden. Um sich mit der Datenbearbeitung einverstanden zu erklären, ist es jedoch notwendig, dass ein Bewusstsein über die Datenbearbeitung vorhanden ist. Ein gangbarer Weg wäre beispielsweis, dass der Datenbearbeiter jedem Kunden einen Kunden-Account zur Verfügung stellt. Ergeben sich Änderungen in Bezug auf den Inhalt von Art. 13 Abs. 2 lit. a. – c., so informiert der Verantwortliche die betroffene Person. Die Kenntnisnahme über den Inhalt der Änderungen sowie die Zustimmung dazu erfolgt über den Kunden-Account. Vorschlag: *Der Verantwortliche informiert die betroffene Person über Änderungen gemäss Art. 13 Abs. 2 lit. a. – c.*
SKS	DSG	15	1		Die Formulierung, wonach die betroffene Person informiert werden muss, wenn Entscheidung durch automatisierte Datenbearbeitung erfolgt, wenn die Bearbeitung *rechtliche Wirkungen* oder *erhebliche Auswirkungen* auf die betroffene Person hat, ist ungenügend. Fast jeder Entscheid hat eine rechtliche Wirkung und im Begriff *erheblich* liegt ein enorm grosser Interpretationsspielraum. Es ist daher zu fordern, dass der Bundesrat entsprechende Definitionskompetenzen erhält.
SKS	DSG	18	1		Die Forderung nach technischem Datenschutz mit seinen modernen Instrumenten (z.B. Pseudonymisierung, Datenminimierung etc.) wird unterstützt. Mit der Formulierung von Art. 18 Abs. 1 ist die SKS jedoch nicht einverstanden. Die Bestimmung ist in zweierlei Hinsicht unzureichend: zum einen reicht es nicht aus, dass bloss *angemessene* Massnahmen getroffen werden zur Verringerung des Risikos von Persönlichkeits- und Grundrechtsverletzungen. Zum anderen soll dieses Risiko nicht bloss verringert, sondern nach Möglichkeit eliminiert werden. Vorschlag: *Der Verantwortliche und der Auftragsbearbeiter treffen Massnahmen, damit es ab Zeitpunkt der Planung der Datenbearbeitung zu keinen Verletzungen der Persönlichkeit oder der Grundrechte kommt*.

SKS	DSG	18	2		Gemäss Art. 18 Abs. 2 geht vom Prinzip privacy by default aus. Dieser Ansatz stellt materiellrechtlich einen der Eckpfeiler eines modernen Datenschutzgesetzes, welches sich in einem digitalen Umfeld behaupten muss, dar. Die Bestimmung wird daher mit Nachdruck unterstützt.
SKS	DSG	20	5		Gemäss Art. 20 Abs.5 ist der Auftragsbearbeiter auskunftspflichtig, *wenn er nicht bekannt gibt, wer der Verantwortliche ist*. Es gibt keinen Grund, wieso der Auftragsbearbeiter die Identität des Auftraggebers nicht bekannt geben sollte. Im Gegenteil: der Betroffene muss das Recht haben, in jedem Fall zu erfahren, wer den Auftrag für eine Datenbearbeitung gegeben hat. Die Passage „wenn er nicht bekannt gibt, wer der Verantwortliche ist“ ist somit zu streichen.
SKS	DSG	23	3		Art. 23 Abs. 3 bestimmt, unter welchen Voraussetzungen trotz einer Datenbearbeitung im Sinne von Abs. 2 lit. a. bis d. keine Persönlichkeitsverletzung vorliegt. So liegt dann keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Diese Bestimmung entspricht dem bisherigen Art. 12 Abs. 3. Hierzu sind dieselben Bemerkungen anzubringen wie bereits bei Art. 6 Abs. 1. lit. e.: In einem digitalisierten Umfeld ist der Begriff der *allgemeinen* Zugänglichkeit kein ausreichend scharfes Beurteilungskriterium mehr. Daher ist *allgemein* mit *öffentlich* zu ersetzen. Zudem ist es nicht zu rechtfertigen, dass eine Datenbearbeitung durch die betroffene Person untersagt werden muss – im Gegenteil: die betroffene Person hat der Datenbearbeitung ausdrücklich zuzustimmen. Vorschlag: *In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten öffentlich zugänglich gemacht hat und einer Bearbeitung ausdrücklich zugestimmt hat.*
SKS	DSG	24	2		Art. 24 sieht vor, dass Persönlichkeitsverletzungen gemäss Art. 23 bei Vorliegen von bestimmten Rechtfertigungsgründen zulässig sind, z.B. wenn ein überwiegendes privates oder öffentliches Interesse gegeben ist. Gemäss Art. 24 Abs. 2 ist ein überwiegendes Interesse der bearbeitenden Person möglicherweise gegeben, wenn die Voraussetzungen von lit. a. bis f. erfüllt seien. Den in lit. a. bis f. aufgezählten Rechtfertigungsgründen kann in dieser Form nicht zugestimmt werden. So kann es beispielsweise nicht sein, dass besonders schützenswerte Daten bearbeitet werden, weil die bearbeitende Person mit einer anderen Person in wirtschaftlichen Wettbewerb treten will.

					An der Unverhältnismässigkeit dieser Rechtfertigungsgründe ändert auch die Tatsache nichts, dass im Vergleich zur bisherigen Rechtfertigungs-Bestimmung (Art. 13) das Vorliegen eines überwiegenden Interesses nur *möglicherweise* angenommen wird, wenn die Voraussetzungen gemäss lit. a. bis f. erfüllt sind. Mit dem Begriff *möglicherweise* soll sicherstellte werden, dass stets eine Abwägung vorzunehmen ist zwischen den Interessen der betroffenen Person und derjenigen der bearbeitenden Person. Bei dieser Interessenabwägung handelt es sich jedoch um eine Selbstverständlichkeit, die ohnehin bei der Datenbearbeitung berücksichtigt werden muss. Um eine Verletzung der Persönlichkeitsrechte der betroffenen Person rechtfertigen zu können, müssten objektiv betrachtet schwerwiegende Gründe gegeben sein, wie beispielsweise das Abwenden eines Ereignisses, bei dessen Eintritt die Unversehrtheit oder allgemein die Rechte einer Vielzahl von Drittpersonen betroffen wären. Eine korrekte Datenbearbeitung im Rahmen der in lit. a. bis f. aufgezählten Sachverhalte wird bereits durch die Grundsätze von Art. 4 sichergestellt. Höchstens in der in lit. e. genannten Datenbearbeitung kann ein Rechtfertigungsgrund gesehen werden – unter der Voraussetzung, dass die in lit. e. genannten Einschränkungen strikte eingehalten werden.
SKS	DSG	27	3	b	Die Bestimmung sieht vor, dass eine Datenbearbeitung durch ein Bundesorgan unter anderem auch ohne rechtliche Grundlage erfolgen kann, sofern die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Hierzu sind wiederum dieselben Bemerkungen anzubringen wie bereits bei Art. 6 Abs. 1. lit. e. und Art. 23 Abs. 3: In einem digitalisierten Umfeld ist der Begriff der *allgemeinen* Zugänglichkeit kein ausreichend scharfes Beurteilungskriterium mehr. Daher ist *allgemein* mit *öffentlich* zu ersetzen. Zudem ist es nicht zu rechtfertigen, dass eine Datenbearbeitung durch die betroffene Person untersagt werden muss. Vorschlag: *Die betroffene Person hat ihre Personendaten öffentlich zugänglich gemacht und in die Bearbeitung eingewilligt.*
SKS	DSG	29	2	d	Gemäss dieser Bestimmung dürfen Bundesorgane im Einzelfall ausnahmsweise Daten bekannt geben, ohne dass dafür die notwendigen gesetzlichen Grundlagen bestehen, wenn die betroffene Person ihre

					Daten *allgemein* zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt hat. Hierzu sind wiederum dieselben Bemerkungen anzubringen wie bereits bei Art. 6 Abs. 1. lit. e., Art. 23 Abs. 3 und Art. 27 Abs. 3 lit. b.: In einem digitalisierten Umfeld ist der Begriff der *allgemeinen* Zugänglichkeit kein ausreichend scharfes Beurteilungskriterium mehr. Daher ist *allgemein* mit *öffentlich* zu ersetzen. Zudem ist es nicht zu rechtfertigen, dass eine Datenbearbeitung durch die betroffene Person untersagt werden muss. Vorschlag: *Die betroffene Person hat ihre Personendaten öffentlich zugänglich gemacht und in die Bearbeitung eingewilligt.*
SKS	DSG	30	1		Die Bestimmung sieht vor, dass die betroffene Person, die ein schutzwürdiges Interesse geltend macht, gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen kann. Im Umkehrschluss kann davon ausgegangen werden, dass die betroffene Person vorgängig über die Datenbekanntgabe zu informieren ist. Eine derartige Informationspflicht ist jedoch dem Gesetzesentwurf nicht zu entnehmen. Diese Informationspflicht ist daher an passender Stelle zu ergänzen.
SKS	DSG	39	2		Art. 39 Abs. 1 zählt auf, welche Nebenbeschäftigungen der EDÖB nicht ausüben darf. Unter anderem darf er kein Amt der Eidgenossenschaft oder eines Kantons bekleiden. Diese Einschränkung wird sehr begrüsst. Das Bekleiden eines politischen Amtes ist in aller Regel mit der Mitgliedschaft in einer politischen Partei verbunden ist. Der EDÖB sollte jedoch eine in höchstem Masse unabhängig, rein sachlich orientiert und ohne politische Hintergründe und Verflechtungen handelnde Person sein. Auf die Möglichkeit gemäss Abs. 2, vom dem in Absatz 1 aufgestellten Verbots von Nebenbeschäftigungen abzusehen, ist zu verzichten. Ausnahmen oder nur schon die Möglichkeit, solche zu gewähren, würden zu einer Aufweichung der durch das Verbot von Nebenbeschäftigungen garantierten Unabhängigkeit des EDÖB führen.
SKS	DSG	50ff.			Eine effiziente Rechtsdurchsetzung benötigt ein Instrumentarium, mit welchem den durch das Recht verpflichteten entsprechend Druck aufgesetzt werden kann. Die Erweiterung des Strafkatalogs sowie die markante Erhöhung des maximalen Bussenbetrags werden daher sehr begrüsst. Jedoch haften den vorgesehen Strafbestimmungen zwei wesentliche Mängel an: 1. Einzig „private Personen“ werden von den Strafbestimmungen erfasst. Wenn damit lediglich

					natürliche Personen gemeint sind, dann ist dies eine unzulässige Einschränkung 2. . Auch Unternehmen müssen der Strafbarkeit unterliegen. Gerade im digitalen Umfeld – und es ist unter anderem der selbsterklärte Anspruch der vorliegenden Gesetzrevision, das DSG ins digitale Zeitalter überführen zu wollen – sieht sich der Einzelne einer Datenbearbeitung ausgeliefert, die nicht in erster Linie durch Einzelpersonen, sondern durch Unternehmen vorgenommen wird. Mit der Beschränkung der Strafbarkeit auf Einzelpersonen geht ein wesentlicher Teil der präventiven Wirkung der strafrechtlichen Bestimmungen verloren. Die Strafbarkeit muss somit zwingend auf Unternehmen ausgeweitet werden. 3. Der Strafkatalog ist unvollständig. Es ist nicht ersichtlich, wieso Verletzungen der grundlegenden Basisverpflichtungen, die bei der Datenbearbeitung gemäss Art. 4 erfüllt sein müssen, nicht ebenfalls als Straftatbestand aufgeführt ist. In Art. 4 sind zentrale materiellrechtliche Bestimmungen enthalten, die für eine verhältnismässige, transparente, zweckgebundene und im Einverständnis der betroffenen Person erfolgende Datenbearbeitung notwendig sind. Vorschlag: *Mit Busse bis zu 500 000 Franken werden Datenbearbeiter bestraft, wenn bei einer durch sie selbst oder einen Auftragsbearbeiter vorgenommenen Datenbearbeitung vorsätzlich Grundsätze von Art. 4 nicht eingehalten werden.*

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
SKS	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
SKS	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")		
Name/Firma	**Kapitel-Nr.**	**Bemerkung/Anregung**

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
SKS		

Amstutz Jonas BJ

Von: Hess Markus <markus.hess@kellerhals-carrard.ch>
Gesendet: Montag, 3. April 2017 10:05
An: Amstutz Jonas BJ
Cc: Stengel Cornelia; Nisevic Gordana
Betreff: Vernehmlassung zum E-DSG
Anlagen: VE-DSG Stellungnahme SLV (def) (5116999).doc

Sehr geehrter Herr Amstutz

Gerne übermittle ich Ihnen in der Beilage die Vernehmlassung zum Entwurf einer Totalrevision des Datenschutzgesetzes in der gewünschten Form. Besten Dank für Ihre Kenntnisnahme und freundliche Grüsse

Markus Hess

Dr. Markus Hess
Geschäftsführer
Schweizerischer Leasingverband (SLV)
Rämistrasse 5 / Postfach
CH-8024 Zürich

Tel: +41 58 200 39 46 // M 079 407 35 91

E-Mail: markus.hess@leasingverband.ch
Homepage: www.leasingverband.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schweizerischer Leasingverband

Abkürzung der Firma / Organisation : SLV

Adresse : Rämistrasse 5, Postfach, 8024 Zürich

Kontaktperson : Dr. Cornelia Stengel, stv. Geschäftsführerin SLV

Telefon : 044 250 49 90

E-Mail : cornelia.stengel@leasingverband.ch

Datum : 3. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SLV	Der SLV nimmt zu den Regelungen des VE-DSG Stellung, welche die Privatwirtschaft, und dort insbesondere die Leasinggesellschaften, betreffen. Auf eine Stellungnahme zu den übrigen Regeln des VE-DSG und die weiteren Anpassungen in Zusammenhang mit Schengen, wird hingegen verzichtet. Der SLV begrüsst den weiterhin grundsätzlich prinzipienbasierten Ansatz des VE-DSG, die grundsätzliche Zulässigkeit von Datenbearbeitungen sowie das verfolgte Ziel, einer zum nahen Ausland äquivalenten Datenschutzgesetzgebung. Allerdings ist darauf zu achten, dass die neuen Bestimmungen keinesfalls über das hinausgehen, was die DSGVO fordert. Ein solcher „Swiss Finish“ wird ausdrücklich abgelehnt.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SLV	DSG	2	1		Der Verzicht auf den Schutz von Daten juristischer Personen ist aus Sicht von SLV sinnvoll. Dieser Schutz ist bereits heute von geringer praktischer Bedeutung, behindert aber oftmals die Bekanntgabe von Daten ins Ausland. Zudem ist auch in der EU-DSGVO sowie im Übereinkommen des Europarats kein Schutz von Daten juristischer Personen vorgesehen. Ein Verzicht darauf führt damit nicht zu einem tieferen, nicht-äquivalenten Datenschutzniveau in der Schweiz.
SLV	DSG	2	2		Der Wegfall der Ausnahme gemäss Art. 2 Abs. 2 lit. c DSG für hängige Zivilprozesse, Strafverfahren etc. öffnet dem Missbrauch Tür und Tor. Insbesondere das Auskunftsrecht soll nicht zur Beweisbeschaffung benutzt werden können – dafür sind die Regeln zu Editionsbegehren in der ZPO einzuhalten.
SLV	DSG	3		f	Die Definition von „Profiling“ ist auf elektronische Aktivitäten zu begrenzen. Dies umso mehr, als auch die EU-DSGVO diese Einschränkung vorsieht. Um Rechtsunsicherheit zu vermeiden, wird zudem vorgeschlagen, den Begriff „wesentliche persönliche“ zu wiederholen, und damit klar zu stellen, dass nur „wesentliche persönliche Entwicklungen“ gemeint sind. Zusammenfassend werden folgende Änderungen und Präzisierungen von Art. 3 lit. f VE-DSG vorgeschlagen (Änderungen fett und unterstrichen): «Profiling: jede **elektronische** Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder **wesentliche persönliche** Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;»
SLV	DSG	4	3		Die Bestimmung des Art. 4 Absatz 3 VE-DSG wurde gegenüber den geltenden Art. 4 Abs. 3 und 4 DSG um das Wort **«klar»** ergänzt. Diese Verschärfung ist unnötig und wird vom SLV klar abgelehnt, zumal gemäss erläuterndem Bericht keine materiellen Änderungen beabsichtigt sind. Massgebend muss der unter Berücksichtigung aller Umstände und gemäss Treu und Glauben objektivierbare Grad der Erkennbarkeit des

					Zwecks sein.
SLV	DSG	5	1		**Datenbekanntgabe ins Ausland:** Der Absatz 1 von Art. 5 VE-DSG ist verwirrend, da unklar bleibt, inwiefern die darin gemachte Aussage das in den folgenden Absätzen minutiös dargestellte Verfahren beeinflusst. Richtigerweise spielt die Aussage von Abs. 1 keine Rolle, soweit die in den nachfolgenden Absätzen getroffenen Regelungen eingehalten werden. Demzufolge kommt Abs. 1 keine selbständige Bedeutung zu und ist folgerichtig ersatzlos zu streichen.
SLV	DSG	5	3		Für den Fall, dass (noch) kein Entscheid des Bundesrats hinsichtlich der Angemessenheit des Schutzes in einem Land vorliegt, soll der Verantwortliche diese Angemessenheit prüfen können. Entsprechend müsste Art. 5 Abs. 3 VE-DSG folgendermassen ergänzt werden (Ergänzung fett und unterstrichen): «Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, **wenn der Verantwortliche selbst festgestellt hat, dass ein angemessener Schutz gewährleistet ist oder,** wenn ein geeigneter Schutz gewährleistet ist durch: […]»
SLV	DSG	5	3/5	c/d	Die in Art. 5 Abs. 3 lit. c Ziff. 1 und lit. d sowie Abs. 5 VE-DSG vorgeschlagene **Genehmigungspflicht** wird vom SLV abgelehnt. Die Pflicht zur Genehmigung durch den Beauftragten führt zu einem enormen Mehraufwand, ggf. zu grossen Projektverzögerungen bei Unternehmen und dürfte auch die Behörde überlasten. Gleichzeitig trägt eine Genehmigungspflicht kaum etwas zum bessern Datenschutz bei, steht doch das Unternehmen weiterhin selbst in der Verantwortung. Schliesslich sieht auch die EU-DSGVO eine solche Genehmigungspflicht nicht vor. Die vom VE-DSG vorgesehene Genehmigungspflicht wäre deshalb überschiessender Swiss Finish, welcher den grenzüberschreitenden Datenfluss erheblich und unnötigerweise erschweren würde und dem Äquivalenzprinzip in Bezug auf die europäische Datenschutzgesetzgebung abträglich wäre.
SLV	DSG	5	6		Die Informations- bzw. Meldepflicht in Art. 5 Abs. 6 VE-DSG ist zu streichen, da sie keinen Beitrag zum Datenschutz leistet. Eine solche Meldepflicht ist zudem systemfremd, geht es doch um bereits vorliegende

					standardisierte Garantien. Weshalb die Verwendung solcher Standards in jedem Fall erneut eine Meldepflicht auslösen soll, ist unerfindlich. Zudem entsprechen solche Meldepflichten nicht dem etablierten EU-Recht und sind deshalb ein Swiss Finish, welcher der gesetzgeberischen Absicht und dem erklärten Ziel von Äquivalenz mit der europäische Datenschutzgesetzgebung widersprechen (vgl. EuGH-Entscheid Schrems u. gestützt darauf ergangener Entscheid der EU-Kommission vom 16.12.2016, wonach von ihr genehmigte Datenschutz-Standardklauseln nicht erneuter Bewilligung im Einzelfall bedürfen und deshalb ohne Einschränkung verwendet werden dürfen; Art. 45 EU-DSGVO). Zumindest die Meldepflicht oder konsequenterweise der ganze Absatz 6 ist demzufolge zu streichen.
SLV	DSG	6	a		Die Einschränkung „im Einzelfall“ ist weder sinnvoll noch notwendig, da selbst für wiederkehrende Sachverhalte wegen gleichbleibender Erkennbarkeit und unverändertem Erwartungshorizont eine einmalige Einwilligung ausreichen muss. Der Zusatz „im Einzelfall“ widerspricht auch der Gesetzessystematik, wonach nur für die unter lit. c und d genannten Fälle die „Bekanntgabe im Einzelfall“ geregelt werden soll. Der Zusatz „im Einzelfall“ ist deshalb bei lit. a ersatzlos zu streichen.
SLV	DSG	6	b		Der gewählte Wortlaut ist zu eng, da es regelmässig um Zusatzverträge geht, welche nicht direkt mit dem Vertragspartner abgeschlossen werden, aber in dessen Interesse liegen, weil z.B. solche Zusatzverträge nötig sind, um den mit dem Vertragspartner geschlossenen Vertrag zu erfüllen. Die Formulierung ist deshalb am Ende wie folgt zu ergänzen (Ergänzungen fett und unterstrichen): „ … des Vertragspartners **oder von Personen, in deren Interesse der Vertrag abgeschlossen werden soll,** handelt. Diese Anpassung sollte auch bei Art. 24 Abs. 2 lit. a VE-DSG vorgenommen werden.
SLV	DSG	8			**Empfehlungen der guten Praxis:** Der SLV begrüsst insbesondere die in Art. 8 VE-DSG definierte Möglichkeit zur Erarbeitung von Empfehlungen der guten Praxis und den aktiven Beizug der interessierten Kreise. Allerdings sollen diese nicht vom Beauftragten, sondern von den jeweiligen Branchen selbst erarbeitet und bestenfalls auch nicht genehmigungspflichtig sein. Es soll an dieser Stelle keine Rechtsetzungskompetenz

					des Beauftragten eingeführt werden.
SLV	DSG	13	2		**Informationspflichten:** **Ganz grundsätzlich sollten die Regeln zur Informationspflicht überarbeitet werden. Eine risikobasierte Transparenzpflicht würde völlig genügen und auch einer „Informationsflut" vorbeugen.** Art. 13 Abs. 2 VE-DSG muss dahingehend präzisiert werden, dass die zu erteilenden Informationen nur im erstmaligen Zeitpunkt der Datenbeschaffung richtig und vollständig sein müssen. Spätere Änderungen, insbesondere der Identität des Verantwortlichen, müssen der betroffenen Person nicht mitgeteilt werden. Diesbezüglich sollte insbesondere darauf verzichtet werden, dass der Verantwortliche namentlich genannt werden muss, da die Person des Verantwortlichen wechseln kann. Als Kontaktdaten des Verantwortlichen muss es genügen, dass eine klare und fix definierte Funktionsbeschreibung mitgeteilt wird.
SLV	DSG	13	4		Problematisch und deshalb zu streichen, ist die Pflicht gemäss Art. 13 Abs. 4 VE-DSG, aktiv die *Identität* der Auftragsdatenbearbeiter bekannt zu geben. Die Identität von Auftragsdatenbearbeitern wird regelmässig zum Geschäftsgeheimnis eines Unternehmens gehören und damit wohl ohnehin unter die Ausnahmen von Art. 14 Abs. 3 VE-DSG fallen. Dementsprechend geht auch die EU-DSGVO nicht soweit, weshalb diese Regelung einen mit Blick auf die angestrebte Äquivalenz mit der europäischen Datenschutzgesetzgebung kontraproduktiven Swiss Finish darstellen würde. Absatz 4 wird primär im Rahmen von Outsourcing-Verhältnissen zum Tragen kommen, bei welchen die Verantwortung der Datenbearbeitung gegenüber der betroffenen Person beim auslagernden Unternehmen verbleibt, und auch nur dieses auskunftspflichtig sein kann. Es kann nicht sein, dass Dienstleistungserbringer gegenüber Kunden von Dritten auskunftspflichtig sind.
SLV	DSG	15	5		Eine Information „spätestens bei Speicherung" ist ein Swiss Finish. Art. 14 Abs. 3 lit. a DSGVO sieht hier eine Frist von bis zu einem Monat vor.
SLV	DSG	14	3	a	Art. 14 Abs. 3 lit. a VE-DSG ist zu eng gefasst. Direkte Einschränkungen ergeben sich nur ganz selten aus einem Gesetz. Häufiger ist der Fall, dass ein Gesetz zwingende Abklärungspflichten, oft verbunden mit damit einhergehenden Geheimhaltungspflichten vorsieht, welche indirekt zu einer Einschränkung von

					Informationspflichten führen. Dies ist in der Regelung von Art. 14 Abs. 2 lit. a VE-DSG zu präzisieren und zum besseren Verständnis mit der Aufzählung einiger typischer Beispiele zu ergänzen. Zu denken ist etwa an zwingend vorgeschriebene Abklärungen zur Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Korruption.
SLV	DSG	14	3	B	Unter Art. 14 Abs. 3 lit. b VE-DSG ist nicht einsehbar, weshalb nur überwiegende Interessen Dritter massgebend sein sollen. Gleichermassen müssen überwiegende Interessen des Verantwortlichen und überdies der Öffentlichkeit relevant sein. Nur eine umfassende Interessenabwägung kann in zahlreichen Konstellationen zu einer sachgerechten Lösung führen.
SLV	DSG	15			**Automatisierte Einzelentscheidung:** Der Anwendungsbereich dieser Regelung in der vorgeschlagenen Form ist gewaltig. So wären nicht nur die in den Erläuterungen erwähnten Situationen (Vertragsabschluss und Verkehrsbussen) betroffen, sondern beispielsweise auch automatisierte Kontrollen von Transaktionen (Kontrolle Zahlungseingang inkl. Buchung und Auslösung von Mahnungen etc.) oder Sicherheitsmechanismen wie Spamfilter etc. Während gemäss Art. 22 Abs. 2 lit. b DSGVO Ausnahmen möglich sind, sieht Art. 15 VE-DSG keine solchen vor. Das ist unbedingt zu ändern und der Erlass von Ausnahmen zumindest auf dem Verordnungsweg zu ermöglichen.
SLV	DSG	15	1		Um Klarheit zu schaffen, dass nicht jede (rechtliche) Wirkung, wie z.B. ein Geldbezug am Bankomat (Entscheid, ob Geld ausbezahlt wird, erfolgt automatisch) betroffen ist, sollte der Begriff „erhebliche“ wiederholt verwendet werden. Art. 15 Abs. 1 VE-DSG müsste folgendermassen ergänzt werden (Ergänzung fett und unterstrichen): „…und diese **erhebliche** rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffenen Person hat“
SLV	DSG	15	2		Das in Art. 15 Abs. 2 VE-DSG neu vorgeschlagene Recht einer betroffenen Person, sich zu einer automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern („Anhörungspflicht“), ist wettbewerbs- und auch innovationsbehindernd. Darüber hinaus ist dieses Recht aber auch schlicht unnötig, insbesondere angesichts der ebenfalls neu eingeführten Pflicht, die betroffene

					Person darüber zu informieren, wenn eine automatisierte Einzelentscheidung gefällt wurde (vgl. Abs. 1 von Art. 15 VE-DSG). Die Kunden können selbst entscheiden, ob sie von einem Anbieter Dienstleistungen beziehen möchten, der voll-automatisierten Entscheide trifft oder zu einem Anbieter, der zusätzlich oder vollständig auf die Arbeitskraft natürlicher Personen setzt. Der Kunde wird davon gemäss Art. 15 Abs. 1 VE-DSG bereits ausreichend informiert (z.B. mit einem Piktogramm). Art. 15 Abs. 2 VE-DSG ist ersatzlos zu streichen. (Folgerichtig ist auch der entsprechende thematische Abschnitt in **Art. 20 Abs. 3 VE-DSG** zu streichen, vgl. unten.)
SLV	DSG	16			**Datenschutz-Folgenabschätzung** Die vorgeschlagene Bestimmung in Art. 16 VE-DSG ist sehr unklar formuliert und soll gemäss dem erläuternden Bericht sehr extensiv ausgelegt werden. So werden als Indiz für ein erhöhtes Risiko fast alle denkbaren Tätigkeiten/Tatbestände im Umgang mit Daten aufgezählt. Trotz der sehr offenen und unklaren Bestimmung soll ein Verstoss gegen die Bestimmung strafrechtlich sanktioniert werden. Dies widerspricht klar dem strafrechtlichen Prinzip von „nulla poena sine lege stricta". Eine Datenbearbeitung braucht für ein Unternehmen, das die Bestimmungen des Datenschutzgesetzes einhalten will, bereits heute eine fachkundige Beurteilung und entsprechende Massnahmenpakete. Dies gesetzlich zu verankern, inklusive einer Benachrichtigungspflicht an den Beauftragten, der innerhalb einer relativ langen Frist Einwände mitteilen kann und später, trotz Nichtäusserung, eine Untersuchung einleiten kann, bringt keinen Mehrwert, sondern verursacht vielmehr erhebliche Rechtsunsicherheit. Wenn schon müsste die Pflicht zur Datenschutzfolgeabklärung, wie auch gemäss EU-DSGVO, auf Datenbearbeitungen beschränkt werden, bei welchen nach einer Folgeabschätzung mit entsprechenden Massnahmen ein hohes Risiko verbleibt, beschränkt werden.
SLV	DSG	16	1		Die Begriffe „voraussichtlich" und „erhöht" in Zusammenhang mit dem Risiko sind unklar. In der Schweiz gibt es keine Drittwirkung für Grundrechte, weshalb private Datenbearbeiter ein Risiko für Grundrechte nicht zu prüfen haben. Dies ist klarzustellen. Schliesslich ist es unsinnig, den Auftragsdatenbearbeiter als Dienstleistungserbringenden für den Verantwortlichen ebenfalls zu verpflichten, eine Datenschutz-

					Folgenabschätzung durchzuführen. Diese Überlegungen führen zu folgenden Änderungsanträgen: „Führt die vorgesehene Datenbearbeitung **mit überwiegender Wahrscheinlichkeit** zu einem hohen Risiko für die Persönlichkeit ~~**oder die Grundrechte**~~ der betroffenen Person, so muss der Verantwortliche ~~**oder der Auftragsdatenbearbeiter**~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen.“
SLV	DSG	16	2		Der Begriff „Persönlichkeit oder Grundrechte“ entspricht nicht der Schweizer Gesetzessystematik und sollte durch der Begriff „Persönlichkeitsverletzung“ ersetzt werden (vgl. insb. Art. 23 ff. VE-DSG). In der Schweiz haben Grundrechte keine Drittwirkung.
SLV	DSG	16	3/4		Der Beauftragte wird massiv grösseren Aufwand haben, wenn er jede dieser Einschätzungen zu studieren und zu beurteilen hat. Hat der Beauftragte die dafür notwendigen Kapazitäten gar nicht, macht die Regel definitiv keinen Sinn, sondern produziert nur unnötigen Aufwand für die Verantwortlichen. Die Frist für die Stellungnahme durch den EDÖB ist viel zu lang, auch im Vergleich mit der 8-wöchigen Frist der DSGVO.
SLV	DSG	17			**Meldepflicht bei Verletzung des Datenschutzes** Die in Art. 17 VE-DSG vorgeschlagene Meldepflicht hat einen klaren rechtsdogmatischen Mangel und führt zu einer regelrechten „Angstkultur“ im Bereich des Datenschutzes. Zwar wird auch ein Verstoss gegen die Meldepflicht selbst sanktioniert, wenn die Verletzung entdeckt würde, aber die Meldung gemäss Art. 17 entspricht einer Selbstanzeige, welche mit Sicherheit zu einer Sanktion führt, weil für diesen Fall keine Erleichterungen bei den Sanktionen vorgesehen sind (anders als z.B. im Kartellrecht). Entsprechend wird ein korrekt handelnder Mitarbeiter, der eine Datenschutzverletzung meldet, auf jeden Fall bestraft, während die wirklich „schwarzen Schafe“, welche nicht im Traum daran denken, eine DSG-Verletzung zu melden, mangels Bekanntwerden des Sachverhaltes i.d.R. straffrei bleiben dürften. Die Mitarbeiter eines Unternehmens müssten sich auch gegenseitig anzeigen, um selbst straffrei zu bleiben, wenn sie unbeteiligt waren. Wir bezweifeln die Sinnhaftigkeit dieser Regel. Bei Datenschutzverstössen steht immer auch die Reputation eines Unternehmens auf dem Spiel. Insofern ist es im Eigeninteresse eines jeden seriösen Unternehmens, Kunden korrekt und rechtzeitig zu informieren. Dies hat den auch bisher immer auch ohne gesetzliche

					Vorschriften funktioniert. Infolge dessen sollte diese Bestimmung **ersatzlos gestrichen** werden. ***Eventaliter*** müsste sie jedenfalls auf wirklich heikle Fälle beschränkt werden. Diese Fälle sind mit qualitativen und quantitativen Kriterien angemessen einzugrenzen. Qualitative Kriterien wären insbesondere ein hoher Verletzungsgrad (analog EU-DSGVO) und die Tatsache, dass durch die Meldung an den Beauftragten ein Mehrwert geschaffen werden kann, z.B. mittels Unterstützung durch den Beauftragten in Fällen, welche vom betroffenen Verantwortlichen nicht mehr allein aus eigener Kraft bereinigt werden kann. Dies kann z.B. dann der Fall sein, wenn - als quantitatives Kriterium durch ein grösseres Sicherheitsleck massenweise Kundendaten gestohlen oder öffentlich werden. Zudem wäre die „unverzügliche“ Meldepflicht gemäss Art. 17 Abs. 4 VE-DSG zu präzisieren. Eine Meldepflicht kann sachlogisch erst ab dem Zeitpunkt bestehen, in welchem der Verantwortliche mit einiger Klarheit weiss, was überhaupt geschehen ist und welche Kunden (-Segmente) betroffen sind. Ohne diese Eingrenzungen wäre die Schweizer Regelung überschiessend und entgegen dem Revisionszweck nicht äquivalent mit der entsprechenden europäischen Gesetzgebung.
SLV	DSG	19		a	Art. 19 lit. a VE-DSG belässt extrem weiten Spielraum mit Bezug auf Form und Inhalt, was mit Blick auf die strafrechtlichen Sanktionen unhaltbar ist. Eine Präzisierung auf dem Verordnungsweg wäre mit Blick auf die Rechtsstaatlichkeit bedenklich. Die Dokumentationspflicht ist daher durch das blosse **Erfordernis eines Verzeichnisses der Datenbearbeitungen** zu ersetzen, wie dies auch die DSGVO vorsieht.
SLV	DSG	19		b	Art. 19 lit. b VE-DSG ist eine massive Verschärfung der heutigen Rechtslage und würde zu komplizierten Abläufen und grossen (finanziellen) Aufwänden führen. Der SLV setzt sich aus folgenden Gründen für eine Streichung dieser Bestimmung ein: • Der aktuelle Vorschlag würde dazu führen, dass Unternehmen in die Rolle eines (öffentlichen) Registers gedrängt würden und für die ständige Aktualisierung der Daten auch bei Dritten sorgen müssten. Solche Pflichten sind überschiessend und sprengen den Rahmen einer vernünftigen Datenschutzgesetzgebung.

					• Der Nutzen dieser Bestimmung im Hinblick auf nicht besonders schützenswerte Daten ist besonders fragwürdig. Schliesslich sind viele nicht besonders schützenswerte Daten sogar öffentlich zugänglich (z.B. über Internetrecherche). • Eine Information zu Verletzungen des Datenschutzes geht über Art. 30 DSGVO hinaus und ist auch schlicht unsinnig. Denn diese Information müsste auch erfolgen, wenn an die betroffene Person selbst keine Breach-Notification gemacht werden müsste. • Die Bestimmung ist in keiner Art und Weise eingeschränkt, so dass weder das Interesse der betroffenen Person, noch eine Wunsch zur Nachinformation durch die betroffene Person nötig ist. Es müsste also beispielsweise auch über automatische Löschungen von Daten z.B. nach Ablauf einer gesetzlichen Aufbewahrungspflicht, nachinformiert werden. Nach alledem fordert der SLV die ersatzlose Streichung von lit b des Art. 19 VE-DSG. *Eventualiter* könnte die Bestimmung so eingeschränkt werden, dass die Nachinformation nur nötig ist, wenn dies von der betroffenen Person aus berechtigten Gründen verlangt.
SLV	DSG	20/21			**Auskunftsrecht:** Die Information darüber, wie bestimmte Entscheide zustande kommen, gehört zum Geschäftsgeheimnis eines Finanzinstitutes und ist demnach, insbesondere in der aktuell vorgesehen, detaillierten Form gemäss Art. 20 Abs. 3 VE-DSG, klar unverhältnismässig. So ist zum Beispiel das Vorgehen im Rahmen der Einschätzung von Ausfallrisiken bei der Leasing- bzw. Kreditvergabe ein wichtiges, differenzierendes Know-How einer Leasinggesellschaft. Die Auskunft über die für diese Einschätzung genutzten Daten und deren Gewichtung führt zu einer Replizierbarkeit dieser Einschätzung und damit zur Aufgabe dieses Geschäftsgeheimnisses. Die Einschränkungsbestimmung des Art. 21 Abs. 1 VE-DSG dürfte daher mehr die Regel als die Ausnahme bilden. Schliesslich ist die Befürchtung nicht von der Hand zu weisen, dass die Einführung einer „Pflicht zur Anhörung“ zu einer Begründungspflicht führt und letztlich die Vertragsfreiheit eines Unternehmens erheblich einschränkt.
SLV	DSG	20	3		Die Regel von Art. 20 Abs. 3 VE-DSG muss gestrichen werden. Dies ist konsequent, da sich der SLV auch

					für eine Streichung der Anhörungspflicht von Art. 15 Abs. 2 VE-DSG einsetzt (vgl. oben). Eventualiter, müsste jedenfalls Art. 20 Abs. 3 VE-DSG als dort - unter dem allgemeinen Auskunftsrecht - sachfremde Regelung gestrichen und mit Art. 15 VE-DSG zu einer in sich stimmigen Gesamtlösung verbunden werden. Dabei wäre die Regelung (entsprechend dem richtigen Ansatz der DSGVO [Art. 15 Abs. 1 lit. h], mit welchem der VE-DSG äquivalent sein will) auf Fälle mit „erheblichen Auswirkungen“ zu begrenzen. Sodann wäre klarzustellen, dass eine einmal in angemessener Art und Weise erfolgte Information im Sinne der Gesetzessystematik ausreichend ist und es wäre klarzustellen, dass dieses Auskunftsrecht nur einer von der jeweiligen automatischen Einzelentscheidung tatsächlich betroffenen Person ausgeübt werden könnte.
SLV	DSG	23	2		Nachdem es sich beim Begriff „Profiling“ um einen sehr weit gefassten Begriff handelt, sollte eine entsprechende Datenbearbeitung nicht automatisch angenommen werden, wenn keine ausdrückliche Einwilligung der betroffenen Person vorliegt.
SLV	DSG	50 ff.			**Sanktionen** Viele Pflichten und damit die Tatbestände sind zu wenig konkret und erfüllen damit die Regel von „nulla poena sine lege stricta“ nicht. Nur wenn aufgrund der gesetzlichen Bestimmung klar ist, welches Verhalten gefordert ist bzw. welche Unterlassung eine Verletzung darstellt, ist eine Sanktionierung möglich. Strafrechtlich sanktionierbar dürfen mit Blick auf die weitreichenden Folgen jedenfalls zum Vornherein nur solche Pflichten sein, die (i) eine wesentliche Verbesserung des Datenschutzes bei den betroffenen Personen sicherstellen wollen und - kumulativ - (ii) genügend präzis formuliert sind, damit der Verantwortliche bzw. dessen Mitarbeitenden durch geeignete Handlungsweisen, Implementierung geeigneter Massnahmen, etc. tatsächlich verhindern können, je mit strafrechtlichen Vorwürfen konfrontiert zu werden. Ganz grundsätzlich ist zu überdenken, ob das Konzept der strafrechtlichen Sanktionen tatsächlich die richtige Wahl ist. Der SLV verweist diesbezüglich auf die diesbezügliche Stellungnahme von economiesuisse („Vorschlag der Wirtschaft“), welche vollumfänglich unterstützt wird.
SLV	DSG	59			**Übergangsfristen**

					Die 2 Jahre Übergangsfrist muss generell gelten, nicht nur für die Umsetzung einzelner Elemente, um den Unternehmen genügend Zeit zu geben, ihre Systeme und Prozesse an die neue gesetzliche Ausgangslage anzupassen.

Gerne hoffen wir, Ihnen mit unseren Ausführungen zu dienen und bitten um Berücksichtigung der vorgetragenen Argumente und Anträge.

Freundliche Grüsse

sig. Dr. Cornelia Stengel
stv. Geschäftsführerin

SOCIÉTÉ MÉDICALE DE LA SUISSE ROMANDE

FRIBOURG – GENÈVE – JURA – NEUCHÂTEL – VALAIS – VAUD

Par email: jonas.amstutz@bj.admin.ch
Département fédéral de justice et police
Monsieur Jonas Amstutz
Postfach
3003 Bern

Lausanne, le 3 avril 2017

Procédure de consultation la Loi sur la protection des données
Prise de position de la SMSR

Cher Monsieur,

Vous trouverez ci-dessous la prise de position de la Société Médicale de la Suisse Romande suite à la procédure de consultation sur la révision LPD.

Au premier abord, l'AP-LPD ne contient pas de dispositions spécifiques à la pratique médicale. Cela étant, la révision LPD se base sur une approche fondée sur les risques potentiels pour les personnes concernées : plus les menaces pesant sur la sphère privée des personnes concernées sont grandes, plus les exigences imposées aux personnes traitant les données personnelles sont élevées. Ainsi, les obligations à la charge de ces personnes seront d'autant plus strictes dans le domaine médical où les données sont sensibles, que dans d'autres domaines où les données sont moins sensibles. Il est donc utile que la profession médicale se penche sur ces questions en amont de l'édiction de la loi. Vous trouverez ci-après présentés de manière synthétique quelques éléments paraissant pertinents à la SMSR. Ils font référence au récapitulatif fourni par la FMH ainsi qu'au Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales du département fédéral de justice et police (DFJP) du 21 décembre 2016 (le « Rapport Explicatif »).

A. Le renforcement des dispositions légales en matière de protection des données est positif. Les points suivants doivent en particulier être salués :

1. L'intégration désormais expresse des données génétiques[1] dans la notion de « données sensibles » (art. 3 let. c ch. 3 AP-LPD ; para. 1.4.1 et 8.1.1.3 du Rapport Explicatif) est bienvenue, et de nature à renforcer la confiance des patients en raison de la protection accrue accordée à ce type de données.

[1] Ainsi que des données biométriques identifiant un individu de manière unique et les données concernant la vie sexuelle

2. Les obligations du responsable du traitement des données (principe de transparence) sont orientées davantage sur la protection de la personne concernée (para. 1.4.1 du Rapport Explicatif). Comme indiqué ci-dessous, certaines de ces obligations méritent d'être clarifiées.

3. L'introduction d'un devoir d'informer et d'entendre la personne concernée en cas de décisions individuelles automatisées est positive (art. 20 al. 2 let. e et al. 3 AP-LPD ; para. 8.1.3.3 du Rapport Explicatif). Cela concerne notamment les cas où une assurance régie par la LCA (ex. assurance-maladie privée, assurance-vie) refuse de conclure un contrat avec une personne après évaluation par un algorithme de ses données de santé.

4. Il paraît correct de ne pas introduire un droit à la portabilité des données (para. 1.6.4 du Rapport Explicatif), qui vise à structurer les données d'une manière permettant de les transmettre facilement d'un système de traitement automatisé à un autre. Un tel droit ne vise pas directement à la protection de la personnalité et engendrerait un surcoût important.

5. L'AP-LPD prévoit le droit des tiers d'accéder aux données personnelles d'une personne décédée (art. 12 AP-LPD ; para. 8.1.2.9 du Rapport Explicatif). En matière médicale, il arrive souvent que des proches demandent à accéder au dossier médical du défunt. En raison des dispositions de l'art. 321 CP sur le secret professionnel, cette situation pose problème. La réglementation proposée est ainsi bienvenue dans la mesure où elle permet aux proches du défunt d'avoir accès à son dossier médical sous réserve d'opposition de ce dernier ou d'intérêts prépondérants de tiers. A noter que l'AP-LPD opère une levée automatique du secret professionnel ou de fonction au sens de l'art. 321 ch. 3 CP (art. 12 al. 3 AP-LPD), sans que le médecin doive se faire préalablement délier par l'autorité de levée du secret de l'art. 321 ch. 2 CP. Par ailleurs, l'accès au dossier a lieu dans devoir obligatoirement passer par l'intermédiaire d'un médecin2[2] (à noter que l'art. 12 AP-LPD ne contient aucune disposition similaire à l'art. 20 al. 4 APLPD applicable au droit d'accès des personnes concernées). Cette solution est plus libérale que disposition correspondante du droit genevois (art. 55a LSanté), laquelle prévoit non seulement la saisine obligatoire de la Commission du secret médical, mais également l'accès aux données du défunt obligatoirement par l'intermédiaire d'un médecin. La réglementation prévue par l'AP-LPD paraît appropriée sur ce point.

6. Selon l'art. 8 AP-LPD, le préposé fédéral à la protection des données peut édicter des recommandations de bonne pratique précisant les dispositions de protection des données dans certains domaines, en associant les milieux intéressés. Ces derniers peuvent en outre compléter les recommandations du préposé ou élaborer leurs propres recommandations, qu'ils peuvent ensuite faire approuver par le préposé. Cette méthodologie paraît particulièrement bien adaptée au secteur de la santé, et devrait permettre de préciser les notions et modalités d'application de la LPD en ce qu'ils s'appliquent à la profession médicale. En permettant aux milieux concernés d'être eux-mêmes actifs dans la réglementation de leur secteur, le Conseil fédéral entend favoriser l'émergence de solutions de branches, concertées et largement acceptées. Dans ce contexte il semblerait judicieux que les milieux médicaux se concertent, et que la FMH approche le préposé de manière proactive avec de telles recommandations pour la branche médicale.

[2] A noter que l'art. 12 AP-LPD ne contient aucune disposition similaire à l'art. 20 al. 4 AP-LPD, applicable au droit d'accès de la personne concernée.

B. <u>Certaines questions méritent d'être clarifiées, en particulier compte tenu de l'introduction d'un système de sanctions pénales plus lourde dans la nouvelle LPD :</u>

1. L'AP-LPD prévoit désormais clairement un <u>droit à l'effacement des données</u> (art. 25 al. 1 let. c AP-LPD ; para. 1.4.2.2 du Rapport Explicatif), lequel correspond au « droit à l'oubli » conféré de manière générale par la protection de la personnalité en droit civil. Il serait utile de traiter explicitement les exceptions au droit à l'effacement au niveau de la LPD. S'agissant en particulier de la pratique de la médecine, les lois sanitaires cantonales prévoient généralement des délais spécifiques de conservation du dossier médical. A Genève, l'art. 57 LSanté commande une durée de conservation minimale de 10 ans et une durée maximale de 20 ans, sauf circonstances spéciales commandant une durée de conservation plus longue. Pareille réglementation va à l'encontre d'un droit à l'effacement des données à la demande de la personne concernée. Une réserve explicite dans la LPD en faveur de ces dispositions (ou leur exclusion pure et simple) serait appropriée afin d'éviter des difficultés en pratique.

2. L'AP-LPD prévoit désormais un <u>consentement exprès lorsqu'il s'agit de traiter des données sensibles</u> (art. 4 al. 6 AP-LPD ; para. 8.1.2.1 du Rapport Explicatif). Le Rapport Explicatif clarifie par ailleurs cette notion, qui recouvre les données médicales (art. 3 let. c ch. 2 AP-LPD). Il conviendrait toutefois de préciser comment cette exigence se traduit dans le domaine médical, où il est largement admis que le consentement à l'acte médical (qui inclut nécessairement le consentement au traitement de données personnelles sensibles) peut être donné de façon tacite ou par actes concluants. Il importe que cette question soit clarifiée en amont de l'édiction de la loi afin d'éviter des difficultés pour la pratique médicale quotidienne.

3. L'AP-LPD contient une nouvelle notion de « <u>profilage</u> », défini comme « toute exploitation de données, personnelles ou non, qui consiste à analyser ou prédire les caractéristiques personnelles essentielles d'une personne », notion couvrant notamment la santé (para. 8.1.1.3 let. f du Rapport Explicatif). En d'autres termes, tout traitement de données consistant à analyser ou prédire des caractéristiques essentielles de la personnalité, par exemple la santé, sera considéré comme du profilage (para. 8.2.2 du Rapport Explicatif). Selon cette définition, toute activité de diagnostic médical pourrait être considérée comme une activité de profilage. Il conviendrait de préciser si tel est bien le cas, car à l'instar des données sensibles mentionnées ci-dessus au point B 2, le profilage requiert un consentement exprès (art. 4 al. 6 AP-LPD), ce qui exclurait le consentement tacite ou par actes concluants.

4. S'agissant du <u>droit d'accès par la personne dont les données sont traitées</u> (para. 8.1.4.2 et 8.1.3.2 du Rapport Explicatif). Dans le domaine médical, le droit d'accès au dossier est prévu par plusieurs sources, en particulier à Genève l'art. 55 al. 1 LSanté. L'exception en faveur des droits prépondérants de tiers figurant à l'art. 55 al. 2 LSanté est également prévue à l'art. 14 al. 3 let. b AP-LPD. En ce qui concerne l'exception concernant les notes personnelles du médecin prévue à l'art. 55 al. 2 LSanté, elle ne connaît pas d'équivalent dans l'AP-LPD, sous réserve d'une application large de l'art. 14 al. 4 let. a AP-LPD (intérêts prépondérants de la personne qui traite les données). Dans un but de clarté, il serait souhaitable de préciser le statut des notes personnelles du médecin dans la LPD révisée. Enfin, si le principe de l'accès gratuit est en soi positif (art. 20 al. 1 AP-LPD), il convient de maintenir l'exception figurant à l'art. 2 al. 1 let. b OLPD pour les cas où la communication des renseignements demandés occasionne un volume de travail considérable.

5. L'obligation de procéder à une analyse d'impact du traitement puis de la communiquer ensuite au préposé, lorsque le traitement des données envisagé est susceptible d'entraîner un « risque accru » pour la personnalité et les droits fondamentaux de la personne concernée (art. 16 AP-LPD ; para. 8.1.3.4 du Rapport Explicatif), nécessite d'être clarifiée. En effet, selon l'interprétation proposée de la notion de « risque accru », on ne saurait exclure que cette obligation s'applique largement à l'activité médicale. Il conviendrait dès lors de mieux cerner la notion de « risque accru » de l'art. 16 al. 1 APLPD, afin d'indiquer clairement que les médecins n'ont pas à effectuer une analyse d'impact pour chaque traitement médical entrepris ni en référer au préposé.

* * *

En vous remerciant pour la suite que vous ne manquerez pas de donner à la présente prise de position, nous vous prions de croire, cher Monsieur, à l'expression de nos salutations respectueuses.

Pour la SMSR

Pierre-Alain Schneider
Président

Amstutz Jonas BJ

Von: Jeanneret Danielle <danielle.jeanneret@snf.ch>
Gesendet: Freitag, 31. März 2017 11:59
An: Amstutz Jonas BJ
Betreff: AP révision LPD
Anlagen: Revision-totale-de-la-loi-sur-la-protection-des-donnees_Formulaire-pour-prise-de-position_fr.doc

Bonjour Monsieur Amstutz,

En annexe, vous trouverez la prise de position du Fonds national suisse de la recherche scientifique dans la procédure de consultation sur l'avant-projet de loi fédérale de révision totale de la loi sur la protection des données (LPD) et sur la modification d'autres lois fédérales.

Meilleures salutations
Danielle Jeanneret

_____
Danielle Jeanneret
Juriste

Fonds national suisse (FNS)
Etat-major de direction/service juridique
Wildhainweg 3, Case postale 8232, CH-3001 Berne
Téléphone: +41 31 308 21 84
danielle.jeanneret@snf.ch | www.fns.ch

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Avis donné par

Nom / société / organisation : Fonds national suisse de la recherche scientifique

Abréviation de la société / de l'organisation : FNS

Adresse : Wildhainweg 3, 3001 Berne

Personne de référence : Danielle Jeanneret

Téléphone : 031 308 21 84

Courriel : danielle.jeanneret@snf.ch

Date : 31.03.2017

Remarques importantes :

1. Nous vous prions de ne pas modifier le formatage de ce formulaire !
2. Utilisez une ligne par article, alinéa et lettre ou par chapitre du rapport explicatif.
3. Veuillez faire parvenir votre avis au **format Word** d'ici au 4 avril 2017 à l'adresse suivante : jonas.amstutz@bj.admin.ch

Nous vous remercions de votre collaboration!

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Table des matières

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Remarques générales

nom/société	remarque / suggestion :
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

nom/société	loi	art.	al.	let.	remarque / suggestion :
Fehler! Verweisquelle konnte nicht gefunden werden.FNS	LPD	24	2	e	Dans le projet de loi révisée, le privilège des chercheurs est soumis à une nouvelle condition, que les données soient traitées par des personnes privées (art. 24 al. 2, let. e) ou par un organe fédéral (art. 32 al. 1, let. b). Lorsque des données sensibles sont transmises à des chercheurs privés, elles ne peuvent pas être transmises sous une forme permettant d'identifier les personnes concernées. Cette nouvelle condition implique que, si un tel transfert de données sensibles à des fins de recherche devait entrer en ligne de compte, il faudrait demander le consentement aux

					personnes concernées (une simple information des personnes concernées ne suffirait plus). Ceci restreint le privilège des chercheurs par rapport à la loi actuelle (art. 13, al. 2, let. e et art 22 de la loi actuelle). Cette nouvelle restriction au privilège des chercheurs touche uniquement les données sensibles qui ne sont pas des données médicales (les données médicales bénéficient déjà aujourd'hui d'une protection renforcée en vertu de la loi fédérale relative à la recherche sur l'être humain - LRH ; RS 810.30). Pour la communauté des chercheurs, cette restriction constitue un obstacle. Elle va vraisemblablement occasionner un surcroit de travail de la part du maître du fichier qui devra demander le consentement aux personnes concernées avant de transmettre les données aux chercheurs. Toutefois, le FNS salue le renforcement de la protection des données sensibles transmises à des fins de recherche et la préservation accrue des intérêts des personnes concernées. Le FNS estime que cette protection renforcée correspond à la position éthique de la communauté des chercheurs en général.
Fehler! Verweisquelle konnte nicht gefunden werden.	LPD	32	1	b	Dans le projet de loi révisée, le privilège des chercheurs est soumis à une nouvelle condition, que les données soient traitées par des personnes privées (art. 24 al. 2, let. e) ou par un organe fédéral (art. 32 al. 1, let. b). Lorsque des données sensibles sont transmises à des chercheurs privés, elles ne peuvent pas être transmises sous une forme permettant d'identifier les personnes concernées. Cette nouvelle condition implique que, si un tel transfert de données sensibles à des fins de recherche devait entrer en ligne de compte, il faudrait demander le consentement aux personnes concernées (une simple information des personnes concernées ne suffirait plus). Ceci restreint le privilège des chercheurs par rapport à la loi actuelle (art. 13, al. 2, let. e et art 22 de la loi actuelle). Cette nouvelle restriction au privilège des chercheurs touche uniquement les données sensibles

					qui ne sont pas des données médicales (les données médicales bénéficient déjà aujourd'hui d'une protection renforcée en vertu de la loi fédérale relative à la recherche sur l'être humain - LRH ; RS 810.30). Pour la communauté des chercheurs, cette restriction constitue un obstacle. Elle va vraisemblablement occasionner un surcroit de travail de la part du maître du fichier qui devra demander le consentement aux personnes concernées avant de transmettre les données aux chercheurs. Toutefois, le FNS salue le renforcement de la protection des données sensibles transmises à des fins de recherche et la préservation accrue des intérêts des personnes concernées. Le FNS estime que cette protection renforcée correspond à la position éthique de la communauté des chercheurs en général.
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

nom/société	remarque / suggestion :
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

nom/société	remarque / suggestion :
Fehler! Verweisquelle konnte	

nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Rapport explicatif (excepté chap. 8 « Commentaire des dispositions»)		
nom/société	**chap. n°**	**remarque / suggestion :**
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Rapport explicatif : chap. 8 « Commentaire des dispositions »		
nom/société	**art.**	**remarque / suggestion :**
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

SNV · FSN

Schweizerischer Notarenverband
Fédération Suisse des Notaires
Federazione Svizzera dei Notai
Federaziun Svizra dals Notars

Schwanengasse 5/7
Postfach
3001 Bern

Per E-Mail: jonas.amstutz@bj.admin.ch

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Bern, 4. April 2017

Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz – VERNEHMLASSUNG zum Vorentwurf (VE)

Sehr geehrte Frau Bundesrätin Simonetta Sommaruga
Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Wir danken für die Gelegenheit zur Stellungnahme und unterbreiten Ihnen hiermit die Vernehmlassung des SNV/FSN.

1. Vorbemerkungen

Der SNV konzentriert sich in seiner Vernehmlassung auf die Sicht der praktizierenden Notarinnen und Notare, die im Rahmen ihrer beruflichen Tätigkeit als Geheimnisträger auftreten. Für den SNV ist zentral, dass vorliegende Gesetzesrevision keine impraktikablen Lösungen vorsieht. In Zusammenhang mit dem zentralen Anliegen des SNV, den nachstehenden Ausführungen zu Art. 12 Abs. 3 VE DSG, sei bereits hier erwähnt, dass die Verletzung des Berufsgeheimnisses der Notare als schweres Vergehen nebst strafrechtlichen Konsequenzen in sämtlichen Kantonen disziplinarische Massnahmen nach sich zieht, welche vom blossen Verweis bis zu einem Berufsausübungsverbot reichen.

Telefon 031 326 51 90
Telefax 031 326 51 99
info@schweizernotare.ch

www.schweizernotare.ch
www.notairessuisses.ch
www.notaisvizzeri.ch
www.notarssvizzers.ch

2. Art. 11: Sicherheit von Personendaten

Abs. 1 ergänzen mit "[…] unbefugtes Bearbeiten, *unbefugten Zugriff* oder Verlust geschützt werden."

Begründung: Der unbefugte Datenzugriff durch Dritte ist nicht im Begriff "Datenbearbeitung" enthalten. Dass die Verletzung des Datenschutzes auch den unbefugten Zugriff mitumfasst, kann lediglich aus dem Erläuternden Bericht erschlossen werden; so bspw. aus Ziffer 8.1.3.5.

3. Art. 12: Daten einer verstorbenen Person

Grundsätzlich begrüsst es der SNV sehr, dass diese Gesetzeslücke geschlossen - und der Umgang mit den Daten einer verstorbenen Person im revidierten DSG geregelt werden soll.

Abs. 2 ergänzen mit "[…] eine faktische Lebensgemeinschaft führten, *oder wenn die Person Willensvollstrecker der verstorbenen Person ist.*"

Begründung: Der Erblasser setzt häufig einen Willensvollstrecker zur umfassenden Abwicklung des Nachlasses ein. Der Willensvollstrecker hat die Interessen des Erblassers umfassend zu wahren, welche sich nicht zwingend mit denjenigen der Erbinnen und Erben decken. Dazu gehört unter Umständen auch, dass der Willensvollstrecker in Erfahrung bringt, ob bei einem Verantwortlichen Daten der verstorbenen Person bearbeitet worden sind, ohne dass dies im Auftrag oder mit einer Vollmacht der Erbinnen und Erben geschieht. Die gesetzliche Fiktion, dass gewissen Personen ein schutzwürdiges Interesse an der Frage nach bearbeiteten Personendaten zukommt, ist deshalb auf den Willensvollstrecker auszudehnen.

Abs. 3 ist zu streichen.

Begründung: Der Absatz hebt das Berufsgeheimnis von Anwälten und Notaren integral auf. Jeder Notar (und wohl auch jeder Anwalt) bearbeitet heute Personendaten im Sinne von Art. 3 lit. a VE DSG, beispielsweise im Rahmen einer Adresskartei seiner Klienten. Der Notar führt zudem ein Urschriftenregister.

Nach Meinung der herrschender Lehre sowie des Bundesgerichts ist das Berufsgeheimnis nach dem Tod des Klienten vom Anwalt bzw. Notaren grundsätzlich auch gegenüber den Erben zu beachten. Insbesondere geht auch das Recht zur Entbindung vom Berufsgeheimnis zufolge Höchstpersönlichkeit des Verhältnisses zwischen

Anwalt bzw. Notar und seinem Klienten nicht einfach auf die Erben über (vgl. STRAZZER, *Die anwaltliche Doppel- und Mehrfachvertretung im erbrechtlichen Mandat – einige Streiflichter aus der Praxis,* in successio 2014 S. 113, 119 f. m.w.H.).

Bei den Notarinnen und Notaren kommt erschwerend hinzu, dass das Berufsgeheimnis für die hauptberufliche Tätigkeit des Notars auf kantonaler Ebene geregelt ist und (entgegen der Regelung bei den Anwälten) auch nicht eine schweizweit einheitliche Regelung für die Entbindung vom Berufsgeheimnis bzw. eine Behörde, welche für eine solche Entbindung vom Berufsgeheimnis zuständig wäre, besteht. Vielmehr ist es sogar so, dass viele Kantone keine solche Behörde kennen.

Widerspricht diese Bestimmung bereits heute anerkannten Grundsätzen für den Anwalt betreffend Berufsgeheimnis gegenüber Erbinnen und Erben, ist sie für Notare schlicht nicht handhabbar: sie führt insbesondere in Verbindung mit möglicherweise vorliegenden überwiegenden Interessen gemäss Art. 12 Abs. 1 lit. b VE DSG dazu, dass sich der Notar bei jeder Anfrage von Erbinnen oder Erben potentiell strafbar bzw. disziplinarisch verantwortlich macht, unabhängig davon, ob er die bearbeiteten Daten bekannt gibt oder nicht: Gibt er Daten bekannt, verstösst er eventuell gegen das Berufsgeheimnis und damit gegen geltendes Straf- und Disziplinarrecht; gibt er die Daten nicht bekannt, verstösst er eventuell gegen die Strafbestimmungen von Art. 50 ff. VE DSG.

4. Art. 17: Meldung von Verletzung des Datenschutzes

Abs. 1 ergänzen mit "[…] unbefugte Datenbearbeitung, *Datenzugriff* oder den […]"

Begründung: Vgl. Begründung zu Art. 11, S. 2 hiervor.

Abs. 4 ergänzen mit "Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung, *unbefugten Datenzugriff und über einen Verlust von Daten.*"

Begründung: Damit der Verantwortliche die Pflichten nach den Absätzen 1 und 2 dieses Artikels erfüllen kann, muss er entsprechend informiert werden. Dies erfordert eine analoge Pflicht des Auftragsbearbeiters.

5. Art. 50: Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten

Abs. 3 lit. b ergänzen mit "den Verantwortlichen über eine unbefugte Datenbearbeitung, *unbefugten Zugriff oder Verlust* nach Artikel 17 Absatz 4 zu informieren."

Begründung: Diese Ergänzung ergibt sich aus der vorgeschlagenen Ergänzung zu Art. 17 Abs. 4.

6. Art. 51: Verletzung der Sorgfaltspflichten

Abs. 1 lit. c ergänzen mit "es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung, *unbefugten Zugriff* oder Verlust zu schützen (Art. 11);"

Begründung: Diese Ergänzung ergibt sich aus der vorgeschlagenen Ergänzung zu Art. 11 Abs. 1.

Für Ihre Kenntnisnahme danken wir Ihnen bestens.

Mit freundlichen Grüssen

Für den Schweizerischen Notariatsverband / Fédération Suisse des Notaires
Das Generalsekretariat

Oliver Reinhardt, Notar
Co-Generalsekretär

Christoph Brügger
Co-Generalsekretär

Amstutz Jonas BJ

Von: Urs Glutz <urs.glutz@swisspower.ch>
Gesendet: Dienstag, 4. April 2017 10:17
An: Amstutz Jonas BJ
Betreff: Totalrevision des Datenschutzgesetzes
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de.doc

Sehr geehrter Herr Amstutz

Im Anhang erhalten Sie die Stellungnahme der Swisspower AG zur Totalrevision des Datenschutzgesetzes.

Für die Berücksicht unserer Inputs danken wir Ihnen im Voraus bestens.

Freundliche Grüsse
Urs Glutz

_____

Swisspower AG
Bändliweg 20, Postfach, CH-8048 Zürich
Urs Glutz
Leiter Public Affairs, Mitglied der Geschäftsleitung
Telefon direkt: +41 44 253 82 12
Telefon: +41 44 253 82 11
urs.glutz@swisspower.ch
www.swisspower.ch

Neue Telefonnummer ab 1. Januar 2017

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Swisspower AG

Abkürzung der Firma / Organisation : SPAG

Adresse : Bändliweg 20

Kontaktperson : Urs Glutz

Telefon : 044 253 82 12

E-Mail : urs.glutz@swisspower.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	Swisspower begrüsst die Anpassung des Datenschutzgesetzes an die neuen Gegebenheiten. Wollen aber gleichzeitig auch darauf hinweisen, dass der administrative Aufwand so gering wie möglich zu halten ist.
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden. Swisspower	DSG	8		1+2	Ersatzlos streichen weil das zu einer Komplexität in der Praxis führt. Der EDÖB würde mit solchen Empfehlungen de facto fast Rechtskraft für Verordnungen zugestanden.
Fehler! Verweisquelle konnte nicht gefunden werden. Swisspower	DSG	13	2		Umgehend streichen. Benötigen schon etwas mehr Zeit um zu informieren.
Fehler! Verweisquelle konnte nicht gefunden werden. Swisspower	DSG	13	5		Streichen: so muss die betroffene Person ~~spätestens bei der Speicherung der Daten~~ informiert werden; Wenn Personendaten eingekauft werden und im Betrieb gespeichert werden – soll dann das Unternehmen alle diese Personen via Brief oder Mail angeschrieben werden. Ist eine utopische Bestimmung.
Fehler! Verweisquelle konnte nicht gefunden werden. Swisspower	DSG	18		1+2	Ersatzlos streichen. Zu vage und wenn dieser Artikel streng ausgelegt wird, verursacht er immense Kosten.
Fehler! Verweisquelle konnte nicht gefunden werden. Swisspower	DSG	19	b		Wie der Absatz b in seinem Beschrieb festhält, sind solche Mitteilungen mit unverhältnismässigem Aufwand ausgeschlossen. Wir empfehlen diesen Absatz b ersatzlos zu streichen da er mit grossen Kosten verbunden ist.

Fehler! Verweisquelle konnte nicht gefunden werden. Swisspower	DSG	50 51		1+2+3 2	Swisspower ist für eine gewisse Anpassung aufgrund der EU Kompatibilität. Doch ist die Ausgestaltung des Art. 50 so nicht akzeptabel. Die massive Bussenandrohung schiesst weit über das Ziel hinaus. Es kann nicht sein, dass die Mitarbeiter in diesem Ausmass persönlich haften. Dann kommt noch dazu, dass damit die unpraktikablen Infofomationspflichten (Art. 13 und 15), Meldepflichten (Art. 17), Dokumentationspflichten (Art. 19) mit Bussen belegt werden. Auch die uneinhaltbaren Datensicherheitspflichten (Art. 11), Privacy be Design (Art. 18) sind davon betroffen.
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung

Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		

Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Swiss Retail Federation

Eidgenössisches Justiz- und
Polizeidepartement EJPD
CH-3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

4. April 2017

Vernehmlassung zum neuen Datenschutzrecht: Stellungnahme Swiss Retail Federation

Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Einladung zur Stellungnahme zur geplanten Totalrevision des Datenschutzgesetzes (DSG). Die *Swiss Retail Federation*, nachfolgend Swiss Retail, wahrt und fördert die Interessen der mittelständischen Detailhandelsunternehmen (stationär und online) in der Schweiz. Unter unseren Mitgliedern sind Warenhäuser, Fachmärkte und Fachgeschäfte, Verbraucher- und Abholmärkte, selbstständige Detaillisten, Food-Fachhändler und Kioske. Sie bieten insgesamt rund 40'000 Arbeitsplätze an und weisen einen jährlichen Umsatz von 12 Mia. Franken auf.

Die Mitglieder von Swiss Retail sind von der Revision der aktuellen Datenschutzgesetzgebung in vielfältiger Weise betroffen. Insbesondere im Bereich Kundenbindungs- und Bonusprogramme ist der Schutz von Daten ein sensibles Thema und für den Schweizer Detailhandel von grosser Bedeutung.

Gerne nehmen wir wie folgt Stellung:

- **JA** zu einer grundsätzlichen Revision des Datenschutzgesetzes
- **NEIN zum vorliegenden Vorentwurf. Für den Detailhandel sind folgende Anpassungen notwendig, um die neue Datenschutzgesetzgebung unterstützen zu können:**
  - **Keine Bestimmungen, die über die EU-Regelungen hinausgehen („Swiss Finish") und die Unternehmen unnötig finanziell und administrativ belasten**
  - **Der Nutzen der Daten für den digitalen Fortschritt ist im Interesse der Konsumenten und der Unternehmen zu berücksichtigen und gegenüber dem Persönlichkeitsschutz sorgfältig abzuwägen**
  - **Keine Behinderung von Innovation und Entwicklung neuer Geschäftsmodelle**
  - **Bedarfsgerechte und konsumentenfreundliche Auskunfts- und Informationspflichten**
  - **Berücksichtigung des Prinzips der Selbstregulierung [*Good practice*-Initiativen durch (Branchen-)Verbände]**
  - **Verzicht auf strafrechtliche Sanktionen von Privatpersonen, ausser bei Absicht**

- **JA zur Übernahme der Richtlinie (EU) 2016/680** zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen
- **JA zur Revision des Übereinkommens SEV 108** zum Schutz von Menschen bei der automatischen Verarbeitung personenbezogener Daten

Im Folgenden finden Sie unsere grundsätzlichen Bemerkungen, gefolgt von den wichtigsten Kernanliegen für den Detailhandel. Im beiliegenden Formular finden Sie zudem ergänzend unsere konkreten Anträge und Bemerkungen zum Gesetzestext.

Grundsätzliche Bemerkungen

Swiss Retail begrüsst die Absicht des Bundesrats, das aktuelle Datenschutzgesetz aufgrund der neuen EU-Datenschutzgesetzgebung, welche ab 1. Mai 2018 in Kraft tritt, zu überarbeiten. Den Detailhandels-Unternehmen ist bewusst, dass eine entsprechende Angleichung der Schweizer Gesetzgebung notwendig wird, um weiterhin Daten in einem internationalen Kontext zu bearbeiten und wettbewerbsfähig zu bleiben. Die Totalrevision soll genutzt werden, um auch bestehende Bestimmungen zu hinterfragen und an die technologischen Entwicklungen anzupassen.

Die Detailhandelsbranche steht gegenwärtig unter grossem Druck und befindet sich in einem durch die Digitalisierung angetriebenen Strukturwandel. Das stationäre Geschäft wird zunehmend in den Online-Handel verlagert und die Unternehmen sind darauf angewiesen, neue Geschäftsmodelle und -strategien zu entwickeln, um die teils sinkenden Umsätze aufzufangen. **Die bessere Personalisierung von Angeboten und Angebotsinspiration wird für den Schweizer Detailhandel daher künftig überlebenswichtig sein, insbesondere, um auch im internationalen Konkurrenzkampf bestehen zu können.**

Wir möchten festhalten, dass eine Einschätzung des Vorentwurfs aufgrund der hohen Komplexität der Vorlage insgesamt schwierig ist. Der Vorentwurf lässt zahlreiche Fragen offen und es bleibt unklar, wie sich die Revisionsvorschläge auf die betrieblichen Abläufe und das wirtschaftliche Wohlergehen der betroffenen Unternehmen auswirken würden. Aus dem erläuternden Bericht geht zudem oftmals nicht klar hervor, welche Bestimmungen zwecks EU-Kompatibilität übernommen werden müssen und bei welchen Änderungen es sich um „freiwillige“ Regelungen handelt. Diese Frage ist aus unserer Sicht jedoch zentral.

Grundsätzlich gilt, dass nur revidiert werden soll, was auch wirklich notwendig ist. Die EU-Kompatibilität und die Gleichwertigkeit der Schweizerischen Gesetzgebung sind sicherzustellen, aber ohne überschiessende Tendenzen und ohne einen „Swiss Finish“, der über die EU-Gesetzgebung hinausgeht. Begrüssenswert ist hingegen, dass die Schweiz ihren Handlungsspielraum nutzt, wie es der Bundesrat beispielsweise im Bereich der Datenportabilität gemacht hat.

Aus Sicht des Detailhandels sind die folgenden sieben Kernanliegen zu berücksichtigen und wir beantragen, den Vorentwurf entsprechend zu überarbeiten:

1. **Datenschutz darf kein Innovationhemmnis sein und den Detailhandel als einzelne Branche nicht übermässig belasten:** Ein wichtiges Ziel der neuen Gesetzgebung muss unseres Erachtens darin bestehen, Personendaten ausreichend zu schützen, ohne dabei Innovationen auszubremsen. Der aktuelle Vorentwurf bestätigt leider unser „Gesamtunbehagen“, dass der Persönlichkeitsschutz per se über die Entwicklungsmöglichkeiten der Unternehmen gestellt wird. Persönlichkeitsschutz und Mehraufwände für die Unternehmen (z.B. Aufwände für die einzuholende Information, der Auskunft oder das Einholen einer Einwilligung) müssen jedoch sorgfältig gegeneinander abgewogen und in ein adäquates Verhältnis gestellt werden. Folgeregulierungen, die nachfolgend unter Punkt 2 - 7 einzeln genannt werden, dürfen keine unverhältnismässigen Investitions- und Betriebskosten nach sich ziehen und die Unternehmen nicht unnötig belastet werden.

2. **Melde-, Auskunfts- und Informationspflichten: Verbesserung der allgemeinen und prinzipiellen Information der betroffenen Personen an Stelle einer Überinformation**

Aus Sicht von Swiss Retail wurden die Informations-, Auskunfts-, und Meldepflichten insgesamt zu weitgehend ausgebaut und gehen teilweise deutlich über die EU Datenschutz-Grundverordnung hinaus. Unter anderem muss sofort bei der Speicherung von Daten informiert werden und zur Informationspflicht gehört auch die Identität des Datenbearbeiters – beides sind Punkte, welche die EU Datenschutz-Grundverordnung nicht verlangt. Zudem muss jeder Datenschutzverstoss, sowohl Verletzungen von Sicherheitsbestimmungen, als auch unverhältnismässig genutzte Daten, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragen (EDÖB) gemeldet werden. Die Informationspflichten sind insgesamt schwammig und bringen eine vermehrte Rechtsunsicherheit. Gleichzeitig fallen die vorgesehenen strafrechtlichen Sanktionen streng aus. Das Ziel einer grösseren Transparenz wird unseres Erachtens nicht erreicht, indem die Unternehmen die betroffenen Personen mehr und öfters über die einzelnen Datenbearbeitungsvorgänge informieren. Wie im Detailhandel beispielsweise Erfahrungen mit Produkteinformationen zeigen, kann ein Zuviel an Informationen unter Umständen sogar kontraproduktiv sein und den Konsumenten desensibilisieren, wenn sich dieser von der Informationsflut überfordert fühlt. Aus Angst vor möglichen Sanktionen werden Unternehmen zudem lieber ein Zuviel an Informationen liefern. **Eine risikobasierte Transparenzpflicht und eine allgemeine Information der betroffenen Personen über die Folgen einer Datenpreisgabe ist unseres Erachtens weitaus zielführender. Die geplanten Meldepflichten gegenüber dem EDÖB sind wirtschaftsfreundlich und pragmatisch auszugestalten.**

Aus Sicht der Detailhandelsbranche sind entsprechend insbesondere nachfolgende Punkte zu berücksichtigen:

- **Keine Bekanntgabe von Identität und Kontaktdaten der Auftragsdatenbearbeiter, keine Informationspflicht bei indirekter Datenbeschaffung:** Art. 13 VE-DSG sieht eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister oder Kartenakzeptanzdienstleister) vor. Die Kontaktdaten der Auftragsdatenbearbeiter sollen offengelegt werden. Diese Zusatzbestimmungen sind zu streichen, denn sie gehen unseres Erachtens klar über das EU-Recht hinaus und sind weder sinnvoll noch erforderlich. In der Praxis ist es für Unternehmen damit praktisch unmöglich, Daten bei Dritten zu beschaffen, da diesen die relevanten Eckwerte (z.B. erstmalige Speicherung) oftmals gar nicht bekannt sind. Im Detailhandel werden Kundendaten häufig durch Kartenakzeptanzdienstleister oder andere Dienstleister bearbeitet. Für die Unternehmen bedeutet es insgesamt ein grosser Mehraufwand und greift zudem in berechtigte eigene Datenschutzinteressen und die Geschäftsgeheimnisse ein. Für die Kunden führt eine solche Regelung wiederum zu einer Informationsflut ohne erkennbaren Mehrwert. Die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben ist zudem bereits in Art. 7 VE-DSG geregelt.

- **Zusätzliche Massnahmen gegen missbräuchliche Auskunftsbegehren:** Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EU-DSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht generell bei Entscheidungen, die auf einer Datenbearbeitung basieren. Die kostenlose Auskunftspflicht kann zu Fehlanreizen und zu einem unverhältnismässigen Mehraufwand für die Unternehmen führen. Im neue Datenschutzgesetz sind daher Mechanismen vorzusehen, um die Unternehmen vor offensichtlich nicht datenschutzrelevanten Auskunftsbegehren zu schützen.

- **Warte- und Antwortfristen dürfen die Handlungsfähigkeit der Unternehmen nicht einschränken:** Der Bearbeitungsaufwand der Meldungen seitens der Behörde ist bereits heute gross und wird in Zukunft dank den ausgebauten Pflichten erneut zunehmen. Für Swiss Retail ist entscheidend, dass die Warte- und Antwortfristen – beispielsweise bei den unter Punkt 4

genannten Datenschutz-Folgeabschätzungen – sich auf ein sinnvolles Mass beschränken, damit die Unternehmen weiterhin handlungsfähig bleiben.

- **Keine übermässige Dokumentations- und Meldepflicht für die Unternehmen**: Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht beispielsweise für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung. Diese besagt, dass *gewisse* Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen. Insgesamt ist klar zu regeln, welche Informationen weitergegeben werden müssen. Die Dokumentations- und Meldepflichten sollen sich nach dem Prinzip der Verhältnismässigkeit richten.

3. **„Profiling" ist als Erweiterung des bestehenden „Persönlichkeitsprofils" zu sehen:** Die unternommenen Anstrengungen für die Einwilligung zur Erstellung und Bearbeitung von Persönlichkeitsprofilen müssen unseres Erachtens zwingend ihre Gültigkeit behalten, auch wenn die Begrifflichkeit zu Profiling geändert wird (Vgl. Art. 4, Abs. 6. VE-DSG). In den Übergangsbestimmungen ist entsprechend klar zu regeln, dass eine „ausdrückliche Einwilligung" nur für ein neues Profiling gilt und für bereits eingeholte Daten nicht erneut das Einverständnis der betroffenen Personen eingeholt werden muss. In den bestehenden Bonus- und Kundenbindungsprogrammen unserer Mitglieder wird bei Neuanträgen beispielsweise in den Allgemeinen Geschäftsbedingungen das explizite Einverständnis der Kundinnen und Kunden für die Erstellung und Bearbeitung von Persönlichkeitsprofilen eingeholt. Ein erneutes Einholen des Einverständnisses gemäss neuem DSG wäre für all diese „alten Anträge" ein grosser Mehraufwand für die Unternehmen und würde die Weiterführung der bestehenden Bonusprogramme gefährden.
   Aus unserer Sicht unabdingbar ist, dass unter einer „ausdrücklichen Einwilligung" auch in Zukunft nicht nur ein aktives mündlich oder schriftliches Einverständnis zur Datenverarbeitung zu verstehen, sondern auch ein konklusives bejahendes Verhalten (bspw. im Rahmen von AGBs, wo betr. der Datenverarbeitung zwar nicht alleine und explizit ein Verständnis gegeben wird, aber implizit, mit Annahme der AGB).

4. **Massvolle Umsetzung der Datenschutz-Folgenabschätzung:** Das in Art. 16 VE-DSG neu eingeführte Instrument der Datenschutz-Folgeabschätzung ist aus Sicht von Swiss Retail zu weit gefasst und auf ein sinnvolles Mass zu beschränken. Die offene und unklare Formulierung führt dazu, dass in der Praxis für alle Datenbearbeitungen vorgängig aufwendige Abklärungen durchgeführt werden müssten. Verstösse würden sanktioniert, was in den Unternehmen zu einer übervorsichtigen Haltung führen und sich innovationshemmend auswirken würde. Die Datenschutz-Folgeabschätzungen und die entsprechende Informationspflicht an den EDÖB sind analog der europäischen EU-DSGVO auf Fälle zu beschränken, bei denen ein «hohes Risiko» und das Risiko einer klaren Persönlichkeitsverletzung besteht. Zudem ist die vorgesehene Reaktionszeit des EDÖB von drei Monaten auf einen Monat zu reduzieren, damit die Handlungsfähigkeit der Unternehmen gewährleistet bleibt. Der Auftragsdatenbearbeiter ist von der Datenschutz-Folgenabschätzungspflicht auszunehmen, da dieser nicht über die notwendigen Angaben verfügt.

5. **Gewährleistung Rechtssicherheit:** Durch die risikobasierte, prinzipienorientierte Ausgestaltung des neuen DSG entstehen vermehrt Interpretationsspielräume und Unklarheiten. Diverse entscheidende Aspekte müssen zudem erst noch auf dem Verordnungsweg präzisiert werden. Swiss Retail fordert, dass der Gesetzgeber bei der Umsetzung (beispielsweise der „Good Practices" durch den EDÖB) auf eine klare Linie achtet. Der Vorentwurf ist auch in Bezug auf eine präzise und einheitliche Terminologie zu überarbeiten, wie beispielsweise eine klare Differenzierung zwischen „Beschaffung" und „Bearbeitung", sowie der Begriffe „Dritte" und „Empfängerinnen und Empfänger".

6. **Sanktionssystem mit Augenmass: keine strafrechtliche Sanktionierung von Privatpersonen bei Fahrlässigkeit, sondern nur bei Absicht:** Swiss Retail lehnt das im Vorentwurf skizzierte Sanktionssystem ab. Die strafrechtlichen Sanktionen wurden im Vorentwurf insgesamt zu stark ausgebaut und fokussieren auf die mit dem Datenschutz betrauten Mitarbeitenden als Privatpersonen, anstatt auf die Unternehmen. Die geplanten Strafverschärfungen (Bussen bis 500'000.-, Freiheitsentzug bis zu 3 Jahre bei Zuwiderhandlungen) schiessen über das Ziel hinaus. Auch die vorgesehene Möglichkeit, Mitarbeitende bereits bei fahrlässigem Handeln zu bestrafen, sind nicht zielführend und untergraben den risikobasierten Ansatz, den die Revision eigentlich verfolgt. Im Detailhandel werden schützenswerte Personendaten heute zumeist in den CRM-Abteilungen von Unternehmen und vermehrt mittels automatisierter Bearbeitungsprozesse bearbeitet. Neben einer allgemeinen Kultur des gegenseitigen Denunzierens würde es zunehmend unmöglich, qualifiziertes Personal zu finden, das sich dem Risiko einer persönlichen Strafbarkeit aussetzt. Die Folge wäre ein sukzessiver Qualitätsabfall im Bereich der Datenbearbeitung.

7. **Selbstregulierung und „Empfehlungen der guten Praxis“:** Swiss Retail fordert eine konsequente Umsetzung des Selbstregulierungsprinzips. Die Initiative für die in Art. 8 VE-DSG skizzierten „Empfehlungen der guten Praxis“ soll von den (Branchen-)Verbänden und nicht vom EDÖB ausgehen. Das garantiert sachgerechte Lösungen, die von Experten mit einem starken Bezug zur Praxis ausgearbeitet und von den Unternehmen auch umgesetzt werden können. Auch unter der EU-DSGVO ist die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen. Dem EDÖB ist ein Mitwirkungsrecht einzuräumen. Die „Empfehlungen der guten Praxis“ sollen freiwillig bleiben, das heisst die Unternehmen halten das auch Gesetz ein, wenn sie an Stelle der Empfehlungen eigene, datenschutzkonforme Lösungen umsetzen.

Swiss Retail lehnt die Totalrevision des DSG in der vorliegenden Form, wie sie in die Vernehmlassung geschickt worden ist, ab. Die Revision enthält zahlreiche Informations- und Handlungspflichten, von welchen der Detailhandel überproportional negativ betroffen wäre. Dies hätte zur Folge, dass die Kosten im Detailhandel zusätzlich steigen und die Unternehmen belasten. Die anfallenden Kosten würden nicht zuletzt indirekt an die Konsumentinnen und Konsumenten überwälzt, was nicht der Sinn der Revision sein kann.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und einer entsprechenden Überarbeitung des Vorentwurfs. Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Dagmar Jenni
Geschäftsführerin

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Swiss Retail Federation

Abkürzung der Firma / Organisation : SRF

Adresse : Bahnhofplatz 1, 3011 Bern

Kontaktperson : Sarah Frey

Telefon : 031 312 40 40

E-Mail : sarah.frey@swiss-retail.ch

Datum : 4.4. 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SRF	**Vorbemerkung: Wir verweisen auf unsere ausformulierte Stellungnahme, welche die wichtigsten Grundsätze und Änderungsanliegen aus Sicht des Detailhandels enthält.**

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SRF	VE-DSG	3		lit. 3	**Antrag:** *Profiling: jede automatisierte Auswertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;* **Begründung:** Die Definition von Profiling geht weit über das EU-Recht hinaus und soll entsprechend der EU-DSGVO angepasst werden. Profilig ist als eine Erweiterung des bestehenden Persönlichkeitprofils gemäss geltendem DSG zu verstehen und die Einführung der neuen Begrifflichkeit darf auf keinen Fall dazu führen, dass Unternehmen keine Auswertungen oder Prognosen mehr machen können. Für den Detailhandel ist die Personalisierung von Angeboten existenziell, um künftig im internationalen Konkurrenzkampf bestehen zu können. Der «Profiling»-Begriff ist in dieser Form noch zu unbestimmt und bringt Rechtsunsicherheit, die Formulierung "um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen" soll in der Folge-Regulierung entsprechend eng eingegrenzt und konkretisiert werden.
SRF	VE-DSG	4	3		**Antrag:** *Personendaten dürfen nur zu einem bestimmten und für die betroffene Person ~~klar~~ erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.* **Begründung:** Der Begriff "klar" ist ambivalent und daher zu streichen. Die Formulierung schafft Rechtsunsicherheit, da nicht ersichtlich ist, was für die betroffene Person ein «klar» erkennbarer Beschaffungszweck ist und welche Voraussetzungen für diese Klarheit gelten.

SRF	VE-DSG	4	4		**Antrag:** Bestimmung ist ersatzlos zu streichen. **Begründung:** Die hier aufgeführte Bestimmung würde eine Pflicht zur Löschung beinhalten in dem Moment, wo der Zweck der Bearbeitung nicht mehr gegeben ist. Diese Forderung ist unklar und würde einen grossen administrativen Aufwand bedingen.
SRF	VE-DSG	4	5		**Antrag:** Übernahme Wording gemäss Art. 5 Abs. 1 des geltenden DSG. Begründung: Das geltende DSG gemäss Art. 5 Abs. 1 ist klarer. Unternehmen haben per se einen betriebswirtschaftlichen Anreiz, möglichst wahrheitsgetreue Daten zu verwenden und kein Interesse, veraltete oder falsche Daten zu bearbeiten, da dies das Ergebnis der Bearbeitung verfälschen oder gar unbrauchbar machen kann.
SRF	VE-DSG	4	6		**Antrag 1:** *Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen.* **Begründung 1:** Das Erfordernis der Einwilligung ist ein «Swiss Finish» und geht über die EU-Regelung hinaus. Eine Einwilligung soll sich nur auf die besonders schützenswerten Personendaten beziehen und nicht auf das Profiling, denn letzteres ist zu weit gefasst und unklar. Dies würde dazu führen, dass Kundinnen und Kunden für jeden noch so unbedeutenden Bearbeitungsvorgang ihre Zustimmung geben müssten und folglich von Informationen überflutet würden. Ausserdem sind folgende Punkte zu beachten: - Grundsätzlich muss die Einholung der Einwilligung einmalig und in Form einer allgemeinen Information (z.B. durch Zustimmung zu den AGB via Opt-in Kästchen) möglich sein. Dies ist auf Verordnungsebene zu gewährleisten. Wenn die Unternehmen wiederholt eine (ausdrücklichen)

					Einwilligung der betroffenen Personen einholen müssen, bedeutet das für sie einen grossen Mehraufwand und verbessert die Transparenz für die Konsumentinnen und Konsumenten nicht. - Für bereits eingeholte Daten soll keine erneute Einwilligung der betroffenen Person eingeholt werden müssen. - Im Detailhandel sind grosse Teile der bestehenden Bonusprogramme noch nicht web-basiert, das heisst das Einholen der Einwilligung zu einer AGB-Änderung ist beispielsweise bei einer Kundenprogrammkarte massiv teurer als bei einem Social-Media-Account. Die im VE-DSG vorgeschlagene Bestimmung diskriminiert daher den Detailhandel als einzelnen Wirtschaftszweig. - Unter einer «ausdrücklichen» Einwilligung soll zudem auch künftig nicht nur ein aktives mündlich oder schriftliches Einverständnis zur Datenverarbeitung zu verstehen sein, sondern auch ein bejahendes Verhalten wie bspw. eine Annahme der allgemeinen AGB.
SRF	VE-DSG	5	5		**Antrag:** *Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens dreissig Tage ~~sechs Monate~~ nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht.* **Begründung:** Die Frist von sechs Monaten macht ein Genehmigungsverfahren nicht praktikabel und würde zu unzumutbaren Verzögerungen bei Auslandtransfers führen. Die Unternehmen würden handlungsunfähig, zumal sich die Frist infolge Nachforderung von Informationen durch den EDÖB noch beliebig verlängern kann. Eine Frist von dreissig Tagen gemäss geltendem DSG ist ausreichend.
SRF	VE-DSG	5	6		**Antrag:**

					Bestimmung ist ersatzlos zu streichen. **Begründung:** Die Pflicht zur Information des EDÖB geht über die Anforderungen der EU-DSGVO hinaus. Sie bedeutet eine nicht akzeptable Mehrbelastung für alle Unternehmen, ohne dass der Datenschutz gestärkt würde. Es ist zudem fraglich, ob der EDÖB die Flut der Meldungen inhaltlich und innert nützlicher Frist bewältigen könnte.
SRF	VE-DSG	6	1	a	**Antrag:** *In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:* *a. die betroffene Person ~~im Einzelfall~~ eingewilligt hat;* *b. ..* **Begründung:** Die Einzelfallbetrachtung führt in der Praxis zu Unklarheiten da meistens die Einwilligung für einen Zweck eingeholt wird und nicht für eine einzelne Übermittlung von Personendaten. Wenn also ein Unternehmen Daten ins Ausland bekannt gibt, soll es hierfür im Voraus und in allgemeiner Weise die Einwilligung einholen können (vgl. Antrag zu Art. 4, Abs. 6)
SRF	VE-DSG	6	2		**Antrag:** Bestimmung ist ersatzlos zu streichen**.** **Begründung:** Die Meldepflicht an den EDÖB trotz Ausnahmetatbestand zu informieren, ist unverhältnismässig und geht über die Anforderungen der EU-DSGVO hinaus. Sie bedeutet eine nicht akzeptable Mehrbelastung für alle Unternehmen, ohne dass der Datenschutz gestärkt würde. Es ist zudem fraglich, ob der EDÖB die Flut der Meldungen inhaltlich und innert nützlicher Frist bewältigen könnte.

SRF	VE-DSG	7	2		**Antrag:** *Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit ~~und die Rechte der betroffenen Person~~ zu gewährleisten. ~~Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters.~~* **Begründung:** Es ist unklar, um welche Rechte es hier geht und welche Pflichten dem Auftragsbearbeiter übertragen werden sollen. In der Praxis ist es nicht umsetzbar, dass der Auftragsbearbeiter sämtliche Rechte der betroffenen Person gewährleisten kann. Die Kompetenz des Bundesrates, die «weiteren Pflichten» des Auftragsbearbeiters präzisieren zu können, ist ersatzlos zu streichen.
SRF	VE-DSG	8			**Antrag:** Bestimmung ist zu streichen und entsprechend der untenstehenden Begründung zu überarbeiten. **Begründung:** Swiss Retail fordert eine konsequente Umsetzung des Selbstregulierungsprinzips. Die Initiative für «Empfehlungen der guten Praxis» soll von den (Branchen-)Verbänden und nicht vom EDÖB ausgehen. Das garantiert sachgerechte Lösungen, die von den Unternehmen umgesetzt werden können. Die Experten aus der Branchen haben im Gegensatz zum EDÖB einen starken Bezug zur Praxis. Die Empfehlungen sollen freiwillig bleiben, das heisst die Unternehmen verhalten sich auch gesetzeskonform, wenn sie an Stelle der «Empfehlungen der guten Praxis» ihre eigenen Lösungen umsetzen. Dem EDÖB ist ein Mitwirkungsrecht einzuräumen.
SRF	VE-DSG	9			**Antrag:** Artikel ist zu streichen als Folge von Art. 8 (vgl. oben).

SRF	VE-DSG	11	2		**Antrag:** Bestimmung ist ersatzlos zu streichen**.** **Begründung:** Der Bundesrat soll keine Bestimmungen über die Mindestanforderungen an die Datensicherheit erlassen können. Auf übermässige Regulierungen ist zu verzichten.
SRF	VE-DSG	13	1-4		**Antrag:** Artikel ist zu streichen und grundlegend zu überarbeiten. **Bemerkung:** Die Informationspflicht wird gemäss VE-DSG auf sämtliche Personendaten ausgeweitet, was zu einem erheblichen Mehraufwand für die Unternehmen führen und in berechtigte eigene Datenschutzinteressen und die Geschäftsgeheimnisse eingreifen würde. Für die Kunden führt eine solche Regelung wiederum zu einer Informationsflut ohne erkennbaren Mehrwert. Die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben ist zudem bereits in Art. 7 VE-DSG geregelt. Der Artikel ist insgesamt unpräzise formuliert und es ist unklar, welche Beschaffungsvorgänge von der Informationspflicht betroffen sind, z.B. was mit bisherigen bzw. früher bearbeiteten Daten geschehen soll. Für Swiss Retail ist zwingend festzuhalten, dass für bereits eingeholte Daten nicht eine erneute Informationspflicht besteht. Eine solche Bestimmung würde beispielsweise die bestehenden Kundenbonusprogramme gefährden. Nicht jede einzelne Datenbeschaffung darf zudem automatisch eine Informationspflicht auslösen, eine solche ist nur bei der Beschaffung von besonders schützenswerten Personendaten angezeigt. Art. 13 VE-DSG sieht in lit. 3, 4 und 5 eine Pflicht zur detaillierten Information der betroffenen Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister oder Kartenakzeptanzdienstleister) vor. Die Kontaktdaten der Auftragsdatenbearbeiter sollen offengelegt werden. Diese Zusatzbestimmungen sind gänzlich zu streichen, denn sie gehen klar über das EU-Recht hinaus. In der Praxis wäre es damit für Unternehmen praktisch unmöglich, Daten bei Dritten zu beschaffen,

					da diesen die relevanten Eckwerte (z.B. erstmalige Speicherung der Daten) oftmals gar nicht bekannt sind.
SRF	VE-DSG	15	1-3		**Antrag:** Bestimmung ersatzlos zu streichen. **Begründung:** Hier enthält der VE-DSG einen weiteren abzulehnenden «Swiss Finish», der über die Bestimmungen der EU hinausgeht. Die Voraussetzung für eine Information soll sich auf erhebliche Auswirkungen beschränken, so wie dies in der EU auch der Fall ist. Die Formulierung der «Auswirkungen» ist so breit gefasst, dass jeder kommerzielle Entscheid (z.B. eine Warenlieferung gegen Rechnung) darunterfallen kann. Die Bedeutung von automatisierten Einzelentscheidungen wird in Zukunft weiter zunehmen. Es darf diesbezüglich keine gesetzlichen Vorschriften geben, welche die Kosten aller automatisierten Vorgänge schon im Voraus stark erhöhen. Unternehmen, die automatische Bearbeitungsvorgänge implementieren, müssen die Sicherheit haben, dass die entsprechende persönliche Auskunftspflicht nicht in jedem Bagatell-Fall erfüllt werden muss, sondern nur in datenschutzrechtlichen Fällen.
SRF	VE-DSG	16	1		**Antrag:** Bestimmung ist zu streichen und grundsätzlich zu überarbeiten. **Begründung:** Das hier eingeführte Instrument der Datenschutz-Folgeabschätzung ist aus Sicht von Swiss Retail insgesamt zu weit gefasst und auf ein sinnvolles Mass zu beschränken. Die offene und unklare Formulierung führt dazu, dass in der Praxis für alle Datenbearbeitungen vorgängig aufwendige Abklärungen durchgeführt werden müssten. Verstösse würden sanktioniert, was in den Unternehmen zu einer übervorsichtigen Haltung führen und sich innovationshemmend auswirken würde. Die Datenschutz-Folgeabschätzungen und die entsprechende Informationspflicht an den EDÖB sind analog der europäischen EU-DSGVO auf Fälle zu beschränken, bei denen ein «hohes Risiko» und das Risiko einer klaren Persönlichkeitsverletzung besteht. Der Auftragsdatenbearbeiter ist von der Datenschutz-Folgenabschätzungspflicht auszunehmen, da dieser nicht über die notwendigen Angaben verfügt.

SRF	VE-DSG	16	3-4		**Antrag:** Beide Bestimmungen sind ersatzlos zu streichen. **Begründung:** Beide Bestimmungen gehen über die Regelungen des EU-Rechts hinaus und führen zu einem hohen Mehraufwand mit einem geringen Mehrwert für die Konsumentinnen und Konsumenten. Die Frist von drei Monaten zur Erhebung von Einwänden kann zudem eine unnötige Verzögerung bei Einführung neuer Geschäftsmodelle bewirken.
SRF	VE-DSG	17			**Antrag:** Bestimmung ist grundlegend zu überarbeiten. **Begründung:** Dieser Artikel geht erneut über die EU-DSGVO hinaus. Der Passus zur Selbstanzeige für den Fall, dass der Verantwortliche Daten verliert oder eine unbefugte Datenverarbeitung vornimmt, ist ersatzlos zu streichen. Die EU-DSGVO sieht eine Selbstanzeige nur dann vor, wenn Schutzmassnahmen versagt haben und darauf tatsächlich ein Sicherheitsrisiko entsteht. Die Folge dieser unklar formulierten Bestimmung wäre eine Flut von Selbstanzeigen und eine Kultur des gegenseitigen Denunzierens innerhalb der betroffenen Unternehmen.
SRF	VE-DSG	18	1-2		**Antrag:** Bestimmung ist ersatzlos zu streichen. **Begründung:** Die in Art. 18 aufgeführten Forderungen nach angemessenen Massnahmen und geeigneten Voreinstellungen zur Vorbeugung von Datenschutzverletzungen ist bereits durch die Prinzipien der Richtigkeit, Verhältnismässigkeit und Zweckbindung abgedeckt und können deshalb ersatzlos gestrichen werden.

SRF	VE-DSG	19		a,b	**Antrag:** Bestimmung ist zu streichen und zu überarbeiten. **Begründung:** Die «weiteren Pflichten», die «Datenbearbeitung zu dokumentieren» und «die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung, oder Vernichtung von Daten, über Verletzung des Datenschutzes.... zu informieren» sind in der Praxis nicht oder nur mit unverhältnismässigem Aufwand umsetzbar, sondern ergeben auch gegenüber dem Betroffenen keinen Sinn, da ständig Korrekturen, Löschungen, etc. vorgenommen werden und der Empfänger mit Mitteilungen geflutet werden könnte. Besonders die Informationspflicht gemäss lit. b. ist nicht umsetzbar. Der Passus schafft vor allem Rechtsunsicherheit und könnte Millionen von unnötigen Mitteilungen auslösen. Der Nutzen einer solchen Regelung ist völlig unklar. Art. 19 VE DSG ist deshalb ersatzlos zu streichen.
SRF	VE-DSG	20			**Antrag:** Bestimmung ist ersatzlos zu streichen. **Begründung:** Die hier neu eingeführte Pflicht zur Begründung jeglicher Entscheide und nicht nur bei automatisierten Einzelentscheidungen, greift massiv in die Freiheit eines Unternehmens ein und geht über die Erfordernisse der EU-DSGVO hinaus, was wir klar ablehnen. Eine kostenlose Auskunftspflicht kann zudem zu Fehlanreizen führen. Es fehlt zudem eine wirksame Klausel, welche die Unternehmen vor offensichtlich nicht datenschutzrelevanten Auskunftsbegehren schützt.
SRF	VE-DSG				
SRF	VE-DSG	23	2	d	**Antrag:** Bestimmung ersatzlos streichen.

					Begründung: Das Erfordernis der Einwilligung zu einem Profiling geht über die EU-Regelung hinaus und ist deshalb zu streichen.
SR	VE-DSG	50-53			**Antrag:** Art. 50, 51, 52 und 53 zu den Strafbestimmungen sind in der vorliegenden Form zu streichen. **Begründung:** Swiss Retail lehnt das im Vorentwurf skizzierte Sanktionssystem ab und fordert eine Lösung mit deutlich mehr Augenmass. Die strafrechtlichen Sanktionen wurden insgesamt zu stark ausgebaut und fokussieren auf die mit dem Datenschutz betrauten Mitarbeitenden als Privatpersonen, anstatt auf die Unternehmen. Die geplanten Strafverschärfungen (Bussen bis 500'000.-, Freiheitsentzug bis zu 3 Jahre bei Zuwiderhandlungen) schiessen über das Ziel hinaus. Auch die vorgesehene Möglichkeit, Mitarbeitende bereits bei fahrlässigem Handeln zu bestrafen, sind nicht zielführend und untergraben den risikobasierten Ansatz, den die Revision eigentlich verfolgt. Eine strafrechtliche Sanktionierung von Privatpersonen soll nur bei Absicht, nicht jedoch bei Fahrlässigkeit erfolgen. Im Detailhandel werden schützenswerte Personendaten heute zumeist in den CRM-Abteilungen von Unternehmen und vermehrt mittels automatisierter Bearbeitungsprozesse bearbeitet. Gesetzlich gewollte Spielräume bei der Datenbearbeitung würden aus Angst vor persönlicher Bestrafung nicht ausgeschöpft. Neben einer allgemeinen Kultur des gegenseitigen Denunzierens würde es zunehmend unmöglich, qualifiziertes Personal zu finden, das sich dem Risiko einer persönlichen Strafbarkeit aussetzt. Die Folge wäre ein sukzessiver Qualitätsabfall im Bereich der Datenbearbeitung, was nicht das Ziel der vorliegenden Revision sein kann.
SRF	VE-DSG	55			**Antrag:** Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109)
SRF	VE-DSG	59			**Antrag:** Es ist eine generelle Übergangsfrist von zwei Jahren zu gewähren und diese Frist ist nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken. Dies entspricht auch den

					Regelungen der EU-DSGVO.

SRG SSR

www.srgssr.ch Schweizerische Radio- und Fernsehgesellschaft
Société suisse de radiodiffusion et télévision
Società svizzera di radiotelevisione
Societad svizra da radio e televisiun

jonas.amstutz@bj.admin.ch

Generaldirektion
Generaldirektor
Giacomettistrasse 1
3000 Bern 31
Telefon +41 31 350 91 11

E-Mail roger.deweck@srgssr.ch
Direktwahl +41 31 350 92 41
Fax +41 31 350 97 09
Datum 4. April 2017

Stellungahme der SRG SSR zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Die Schweizerische Radio- und Fernsehgesellschaft bedankt sich für die Möglichkeit zur Stellungnahme zum Vorentwurf des Datenschutzgesetzes (VE-DSG).

1. Einleitende Bemerkungen

Die SRG ist als Schweizer Medienunternehmen im Dienste der Öffentlichkeit in langer Tradition dem Persönlichkeitsschutz verpflichtet. Dementsprechend nimmt die SRG Datenschutzaspekte ihrer Nutzerinnen und Nutzer, ihrer Mitarbeitenden und anderer von Datenbearbeitungen betroffenen Personen sehr ernst. Die SRG unterstützt folglich Anpassungen des aktuellen Datenschutzgesetzes (DSG), soweit diese aufgrund technischer Entwicklungen sowie aufgrund internationaler Abmachungen zwingend erforderlich sind, und angemessene Bedürfnisse von betroffenen Personen schützen. Evident erscheint diesbezüglich der Bedarf für Anpassungen, die zur Ratifizierung des Protokolls zur Revision des Übereinkommens SEV 108 des Europarates erforderlich sind. Damit wäre auch weiterhin der Angemessenheitsbeschluss der Europäischen Kommission sichergestellt.

Soweit sich der VE-DSG an die EU-DSGVO anlehnt, sind Anpassungen abzulehnen, die über die EU-DSGVO hinausgehen („Swiss Finish“). Ebenso abzulehnen sind Neuerungen und Vorschriften, die nur mit unverhältnismässigem Aufwand umsetzbar sind, sowie ausufernde Sanktionen zulasten natürlicher Personen. Im Vergleich zur EU-DSGVO strengere Regeln für Schweizer Unternehmen sowie die Androhung drakonischer Sanktionen gegenüber ihren Mitarbeitenden bergen die Gefahr unnötiger Zurückhaltung der Unternehmen aus

Angst vor Strafen und von Wettbewerbsnachteilen. Dies stünde letztlich auch im Widerspruch zur bundesrätlichen Strategie „Digitale Schweiz“.

Um Rechtsunsicherheit zu vermeiden, müssen Neuerungen klar formuliert sein und allfällige Missverständnisse ausgeräumt werden. Dies gilt insbesondere im Zusammenhang mit der vom historischen Gesetzgeber vorgesehenen und im VE-DSG übernommenen Sonderstellung der Medien. Jede Unklarheit beinhaltet hier das Risiko, dass sie zur Beeinflussung der redaktionellen Tätigkeiten missbraucht wird. Unklare Regelungen für Medienunternehmen gefährden mit anderen Worten die Erfüllung des Informationsauftrags.

Die SRG konzentriert sich in ihrer Stellungnahme auf einzelne Aspekte des Vorentwurfs, welche für das Unternehmen SRG besonders relevant erscheinen. Für die übrigen Punkte kann sich die SRG der Stellungnahme des Vereins Unternehmens-Datenschutz VUD anschliessen.

2. Bemerkungen zu medienspezifischen Bestimmungen

2.1. Zum Medienprivileg

Der VE-DSG enthält in Art. 22 eine zum aktuellen Art. 10 DSG analoge Bestimmung über die „Einschränkung des Auskunftsrechts für Medienschaffende“. Zudem sieht Art. 24 Abs. 2 lit. d VE-DSG einen Art. 13. Abs. 2 lit. d DSG entsprechenden Rechtfertigungsgrund für Medienschaffende vor. Damit übernimmt der VE-DSG das sog. Medienprivileg aus dem aktuellen Recht.

Der Erläuternde Bericht hält in Ziff. 8.1.4.3 im Zusammenhang mit dem Auskunftsrecht fest, dass das sogenannte Medienprivileg „keine materiellen Änderungen“ erfahren soll. Diese Klarstellung und Bestätigung ist zu begrüssen. Sie gilt auch für den Rechtfertigungsgrund gemäss Art. 24 Abs. 2 lit. d VE-DSG. Allerdings besteht ein gewisses Risiko Relativierung des Medienprivilegs in der Praxis. In Art. 24 VE-DSG wurde in Bezug auf alle aufgezählten Rechtfertigungsgründe das Wort „möglicherweise“ hinzugefügt. Es bezieht sich damit auch auf den Rechtfertigungsgrund für die journalistischen Datenbearbeitungen. Diese Änderung ist generell nicht erforderlich. Sie stiftet vielmehr Verwirrung und Rechtsunsicherheit und gefährdet dadurch auch die journalistische Arbeit der Medienunternehmen. Das Wort „möglicherweise“ ist folglich ersatzlos zu streichen.

2.2. Zu den Folgen des Medienprivilegs auf andere Bestimmungen

Die SRG geht davon aus, dass die Bestimmungen des Vorentwurfes auf redaktionelle Datenbearbeitungen im Medienunternehmen nicht anwendbar sind, wenn Art. 22 („Medienprivileg“) greift. Das heisst mit anderen Worten, dass insbesondere die Anwendung folgender Bestimmungen eingeschränkt ist, wenn sie

Aufschluss über Informationsquellen geben, Einsicht in Entwürfe für Publikationen erlauben oder die freie Meinungsbildung des Publikums gefährden würde[1]:

- Art. 4 Abs. 5 VE-DSG: Nachführungs- und Ergänzungspflicht,
- Art. 4 Abs. 6 a. E / Art 15: in Bezug auf Profiling
- Art. 12 VE-DSG: Daten einer verstorbenen Person
- Art. 13 VE-DSG: Informationspflicht bei der Beschaffung
- Art. 16 VE-DSG Datenschutzfolgeabschätzung
- Art. 17 VE-DSG: Data Breach Notification
- Art. 19 lit. b VE-DSG Dokumentationspflicht
- Art. 25 Abs. 1 lit. c VE-DSG: Recht auf Löschung- und Vernichtung
- Art. 25 Abs. 2 VE-DSG: Recht auf Bestreitungsvermerk
- Art. 41 ff. Untersuchungshandlungen des EDÖB.

2.3. Zur ausschliesslichen Anwendbarkeit von Art. 28 ff. ZGB auf redaktionelle Publikationen periodisch erscheinender Medien

Zusätzlich zu Ziff. 2.2 ist im Rahmen der Revision zudem explizit festzuhalten, dass das DSG auf redaktionelle Medienpublikationen keine Anwendung findet. Dies lässt sich heute klar aus den Materialien zum heutigen DSG ableiten[2], wird aber im VE-DSG bzw. in den Erläuterungen nicht mehr erwähnt. Dieses Schweigen soll aber nicht als Abweichung vom Prinzip des historischen Gesetzgebers interpretiert werden können.

So weist etwa Rosenthal am Beispiel von Zeitungsartikeln zu Recht auf die absurden Auswirkungen von Instrumenten des VE-DSG hin, wenn sie auf redaktionelle Publikationen Anwendung finden würden[3]. Das war vom historischen Gesetzgeber denn auch nie so gedacht. Zwar wollte das Parlament beim Erlass des DSG die Medienunternehmen nicht generell vom Anwendungsbereich des DSG ausnehmen. Dafür führte es das Medienprivileg für gewisse journalistische Datenbearbeitungen im Medienunternehmen ein. Gleichzeitig zeigen die Materialien unmissverständlich, dass das Parlament trotz der Unterstellung der Medien unter das Regime des DSG eines nicht wollte: das DSG auf die redaktionellen Publikationen selbst anwenden. Vielmehr wurde schon im Erstrat festgestellt, dass die materiellen Grundsätze des DSG *„für die Zeit der Bearbeitung vor und der Weiterbearbeitungen nach einer [Medien-]Publikation zu beachten sind.“*[4] Auch im Rahmen der Detailberatungen wurde nochmals klargestellt: *„Wir wollen eben genau das vermeiden, was viele Medienschaffende offenbar befürchten, dass keine*

[1] In diesem Sinne auch schon Rosenthal zur Informationspflicht nach dem früheren Art. 7a DSG, in Rosenthal, Handkommentar DSG, Zürich 2008, Art. 7a Abs. 1, N 9.
[2] Cherpillod, Information et protection des intérêts personnels, ZSR 1999 II 81, 131 f.; Schweizer, Recht am Wort: Schutz des eigenen Wortes im System von Art. 28 ZGB, Diss. Bern 2012, N 325 ff; Schwaibold, Basler Kommentar, ZGB I, 5. Aufl. 2014, Art. 28g N 2
[3] Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in Weblaw Jusletter, 20. Februar 2017, Rz. 93 ff., Rz 71
[4] Amtl. Bull. SR 1990 Bd. 1-3 S. 128.

Kumulation dieser beiden Instrumente für bereits publizierte Daten gelten soll. Das heisst also die Datenschutzbestimmungen gelten für Personendaten, die noch nicht publiziert sind, wenn noch keine Veröffentlichung der Daten stattgefunden hat, d.h. im Vorfeld der Publikation. Wenn sie publiziert sind, gilt das Instrumentarium des ZGB".[5]

2.4. Fazit zur besonderen Stellung der Medien

Der Gesetzgeber hat die Medien mit Rücksicht auf ihren verfassungsrechtlichen Informationsauftrag und zum Schutze der Medienfreiheit in zweifacher Hinsicht privilegiert:

Erstens: Auf redaktionelle Publikationen periodisch erscheinender Medien findet das DSG keine Anwendung. Hier spielt das Instrumentarium des ZGB.

Zweitens: Auf alle anderen Datenbearbeitungen durch das Medienunternehmen und seine Mitarbeiter findet das DSG Anwendung, wobei Bearbeitungen durch Medienschaffende im Sinne des Medienprivilegs von einem besonderen DSG-Regime profitieren.

Der VE-DSG darf diese zweifache Sonderstellung nicht verwässern. Deshalb ist erstens idealerweise in einem neuen Art 2 Abs. 5 VE-DSG festzuhalten, dass das DSG nicht auf Personendaten in redaktionellen Publikationen periodisch erscheinender Medien anwendbar ist.
Zweitens muss der VE-DSG klarstellen, dass das Privileg für Bearbeitungen durch Medienschaffende gegenüber allen datenschutzrechtlichen Instrumenten wie z.B. Melde-, Informations- und Anhörungspflichten oder die Datenschutz-Folgeabschätzung greift, soweit deren Anwendung Aufschluss über Informations-quellen geben, Einsicht in Entwürfe für Publikationen erlauben oder die freie Meinungsbildung des Publikums gefährden würde. Dies könnte generell in einem neuen Art. 2. Abs. 6 VE-DSG oder bei den jeweiligen Bestimmungen ergänzt und in der Botschaft bestätigt werden.

3. <u>Bemerkungen zu weiteren Bestimmungen des Vorentwurfes</u>

3.1. Die Beschränkung des Geltungsbereiches auf „natürliche Personen" wird begrüsst (Art. 2 VE-DSG)

Die SRG begrüsst die Beschränkung des Geltungsbereiches auf natürliche Personen. Die Anwendbarkeit auf juristische Personen nach aktuellem Recht ist eine schweizerische Besonderheit. Der Schutz juristischer Personen ist durch den allgemeinen Persönlichkeitsschütz ausreichend gewährleistet.

[5] Amtl. Bull. NR 1991 Bd. 3 S. 951.

3.2. Der Ausschluss der Anwendbarkeit des DSG auf „hängige Zivilprozesse“ nach Art. 2 Abs. 2 lit. c DSG ist beizubehalten

Art. 2 Abs. 2 lit. c DSG schliesst heute die Anwendbarkeit des DSG auf hängige Verfahren generell aus. Die SRG kann nicht nachvollziehen, wieso das VE-DSG keine entsprechende Bestimmung mehr enthält. Auch das zukünftige Datenschutzrecht hat die Anwendbarkeit des DSG auf hängige Verfahren explizit auszuschliessen, und zwar in Bezug auf alle Instanzen (auf Bundes- und kantonaler Ebene).

3.3. Vereinheitlichung der verwendeten Begriffe (Art. 3 VE-DSG)

Der Vorentwurf verwendet verschiedene Begriffe, die ungenügend definiert und / oder ungenügend von anderen Begriffen abgegrenzt sind (z.B. „Daten“, Dritte, Empfängerin und Empfänger. Die SRG plädiert dafür, dass der Entwurf diesbezüglich überarbeitet und Kohärenz in der Verwendung der Begriffe sichergestellt wird. Zudem ist die SRG der Ansicht, dass der Vorentwurf dort zu weit geht, wo nicht nur personenbezogene Daten, sondern auch Daten ohne Personenbezug erfasst sein sollen (siehe dazu insbesondere nachfolgend zu „Profiling“).

3.4. Beschränkung des Begriffs „Profiling“ (Art. 3 lit. f VE-DSG)

Der Vorentwurf eliminiert die bisherige schweizerische Besonderheit des „Persönlichkeitsprofils“, und übernimmt den auf europäischer Ebene etablierten Begriff des „Profiling“. Diese Angleichung macht Sinn und ist grundsätzlich zu begrüssen. Abzulehnen ist allerdings die im Vorentwurf vorgesehene schweizerische Variante, die eine Verschärfung gegenüber der Regelung in Art. 4 Abs. 4 EU-DSGVO darstellt.

Im Gegensatz zur EU-DSGVO (und zum E-SEV 108) liegt nach dem Vorentwurf „Profiling“

- **bei jeder Auswertung von Daten** vor, und **nicht nur bei einer automatisierten Auswertung**, und
- „Profiling“ liegt auch dann vor, wenn Daten ausgewertet werden, die **keine Personendaten** sind, sofern die Auswertung zu dem **Zweck** erfolgt, wesentliche persönliche Merkmale zu analysieren oder Entwicklungen insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit Intimsphäre oder Mobilität vorherzusagen.

Eine solche schweizerische Variante des Begriffs „Profiling“ bedeutet eine erhöhte Rechtsunsicherheit und einen erhöhten Aufwand für in der Schweiz tätige Unternehmen, was nicht gerechtfertigt ist. Falls der Begriff des „Profiling“ übernommen wird, ist er zwingend wie in Art. 4 Abs. 4 EU-DSGVO in zweierlei Hinsicht zu beschränken. Erstens auf „*automatisierte*“ Verarbeitung, und zweitens auf „personenbezogene“ Daten (Personendaten).

3.5. Keine ausdrückliche Zustimmung für Profiling erforderlich (Art. 4 Abs. 6 a. E. VE-DSG)

Der Vorentwurf sieht eine weitere schweizerische Besonderheit dahingehend vor, dass für Profiling-Sachverhalte die Einwilligung „ausdrücklich“ zu erfolgen hat. Das ist so auch auf europäischer Ebene nicht vorgesehen und abzulehnen ist. Dies würde vielmehr einen weiteren „Swiss Finish“ im Verhältnis zur EU-DSGVO bedeuten, der Schweizer Unternehmen benachteiligt.
Zur eingeschränkten Anwendbarkeit des Art. 4 Abs. 6 a. E. VE-DSG für Medienschaffende siehe vorne Ziff. 2, insbesondere Ziff. 2.2 und. 2.4.

3.6. Selbstregulierung zielführender als Empfehlungen der guten Praxis durch den EDÖB (Art. 8-9 VE-DSG)

Art. 8 Abs. 1 EV-DSG sieht neu vor, dass der EDÖB „Empfehlungen der guten Praxis“ unter Beizug der interessierten Kreise erarbeitet. Einerseits ist eine solche Regulierung durch den EDÖB nicht erforderlich, andererseits sind diese angedachten Befugnisse des EDÖB zu weitgehend und rechtsstaatlich fraglich. Der Erläuternde Bericht verweist auf S. 53 ausdrücklich auf existierende erfolgreiche Selbstregulierung durch Brancheninitiativen. Dementsprechend ist die SRG wie viele andere Schweizer Unternehmen[6] der Ansicht, dass eine Selbstregulierung zielführender ist, welche die Spezifizität pro Branche berücksichtigt. Dies gilt in besonderem Masse für die Medienbranche, die spezifisch gelagerte Beziehungen zu ihren Konsumenten pflegt und in der immer auch die Anforderungen der Medien- und Informationsfreiheit zu berücksichtigen sind.

Ein Blick auf die europäische Ebene bestätigt dieses Anliegen. Auch hier ist eine Selbstregulierung durch Verbände und andere Organisationen vorgesehen (Art. 40 und 40 EU-DSGVO). Eine darüber hinausgehende Regelung für die Schweiz macht keinen Sinn, und könnte allenfalls eine Einheitlichkeit einer schweizerischen Regelung des EDÖB mit einer Selbstregulierung auf europäischer Ebene verhindern.

[6] Anstatt vieler: siehe die Stellungnahme des VUD und des IAB

3.7. Institut des freiwilligen betrieblichen Datenschutzbeauftragten beibehalten

Der Vorentwurf enthält keine Bestimmungen zu betrieblichen Datenschutz-beauftragten, und der Erläuternde Bericht äussert sich dazu nicht. Die SRG ist der Ansicht, dass die aktuelle Regelung sinnvoll ist, und das Institut des betrieblichen Datenschutzbeauftragten im Sinne einer Selbstregulierung sehr wohl von Bedeutung ist. Die SRG regt deshalb an, dass das Institut eines (freiwilligen) betrieblichen Datenschutzbeauftragten beibehalten wird. Allerdings macht das Institut nur unter zwei Voraussetzungen Sinn. Erstens sollte dies mit administrativen Erleichterungen verknüpft werden (z.B. in Bezug auf Meldepflichten). Zweitens sind die im Vorentwurf vorgesehenen Sanktionsmechanismen substantiell zu überarbeiten, das heisst insbesondere die unnötig drakonischen Sanktionen gegen natürliche Personen (inklusive den Datenschutzbeauftragten) zu eliminieren (siehe unten, Ziff. 3.19).

3.8. Der neue Art. 12 VE-DSG gehört nicht ins DSG

Neu sieht der Vorentwurf für Erben und gewisse nahestehende Personen eines Verstorbenen weitgehende Rechte bezüglich der „Daten“ der „verstorbenen Person“ vor (Rechte auf Auskunft, Löschung und Vernichtung).

Diese Bestimmung ist insgesamt ersatzlos zu streichen. Sollte zu diesem Thema eine Regelung notwendig sein, wäre dies nach Ansicht der SRG inhaltlich im ZGB sowie in den passenden Spezialgesetzen zu regeln. Vor allem aber räumt Art. 12 VE-DSG den aufgeführten Personen im Verhältnis zur verstorbenen Person zu weitgehende Rechte ein. Nach Art. 12 Abs. 1 VE-DSG müsste keine ausdrückliche Autorisierung des Verstorbenen vorgewiesen werden können. Vielmehr würde auf „schutzwürdige Interessen der Erben oder Nahestehender abgestellt, die vorliegen, wenn „die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat“ oder „keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen“. Art. 12 VE-DSG auferlegt den „Verantwortlichen“ damit Pflichten, die sie nicht zu verantworten haben. Zu rügen ist insbesondere die oben dargelegte, faktische Überwälzung der Überprüfung der Berechtigung der antragstellenden Personen auf die „Verantwortlichen“, und die in Abs. 1 vorgesehene generelle „Kostenlosigkeit“. Zudem sieht Abs. 3 des Art. 12 VE-DSG vor, dass Amts- und Berufsgeheimnisse nicht geltend gemacht werden könnten, was rechtlich nicht nachvollziehbar ist.

Zur eingeschränkten Anwendbarkeit des Art. 12 VE-DSG für Medienschaffende siehe vorne Ziff. 2, insbesondere Ziff. 2.2 und. 2.4

3.9. Die Auftragsbearbeitung darf nicht unnötig erschwert werden (Art. 3 lit. h und i sowie Art. 7 ff. VE-DSG)

Die SRG begrüsst, dass in lit. h und i des Art. 3 VE-DSG neu die Begriffe „Verantwortlicher“ und „Auftragsbearbeiter“ definiert werden. Die SRG hält es allerdings für wichtig, dass die zwei Begriffe und Konzepte im gesamten revidierten DSG, wenn schon, dann analog demjenigen der europäischen Regelung ausgestaltet werden und nicht darüber hinaus gehen („Swiss Finish“). Letzteres betrifft insbesondere die Rechte und Pflichten von Auftragsbearbeitern, was für Unternehmen im Bereich des Outsourcings von Bedeutung ist. Insbesondere kann die SRG nicht nachvollziehen, dass der VE-DSG auch vom Auftragsbearbeiter eine Datenschutz-Folgeabschätzung verlangt. Dies macht nicht Sinn, und ist auch nicht in der EU-DSGVO vorgesehen.

Fraglich ist auch die in der EU-DSGVO nicht vorgesehene zwingende Zustimmung, welche der Verantwortliche nach Abs. 3 bei der der Beauftragung von Subunternehmern einzuholen hat. Das Outsourcing von technischen Dienstleistungen ist ein für Schweizer Unternehmen übliches und oft auch notwendiges Mittel. In Anbetracht der digitalen und technologischen Entwicklungen wird die Bedeutung von Auftragsbearbeitern auch weiter zunehmen. Ein Unternehmen darf aber datenschutzrechtlich nicht durch unnötige Hürden schlechter gestellt sein, weil es Datenbearbeitungen durch Dritte vornehmen lässt. Das belastet die Unternehmen zusätzlich und benachteiligt sie letztlich auch im Wettbewerb.

3.10. Grundsätze nach Art. 4 VE-DSG

Die SRG begrüsst die ausdrückliche Klarstellung in Art. 4 Abs. 3 VE-DSG, dass Personendaten auch zu einem Zweck verwendet werden dürfen, der mit dem ursprünglichen Zweck „kompatibel“ ist. Abgelehnt wird dagegen der neue Wortlaut des „klar erkennbaren Zwecks“. Der Zusatz „klar“ stiftet Verwirrung und damit Rechtsunsicherheit, und ist nicht erforderlich. Gemäss dem Erläuternden Bericht soll die materielle Rechtslage nicht geändert werden, und es besteht auch kein Klärungsbedarf. Dieser Zusatz ist deshalb ersatzlos zu streichen

Ebenso hält die SRG Abs. 5 des Art. 4 VE-DSG für unklar. Die SRG zieht die bisherige Regelung vor. Sollte die neue Formulierung beibehalten werden, ist der Satzteil «[…] *und wenn nötig nachgeführt wurden*» zu streichen. Eine Pflicht zur permanenten Nachführung ist in der Praxis nicht praktikabel. Es ist zudem nicht ersichtlich, was „wenn nötig“ bedeutet, und ob sich dies auf alle personenbezogenen Daten beziehen würde.

In Abs. 6 wird der in der Praxis ebenfalls sehr relevante Aspekt der „Einwilligung“ geregelt. Die SRG kann nicht nachvollziehen, wieso eine ausdrückliche Einwilligung für „Profiling“-Tatbestände erforderlich sein sollte. Es dürfte sich dabei in der Regel um alltägliche automatisierte Vorgänge handeln. Den Betroffenen wird in Art. 4 Abs.

6 VE-DSG ein Recht auf persönliche Anhörung eingeräumt, was einen ausreichenden Schutz sicherstellt.

Zu streichen ist nach Ansicht der SRG zudem der Zusatz, dass die angemessene Information *«[…] freiwillig und eindeutig»* zu erfolgen hat (Art. 4 Abs. 6 VE-DSG). Das „freiwillig" ist überflüssig, der Zusatz „eindeutig" stiftet im schweizerischen Rechtskontext Verwirrung. Es wird auf die ausführlichen Ausführungen in Jusletter[7] verwiesen.

Zur eingeschränkten Anwendbarkeit für Medienschaffende siehe vorne Ziff. 2, insbesondere Ziff. 2.2 und. 2.4.

3.11. Die Bestimmung zum neuen Erfordernis einer Datenschutz-Folgeabschätzung ist zu klären (Art. 16 VE-DSG)

Der VE-DSG möchte in nicht ausreichend klar definierten Situationen das Erfordernis einer „Datenschutz-Folgeabschätzung" einführen. Zudem stipuliert es in Abs. 3 eine Meldepflicht an den EDÖB und in Abs. 4 die Kompetenz des EDÖB, innerhalb von drei Monaten dem Verantwortliche Einwände mitzuteilen. Faktisch bedeutet dies, dass Unternehmen in sehr vielen Fällen als Vorsichts-massnahme aufwändige Abklärungen, Dokumentation und Datenschutz-Folgeabschätzung vornehmen und den EDÖB informieren werden. Dabei besteht gleichsam das Risiko von Phasen erhöhter Rechtsunsicherheit in unternehmens-internen Prozessen. Dies ist durch eine Klärung im Gesetz selbst (der Voraussetzungen und Anforderungen an eine solche Datenschutz-Folgeabschätzung) zu verhindern.

Es ist zudem nicht ersichtlich, wieso die aktuelle Rolle des EDÖB hier nicht ausreichen sollte. Die Rolle des EDÖB nach dem VE-DSG ist dementsprechend zu beschränken, und analog der EU-DSGVO auszugestalten. Essentiell wird zudem sein, dass der EDÖB innerhalb kurzer Fristen Stellung nimmt; die aktuell im VE-DSG gesehene Frist von 3 Monaten ist zu lang.

Problematisch ist des Weiteren die vage und sehr weite Formulierung, dass eine Datenschutz-Folgenabschätzung erfolgen muss, wenn eine Datenbearbeitung „**voraussichtlich zu einem erhöhten Risiko führt**". Diese Begriffe sind im Gesetz selbst zu klären und einzuschränken. Ebenso ist direkt im Gesetz zu klären, welche Grundanforderungen eine solche Datenschutz-Folgenabschätzung erfüllen muss.

Zur eingeschränkten Anwendbarkeit für Medienschaffende auf Art. 16 VE-DSG siehe vorne Ziff. 2, insbesondere Ziff. 2.2 und. 2.4.

[7] Rosenthal (FN 3).

3.12. Melde- und Informationspflicht müssen verhältnismässig sein („Data Breaches“, Art. 17 und 19 lit. b VE-DSG)

Der Vorentwurf verlangt neu eine „unverzügliche“ Meldung an den EDÖB von jeder „unbefugten Datenbearbeitung“ und von „Datenverlust“ (Art. 17 Abs. 1 EV-DSG), ausser, die Datenschutzverletzung führt „voraussichtlich nicht zu einem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person“. Eine solche Regelung würde Schweizer Unternehmen zwingen, unverhältnismässige interne Kontrollmassnahmen einzuführen, inklusive potentiell rechtlich fragwürdiger Überwachung von Mitarbeitenden. Diese Regelung beinhaltet einen unbegründeten „Swiss Finish“ im Verhältnis zur EU-DSGVO. Dies betrifft auch die Meldefrist, die nach dem Vorentwurf eine „unverzügliche“ ist, nach der EU-DSGVO aber 72 Stunden beträgt. Eine Meldepflicht sollte auf Situationen begrenzt werden, da tatsächlich ein erhöhtes Risiko für die Persönlichkeitsrechte der Betroffenen besteht. Ebenfalls abzulehnen ist die Schweizer Besonderheit gemäss Art. 19 lit. b des Vorentwurfes, wonach jeder Verantwortliche und Auftragsbearbeiter allfällige Drittempfänger der vom Data Breach betroffenen Daten zu informieren hat.

Zur eingeschränkten Anwendbarkeit der Art. 17 und 19 VE-DSG für Medienschaffende siehe vorne Ziff. 2, insbesondere Ziff. 2.2 und. 2.4.

3.13. Die Dokumentationspflicht (Art. 19 VE-DSG) ist genauer zu regeln, und ein Art 11a Abs. 5 lit. c DSG entsprechender Vorbehalt ist aufzunehmen

Der detaillierte Art. 11a DSG bezüglich „Register der Datensammlungen“ ist im Vorentwurf durch den Art. 19 „weitere Pflichten“ ersetzt worden. In Abs. 1 hält der Vorentwurf lapidar als Verpflichtung für die „Verantwortlichen“ und die „Auftragsbearbeiter“ fest „ sie dokumentieren ihre Datenbearbeitung“. Aus Sicht der SRG bedarf diese Dokumentationspflicht einer detaillierteren Regelung im Gesetz selbst, inklusive was das Verhältnis zu den Grundsätzen nach Art. 4 VE-DSG betrifft. Eine Regelung ausschliesslich auf Verordnungsstufe (Erläuternder Bericht, S. 65) ist nicht ausreichend. Unklar ist zudem, wieso der bisherige Abs. 6 nicht aufgenommen wurde, der ausdrücklich eine Delegation der Modalitäten an den Bundesrat vorsieht.

Zur eingeschränkten Anwendbarkeit für Medienschaffende siehe vorne Ziff. 2, insbesondere Ziff. 2.2 und. 2.4.

3.14. Die Informationspflicht der Empfänger von Personendaten ist zu beschränken (Art. 19 lit. b VE-DSG)

Die SRG teilt die bereits geäusserte Kritik an dieser Bestimmung[8]. Sie statuiert eine Pflicht zur Information der Empfängerinnen und Empfänger von Personendaten „über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes. Die Bestimmung ist ausufernd weit formuliert, in der Praxis kaum umsetzbar, und es ist fraglich, ob in der Realität das beabsichtigte Resultat erzielt wird. Auch hier ist der Revisionsbedarf nicht dargetan.

Zur eingeschränkten Anwendbarkeit des Art. 19 lit. b VE-DSG auf Medienschaffende siehe vorne Ziff. 2, insbesondere Ziff. 2.2 und. 2.4.

3.15. Auskunftsrecht (Art. 20 - 22 VE-DSG)

Was das generelle Auskunftsrecht nach Art. 20 VE- DSG anbetrifft, bedauert die SRG, dass sich nichts darüber findet, wie die missbräuchliche oder ausufernde Anrufung des Art. 20 VE- DSG in Zukunft verhindert wird. Fraglich erscheint dementsprechend, dass keine Einschränkung der Kostenlosigkeit vorgesehen ist (Abs. 1). Ebenso hält es die SRG für erforderlich, dass das Auskunftsrecht in der Regel auf weniger weitgehende als die in Abs. 2 vorgesehenen Informationen erstreckt (Abs. 2). Dies betrifft insbesondere die Angabe „der Identität und Kontaktdaten des Verantwortlichen“ (lit. a) und die „verfügbaren Angaben über die Herkunft der Personendaten“ (lit. f). Was Profiling-Sachverhalte betrifft, sollten die zusätzlich erforderlichen Angaben nach Abs. 3 des Art. 20 EV-DSG („das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung“) nach Ansicht der SRG auf „echte“ Fälle von automatisierter Entscheidung beschränkt werden.
Zum Medienprivileg und zur eingeschränkten Anwendbarkeit des Art. 20 Abs. 3 VE-DSG für Medianschaffende siehe vorne Ziff. 2.

3.16. Funktion des EDÖB (Art. 40 bis 45 VE-DSG)

Der Vorentwurf erweitert die Funktion des EDÖB substantiell, ohne dass dafür aufgrund der bisherigen Erfahrungen oder der europäischen Bestimmungen Anlass bestehen würde. Dementsprechend regt die SRG an, dass die Funktion des EDÖB wie bisher beibehalten wird. Die SRG verweist diesbezüglich auf die ausführliche Stellungnahme des VUD.

[8] Rosenthal (FN 3).

3.17. Zu weitgehende Untersuchungsbefugnisse des EDÖB (Art. 41 Abs. 3 VE-DSG)

Nach Art. 41 Ab. 3 EV-DSG erhält der EDÖB neu polizeiliche Untersuchungsbefugnisse, welche einen Swiss Finish darstellen und abzulehnen sind. Sollten sie, selbst in abgeschwächter Form, beibehalten werden, wäre klarzustellen, dass bei solchen Untersuchungshandlungen das Medienprivileg Vorrang hat (siehe generell dazu vorne Ziff. 2).

3.18. Aufschiebende Wirkung vorzusehen für Beschwerden gegen vorsorgliche Massnahmen des EDÖB (Art. 44 Abs. 3 VE-DSG)

Für Untersuchungsverfahren und Verfügungen des EDÖB verweist Art 44. Abs. 1 auf das VwVG. In Art. 3 möchte der Vorentwurf dann aber die aufschiebende Wirkung für Beschwerden gegen vorsorgliche Massnahmen ausschliessen.

Vorsorgliche Massnahmen im Bereich der Datenbearbeitung können massive Konsequenzen für Unternehmen haben, und einen Betrieb wesentlich behindern. Eine unabhängige richterliche Überprüfungsmöglichkeit ist daher entscheidend, und bis diese stattfindet, muss eine **aufschiebende Wirkung** möglich sein. Die SRG beantragt deshalb, dass für Beschwerden gegen vorsorgliche Massnahmen des EDÖB die Möglichkeit einer aufschiebenden Wirkung besteht, entsprechend den allgemeinen Grundsätzen.

3.19. Unverhältnismässige Strafbestimmungen (Art. 50 - 55 VE-DSG)

Die vorgesehenen Strafbestimmungen sind abzulehnen. Sie führen zu einer **nicht sachgerechten Kriminalisierung** der mit Datenschutz befassten Mitarbeitenden. Sie werden dazu führen, dass die gesetzlich gewollten Spielräume bei der Datenbearbeitung aus Angst vor persönlicher Bestrafung nicht ausgeschöpft werden und Unternehmen sehr viel mehr aufwändige Prozesse vorsehen müssen, um die betreffenden Mitarbeitenden zu schützen. Statt sich auf die Einhaltung des Datenschutzes zu fokussieren (die Verletzung der Bearbeitungsgrundsätze wird nicht sanktioniert), werden grosse Ressourcen auf die Einhaltung der formalen, mit Strafe bedrohten flankierendem Massnahmen konzentriert werden, was dem Datenschutz einen Bärendienst erweist. Es wird zudem schwieriger werden, Fachleute für die betreffenden Stellen in den Unternehmen zu gewinnen, da sie sich einem Strafbarkeitsrisiko aussetzen, und ein Versicherungsschutz für solche Fälle nicht möglich ist. Profitieren dürften vor allem die externen Berater, was die Kosten für Unternehmen in die Höhe treibt. Dies führt letztlich zu einem Wettbewerbsnachteil von Schweizer Unternehmen, deren Mitarbeitende mit unverhältnismässigen Strafen zu rechnen haben, während dies auf in der Schweiz aktive Unternehmen ohne schweizerische Niederlassung oder Mitarbeiter in der Schweiz nicht zutreffen wird.

Die Regelung ist auch von behördlicher Seite ineffizient, da nach der Konzeption des Vorentwurfes zwei parallele Verfahren geführt werden müssen, eines vom EDÖB und eines von den kantonalen Strafverfolgungsbehörden, die zudem nicht über das erforderliche Know-how verfügen. Ferner ist bei diversen Antragsdelikten unklar, wer überhaupt antragsberechtigt ist bzw. von wem der Strafantrag ausgeht(z.B. bei einer unterlassenen Datenschutzfolgeabschätzung.

3.20. Ausreichende Übergangfristen von mindestens 2 Jahren vorsehen (Art. 59 VE-DSG)

Der Vorentwurf sieht nur punktuell - betreffend Art. 16, 18 und 19 VE-DSG - eine Übergangsfrist von zwei Jahren vor, was die Schweizer Unternehmen vor unhaltbare Umsetzungsprobleme stellen würde. Die EU hat für das Inkrafttreten der EU-DSGVO eine generelle Übergangsfrist von 2 Jahren vorgesehen.

Die SRG ist der Ansicht, dass ausführliche Übergangsbestimmungen, die eine angemessene Frist einräumen, essentiell sind. Die SRG hält eine generelle Übergangsfrist von 2 Jahren für erforderlich und angemessen.

Für die Berücksichtigung der Anliegen der SRG zur Schaffung einer verhältnismässigen und praxistauglichen Datenschutzregulierung, die zugleich dem verfassungsrechtlich verankerten Informationsauftrag der Medien und der Medienfreiheit Rechnung trägt, danken wir Ihnen im Voraus.

Freundliche Grüsse

Roger de Weck
Generaldirektor

Amstutz Jonas BJ

Von: Voggensperger, Ruth <Ruth.Voggensperger@redcross.ch>
Gesendet: Montag, 3. April 2017 17:19
An: Amstutz Jonas BJ
Cc: Fischer, Vera
Betreff: Vernehmlassung VE-DSG
Anlagen: 2017_Totalrevision-Datenschutzgesetzes_Stellungnahme_def.pdf; 2017_Totalrevision-Datenschutzgesetzes_Stellungnahme_def.doc

Sehr geehrter Herr Amstutz

In der Beilage erhalten Sie die Vernehmlassung zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz.

Freundliche Grüsse
Ruth Cäzilia Voggensperger
Stv. Leiterin Rechtsdienst/Deputy Head Legal Service

Schweizerisches Rotes Kreuz . Croix-Rouge suisse
Abteilung Direktion

Rainmattstrasse 10 . Postfach . Case postale . CH-3001 Bern
Telefon +41 58 400 4 470 . Mobil +41 79 277 30 67
ruth.voggensperger@redcross.ch

www.redcross.ch

Achtung: neue Telefonnummern ab Januar 2017
Attention : nouveaux numéros de téléphone à partir de janvier 2017

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Geschäftsstelle des Schweizerischen Roten Kreuzes

Abkürzung der Firma / Organisation : SRK

Adresse : Rainmattstr. 10, 3000 Bern, Postfach

Kontaktperson : Ruth C. Voggensperger, Stv. Leiterin Rechtsdienst

Telefon : +41 58 400 4 470

E-Mail : ruth.voggensperger@redcross.ch

Datum : 3. April 2017

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SRK	**Vorbemerkung:** Das SRK begrüsst grundsätzlich die mit der Totalrevision des Datenschutzrechts anvisierte Selbstbestimmung der betroffenen Personen über ihre Daten. Wir unterstützen das Ziel des VE-DSG, wonach jede einzelne Person die Verantwortung über ihre Daten selbst in der Hand hat und diese auch wahrnehmen soll. Sie soll die Bearbeitung ihrer Daten kontrollieren, abfragen und ändern können. Sie muss wissen, wer welche Daten wann bearbeitet und sie muss im Notfall Massnahmen zur Hand haben, um die unerlaubte Verwendung ihrer Daten verbieten zu können. Mit der Selbstbestimmung verbunden ist das beibehaltene Regelungskonzept des *opting-out*, d.h. die generelle Erlaubnis, Personendaten im privaten Bereich zu bearbeiten. Wer nicht mitmachen will, soll sich ausklinken. Dieser Entscheid ist im Wesentlichen richtig und zu unterstützen. Wie die Praxis heute jedoch zeigt, bedarf das Regelungskonzept des *opting-out* einer proaktiven Selbstverantwortung des zu Schützenden. Dies ist insbesondere Jugendlichen und jungen Erwachsenen nicht immer klar. Aktivitäten jeglicher Art im w*orld wide web und* auf *social platforms,* welche oft auch marketingmässig Konsequenzen haben, sind anfällig für die Verletzung von personenbezogenen Daten. Wir bedauern deshalb, dass die Prävention für den sinnvollen Umgang mit Daten im Gegensatz zur Sanktion im revidierten Erlass nicht höher gewichtet worden ist. Die Geschäftsstelle des SRK geht bereits heute sehr bewusst und sorgfältig mit den ihr anvertrauten Daten um. Wir bemühen uns um eine zielgerichtete, angemessene Information unserer vielschichtigen Anspruchspersonen mit ihren sehr unterschiedlichen Bedürfnissen, angefangen vom Bezüger einer Dienstleistung, vom aus einer Lawine Geretteten über die Spenderin oder den Gönner bis hin zur besonders bedürftigen und schützenswerten Migrantin. Als gemeinnützige Organisation verfügt das SRK über ehrenamtlich tätige, strategische Leitungsorgane und in den Rotkreuz-Organisationen über eine stattliche Anzahl von Freiwilligen, welche ohne Vergütungen für das SRK tätig sind. Viele Freiwillige sind in Bereichen tätig, welche mit Rettung, Unterstützung und Entlastung zu tun haben. In einer Notsituation muss der Helfende schnell handeln und vielfach geht es um Minuten. Vor diesem Hintergrund stellt sich die Frage nach dem Schutz der zu erhebenden Daten erst sekundär und der Helfer oder die Helferin müssen davon ausgehen, dass der Hilfesuchende prinzipiell sein Einverständnis zu Erhebung der notwendigen Daten geben würde. Dieser Fokus darf nicht aus den Augen verloren werden, wenn es um den angemessenen Datenschutz von hilfesuchenden Personen im SRK geht. Die vorgesehenen Neuregelungen des Datenschutzgesetzes sind, auch wenn einzelne Regelungen durchaus Sinn machen, als Ganzes zu komplex und administrativ zu aufwändig. Gemeinnützige Organisationen ohne eigenen Rechtsdienst oder interne Datenschutzbeauftragte, wozu alle kleineren Rotkreuz-Organisationen zu zählen sind, werden gezwungen sein, das erforderliche Know-how extern teuer einzukaufen und mehr personelle Ressourcen für den erheblichen administrativen Mehraufwand einzusetzen. Die Mittel dafür werden nicht über Spenden generiert werden können. Es wird dazu führen, dass weniger Mittel für die Erfüllung der gemeinnützigen Zwecke zur Verfügung stehen werden. Wir bedauern

	dies und erkennen darin eine weitere Überregulierung, die den Schweizer Gemeinnützigkeitsstandort benachteiligen wird. Auch sind wir der Auffassung, dass wir mit dem bestehenden Datenschutzgesetz, dessen Umsetzung wesentlich effizienter und kostengünstiger ist, als es beim neuen Gesetz der Fall wäre, genügend Instrumente zur Hand haben, um einen angemessenen und wirksamen Schutz von Personendaten zu garantieren. Wir haben Verständnis dafür, dass die Schweiz das revidierte europäische Recht (Übereinkommen SEV 108; EU-Datenschutzgrundverordnung) nachvollziehen will und in einigen Punkten auch anpassen muss. Wir haben hingegen kein Verständnis dafür, dass die neuen Regelungen über die Anforderungen der EU hinausgehen. Ein solcher *Swiss Finish*, der mit einer massiven Verschärfung des Schweizerischen Datenschutzrechts gerade im Verantwortlichkeitsbereich einhergeht, ist nicht nur unnötig, sondern mit einem liberalen, standortfreundlichen Verständnis und dem Gebot der Praktikabilität – gerade auch in ehrenamtlichen bzw. Miliz-Strukturen – nicht zu vereinbaren. Dies trifft insbesondere auch auf die neuen Instrumente zur Sicherstellung des Datenschutzes zu wie die *Meldepflicht* bei Verstössen oder die *Datenschutzfolgenabschätzung.* Müssten diese so umgesetzt werden wie vorgeschrieben, würden sie nicht nur die bestehenden personellen Ressourcen des EDÖB vollständig überfordern, sondern die Ressourcen jeder einzelnen NPO, welche mit den ihr anvertrauten Mitteln haushälterisch und zweckbestimmt umgehen muss. Der dafür zu leistende Aufwand für unsere Rotkreuz-Organisationen wäre enorm, ohne dass für den Schutz der Daten für den Einzelnen an sich etwas gewonnen würde. Die Instrumente machen rechtlich keinen Sinn und sind zu hinterfragen. Kurz zusammengefasst befürworten wir alle Bestimmungen, die die Eigenverantwortung von Unternehmen und Privatpersonen stärken. Aufgeblähte Sicherungsmassnahmen und Sanktionen, welche in der Realität nicht umsetzbar sind oder zur Kriminalisierung führen, lehnen wir hingegen ab. Nachfolgend nehmen wir punktuell zu einzelnen gesetzlichen Regelungen im Vorentwurf Datenschutzgesetz Stellung.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SRK	VE DSG	3		a	Der Begriff des Personenbezugs ist dahingehend klarzustellen, dass dieser im Einzelfall zu beurteilen ist. Eine rein theoretische Möglichkeit, wonach jemand identifiziert werden könnte, darf nicht ausreichen, um den Bezug auf eine Person für bestimmbar zu erklären.
SRK	VE-DSG	3		c	Wir begrüssen die Aufnahme von genetischen und biometrischen Daten in den Katalog der besonders schützenswerten Personendaten. Gerade genetische Daten beinhalten ein grosses Risiko des Missbrauchs durch Dritte. Diese sehr persönlichen Informationen gilt es zu schützen. Wir empfehlen hingegen, den Schutzgedanken der biometrischen Daten zu klären: unter die besonders schützenswerten Daten sollen nur diejenigen biometrischen Daten fallen, welche zum Zweck der eindeutigen Identifikation bearbeitet werden, nicht aber solche Daten, welche nicht zu Erkennungs- sondern zu anderen Zwecken bearbeitet werden. Wir denken hierbei z.B. an die künstlerische Bearbeitung.
SRK	VE-DSG	3 in Verb. mit Art. 23 Abs. 2 lit. d		f	Die Definition des neu eingeführten Begriffs *Profiling* ist extrem breit gefasst und geht deutlich über die Anforderungen der EU hinaus. Gemäss Art. 23 Abs. 2 lit. d soll ein Profiling ohne ausdrückliche Einwilligung der betroffenen Personen *per se* persönlichkeitsverletzend sein. Letztere Regelung halten wir für problematisch, weil es unklar ist, welche Profile in der Praxis unter den Begriff des persönlichkeitsverletzenden Profiling fallen werden. Wir empfehlen mit Nachdruck, den Begriff enger zu fassen und inhaltlich klarer zu formulieren. Sodann ist der Hinweis in Art. 3 lit. f. E-DSG auf „Daten“ zu streichen, da es sich beim Profiling naturgemäss um Personendaten handelt, welche sich auf eine bestimmbare Person beziehen müssen.

SRK	VE-DSG	Art. 6 In Verbindung mit den Erläuterungen	1	c	Wir begrüssen die Erwähnung der Bekanntgabe von Personendaten ins Ausland aus humanitären Gründen in den Erläuterungen zum VE-DSG. Die länderübergreifende Arbeit des SRK und seiner Organisationen beinhaltet für einige Dienstleistungen die Bekanntgabe von Personendaten ins Ausland. Dies trifft insbesondere auf den Suchdienst für vermisste Familienangehörige zu, dessen wichtige humanitäre Funktion unbestritten ist. Da der hier definierte Begriff der *Wahrung eines überwiegenden öffentlichen Interesses* für Laien auf den ersten Blick nicht mit humanitärer Arbeit gleichgesetzt wird, regen wir an, die Ausnahme der Bekanntgabe von Daten ins Ausland aus humanitären Gründen direkt im Gesetz oder in der zu revidierende Verordnung zu regeln.
SRK	VE-DSG	Art. 6 In Verbindung mit den Erläuterungen	1	d	Analog zu den Erläuterungen zur EU-Verordnung (EU) 2016/679 (Ziffer 46 und 112) und dem Protokoll zur Revision des Übereinkommens SEV 108 des Europarates (Ziffer 46) würden wir es mit Blick auf die Arbeit des vorgängig genannten Suchdienstes für vermisste Familienangehörige begrüssen, wenn in die Erläuterungen aufgenommen wird, dass die Bekanntgabe von Personendaten ins Ausland aus humanitären Gründen ebenfalls notwendig sein kann, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder der im Ausland gesuchten Drittperson zu schützen. Sowohl die EU-Verordnung wie auch das Übereinkommen SEV 108 anerkennen, dass Datenbearbeitungen im humanitären Bereich sowohl im öffentlichen Interesse wie auch im privaten Interesse der betroffenen Person liegen können, so zum Beispiel bei der Bearbeitung von Daten von vermissten Personen. In diesen Fällen kann sich die Bearbeitung der Daten der vermissten Person (nicht der Suchenden) auf das private Interesse der suchenden wie auch der gesuchten Person stützen und gleichzeitig liegt die Arbeit im öffentlichen Interesse (Aufklärung des Verschwindens).
SRK	VE-DSG	7 in Verb. mit Art. 13 Abs. 4/5			Die verschärften Regelungen in der Auftragsdatenbearbeitung sind, obwohl gut gemeint, in der Praxis nicht alle umsetzbar. Es ist eine Tatsache, dass Daten, insbesondere solche zum Zweck des Dialogmarketings, d.h. Daten, welche gezielt auf die Interessen von Dienstleistungsempfängern und Kundinnen zugeschnitten sind, vermehrt durch Dritte bearbeitet werden. Viele Firmen leiten ihre Kundendaten zu verschiedenen Bearbeitungszwecken an unterschiedliche Datenempfänger weiter. Diese Tatsache an sich muss aber nicht zwingend mit Datenmissbrauch gleichgesetzt werden. Im Gegenteil bezweifeln wir, ob die neuen Bestimmungen im VE-DSG, welche die

					Auftragsdatenbearbeiter und deren Subunternehmer parallel zum Datenverantwortlichen in Pflicht, nehmen, zielführend sind. Die neuen Bestimmungen könnten dazu führen, dass sich Datenverantwortliche und Auftrags- oder Sub-Auftragsdatenbearbeiter im Falle von Datenschutzverstössen gegenseitig die Verantwortung zuschieben. Gerade im NPO-Bereich entstehen Vertrauensbeziehungen zwischen der hilfeleistenden Organisation und ihren Anspruchspersonen. Der Erhalt dieses Vertrauens kann nicht auf Dritte abgeschoben werden. Die datenerhebende, verantwortliche Organisation, welche die Herrschaft über die Daten hat, ist nach wie vor vollumfänglich in die Pflicht zu nehmen. Sie hat dafür zu sorgen, dass der Auftragsdatenbearbeiter die Datensicherheit gewährleistet und damit das Vertrauen der Anspruchspersonen in die NPO nicht zerstört wird. Regelungen in der VE-DSG, die auf einen direkten Kontakt zwischen der betroffenen Person und dem Auftragsdatenbearbeiter oder seinem Subunternehmer zielen, bringen Rechtsunsicherheit mit sich und verwirren Kunden oder Spenderinnen. Dies trifft indirekt auch auf Art. 13 Abs. 4 VE-DSG zu, wonach die verantwortliche Person oder NPO die betroffene Person umfassend über die Übertragung von Daten an einen Auftragsbearbeiter informieren muss. Die Informationspflicht beinhaltet auch die Identität und die Kontaktdaten des Auftragsbearbeiters. Die Erläuterungen äussern sich leider nicht zur Frage, was die betroffene Person mit diesen Kontaktdaten anstellen soll. Soll sie direkt Kontakt mit dem Auftragsbearbeiter aufnehmen? Soll sie z.B. so grosse und weit entfernte Firmen wie Apple Pay in den USA (Zahlungsverbarbeitung) oder Alipay in China (Zahlungsmittelprüfung) direkt kontaktieren? Für eine NPO, welche mit limitierten Ressourcen arbeiten muss, würde der Umfang dieser vorgängig zu leistenden Informationspflicht einen Mehraufwand bedeuten, der weder bewältig- noch finanzierbar ist. Wichtig ist aus unserer Sicht, dass die verantwortliche NPO vertraglich und de facto sicherstellen muss, dass der Auftragsdatenbearbeiter die Datensicherheit genügend gewährleistet. Auf der Datenschutzerklärung soll der Hinweis gemacht werden, in welchem Rahmen Daten an Dritte zur Bearbeitung weitergeleitet werden. Die betroffene Person soll hingegen einzig im Rahmen ihres persönlichen Auskunftsrechts Anrecht darauf haben, die Kontaktdaten des Auftragsbearbeiters zu erfahren. Wir empfehlen, die neuen Regelungen der Auftragsdatenbearbeitung zu überdenken. Bestimmungen, welche den Auftragsbearbeiter oder dessen Subunternehmer parallel zur

					verantwortlichen Organisation in Pflicht nehmen, sind zu streichen. Bestimmungen, welche eine Informationspflicht über eine transparente Information in der Datenschutzerklärung hinaus verankern, sind ebenfalls zu streichen. Art. 13 Abs. 4 und 5 sind ersatzlos zu streichen.
SRK	VE-DSG	8/9			Der Erlass von selbstverpflichtenden Good-Practice-Codes ist zu begrüssen. Der dritte Sektor, namentlich der NPO-Sektor, macht gute Erfahrungen mit Governance-Kodizes und zertifizierenden Branchenstandards wie den Standards der Stiftung ZEWO. Solche Standards würden zudem die Möglichkeit bieten, nach Branchen vorzugehen und deren spezifische Bedürfnisse nach adäquatem Datenschutz abzubilden. Damit diese Standards praxisorientiert sind, empfehlen wir, das vorgesehene Procedere umzukehren: Die Standards sollen durch die Branchen selbst erarbeitet und erst danach dem EDÖB zur Genehmigung vorgelegt werden. Mit diesem Vorgehen wird sichergestellt, dass die Standards von den betroffenen Organisationen und Unternehmen eingehalten werden. Art. 8 ist dahingegen zu präzisieren. Art 9 halten wir für überflüssig. Da die Empfehlungen kompatibel mit dem geltenden Datenschutzrecht sein müssen, hält der Verantwortliche per se die Datenschutzvorschriften ein (Art. 9 Abs. 1). Wenn die Datenschutzvorschriften auch auf andere Weise eingehalten werden als in den Standards geregelt, so ist das Sache der Unternehmung oder der NPO, solange sie Datenschutzrecht nicht verletzt (Art. 9 Abs. 2), das bedarf aber keiner Erwähnung im Gesetz. Art. 9 ist daher ersatzlos zu streichen.
SRK	VE-DSG	12			Die Diskussion über den Umgang mit Daten verstorbener Personen wird künftig von grösserem Stellenwert sein als heute, da vor allem die automatisierte Datenbearbeitung vor dem Tod eines Menschen nicht mehr Halt macht. Das SRK ist der Meinung, dass es sich bei der Frage nach dem Umgang mit dem „digitalen Tod“ nicht um eine „zeitgeistige Erscheinung“ handelt, sondern um eine Frage von grosser ethischer und rechtlicher Bedeutung. Es fragt sich hingegen, ob die vorgesehen Regelungen in Art. 12 VE-DSG am richtigen Ort sind, insbesondere, da sie als generell-abstrakte Normen nie alle Fälle in der Praxis abdecken können. Systematisch ist es sinnvoller, entsprechende Datenschutzbestimmungen in die jeweiligen Erlasse, aufzunehmen, wo sich die Probleme im Einzelnen stellen, z.B. in das Erwachsenenschutzrecht (Umgang mit

					Patientenverfügungen) oder in die Bestimmungen über das Zivilstandswesen. Wir empfehlen daher die Streichung von Art. 12 und die Aufnahme angemessener Datenschutzbestimmungen in die jeweiligen Erlasse, soweit dort nicht bereits geregelt.
SRK	VE-DSG	13	4-5		Vgl. hierzu unsere Bemerkungen unter Art. 7
SRK	VE-DSG	15 in Verb. mit Art. 20 Abs. 3			Der Anspruch auf „menschliches Gehör“ im Falle von automatisierter Einzelfallentscheidungen ist aus unserer Sicht richtig. Automatisierte Entscheidungen mit rechtlicher Wirkung treffen den Menschen dort, wo er gegen ein Computersystem nichts ausrichten kann: nämlich in der Unmöglichkeit, sich verständlich zu machen, bevor der Entscheid getroffen ist. Trotzdem fragt es sich, ob die hier neu geregelte umfassende Informations- und Auskunftspflicht im Einzelfall Sinn macht. Eine giesskannenartige „präventive“ Informationspflicht und ein breit gefasstes Auskunftsrecht auf Seiten des Betroffenen bringt niemandem etwas. Auch bringt es keinen Mehrwert, wenn die betroffene Organisation im Sinne von Art. 20 Abs. 3 erklären muss, auf welchem Wege automatisierte Einzelfallentscheidungen zustande kommen. Sinn machen Informationen und Auskünfte hingegen dort, wo eine automatisierte Einzelfallentscheidung tatsächlich rechtliche und persönliche Auswirkungen auf eine Person haben. Erst dann soll diese angemessen informiert und angehört werden. Wir empfehlen, Art. 15 und Art. 20 Abs. 3 in diesem Sinne anzupassen.
SRK	VE-DSG	16			Das neue Instrument der Datenschutz-Folgenabschätzung (Privacy Impact Assessment) wirft mehr Fragen auf als es Probleme zu lösen vorgibt. Es schadet sicherlich keinem Unternehmen, — egal ob im For- oder Nonprofit-Bereich tätig —, im Rahmen einer internen Abklärung genau hinzuschauen, was mit den zu bearbeitenden Daten geschieht und wo die Risiken für die betroffenen Personen bzw. vice versa für die Unternehmung und deren Reputation liegen. Es ist aber rechtlich weder geboten, noch sinnvoll, wenn zukünftig *jede* Bearbeitung normaler oder besonders schützenswerter Daten, die *voraussichtlich zu einem erhöhten Risiko führt,* eines vorgängigen Datenschutz-Assessments bedarf. Abgesehen davon, dass das Gesetz nicht darüber Auskunft gibt, wann ein solches Risiko noch normal oder eben erhöht ist, verlangt die EU für die Durchführung einer Folgenabschätzung kein erhöhtes, sondern ein "hohes Risiko". Ob das hohe

					Risiko in der Praxis besser definierbar ist als das erhöhte Risiko, bleibe dahingestellt. Das SRK tätigt seine Kerngeschäfte zu einem grossen Teil im Bereich der besonders schützenswerten Personendaten, sei dies im Gebiet der Entlastung, der Gesundheit, im Suchdienst, in der Rettung, bei der Mithilfe für das Ausstellen einer Patientenverfügung oder in den Hilfeleistungen an besonders Bedürftige. In diesen Bereichen müsste das SRK generell davon ausgehen, dass ein erhöhtes Risiko für die Datenbearbeitung per se vorliegt. Aber auch dann bliebe eine Datenschutz-Folgenabschätzung hypothetisch. In der Praxis hat die Geschäftsstelle SRK in den vergangenen Jahren nicht eine einzige Rüge einer Persönlichkeitsverletzung oder der Verletzung eines Grundrechts zu verzeichnen. Dazu kommt, dass die in Art. 16 Abs. 4 vorgegebenen Fristen unrealistisch sind, weil wir in Notfällen schnell handeln müssen und nicht erst eine langwierige Folgenabschätzung machen können. Der für das SRK und seine Organisationen erforderliche administrative Aufwand für die Datenschutz-Folgenabschätzung in der aktuellen Version wäre enorm. Er stünde in keinem Verhältnis zum Nutzen der Folgenabschätzung. Zudem müsste das SRK erhebliche Mittel einsetzen, um die Folgenabschätzung umzusetzen. Wir beantragen, den Anwendungsbereich der Datenschutz-Folgenabschätzung entweder inhaltlich, d.h. nur für bestimmte Zwecke der Datenbearbeitung oder strukturell, nämlich durch die Ausnahme von gemeinnützigen Organisationen, einzuschränken. Möglich wäre auch, die Datenschutz-Folgenabschätzung als taugliches Instrument für das selbstverantwortliche Handeln auszugestalten, d.h. in den Best Practice-Standards einzelner Branchen zu regeln.
SRK	VE-DSG	17 in Verb. mit Art. 50 Abs. 2 lit. e			Der Vorentwurf sieht vor, eine Meldepflicht für Datenschutzverstösse einschliesslich Datenverlust (Data Breach Notification) einzuführen. Wir begrüssen die Meldepflicht an den EDÖB dort, wo es sich um die Verletzung von Sicherheitsmassnahmen handelt, die zu einem Verlust des Gewahrsams von Daten führt, wie dies z.B. bei gehackten Daten der Fall ist. Eine Meldepflicht hingegen, die jeden Datenschutzverstoss erfasst, ist unrealistisch und auch von Seiten des EDÖB nicht ohne massive Aufstockung zu bewältigen, da solche in der Praxis schätzungsweise täglich vorkommen, ohne dass sie nennenswerte Probleme mit sich bringen. Auch die Benachrichtigung jedes Verstosses an den Betroffenen ist unrealistisch: Versenden wir

					z.B. die falsche Patientenverfügung an das Spital, in welchem der Betroffene behandelt wird, oder senden wir die richtige Patientenverfügung an das falsche Spital, in welchem der Betroffene nicht behandelt wird, so liegt zwar ein Verstoss gegen das Datenschutzgesetz vor, der im Hinblick auf medizinisches Handeln sofort und zeitlich nah zu korrigieren ist, allenfalls den betroffenen Personen mitzuteilen ist. Es ist aber weder ersichtlich noch zielführend, weshalb wir diese Verletzung an den EDÖB melden müssten. Auch die scharfe Strafdrohung bei Nichteinhalten der Meldepflicht in Art. 50 Abs. 2 lit. e führt möglicherweise kontraproduktiv dazu, dass Datenschutzverstösse firmenintern vertuscht werden. Das widerspricht dem anvisierten Ziel nach grösstmöglicher Transparenz für die Betroffenen. Die Meldepflicht ist daher auf eine praktikable Regelung zu beschränken, in welcher nur Fälle gemeldet werden müssen, die eine Vielzahl von Personen betreffen, da sich ein Eingreifen der Aufsichtsbehörden nur dann rechtfertigt. Wir beantragen zudem, die unverzügliche Meldung in eine Meldung ohne unnötigen Verzug umzuformulieren, da Datenschutzverstösse intern zuerst erkannt und aufgearbeitet werden müssen. Beibehalten werden soll Art. 17 Abs. 4, wonach der Auftragsdatenbearbeiter eine unbefugte Datenbearbeitung dem verantwortlichen Unternehmen nach Kenntnisnahme sofort melden muss. Das verantwortliche Unternehmen soll in diesem Fall die notwendigen Massnahmen prüfen und einleiten.
SRK	VE-DSG	Art. 24 In Verbindung mit den Erläuterungen	1		Ergänzend zu den Ausführungen zu Art. 6 Abs. 1 lit. c und d würden wir es begrüssen, wenn der erläuternde Bericht auch hier erwähnen würde, dass ein Rechtfertigungsgrund ebenfalls aus humanitären Gründen vorstellbar ist, - sofern durch ein überwiegendes privates oder öffentliches Interesse gedeckt. So z.B. bei der in den Genfer Konventionen verankerten Aufklärung des Aufenthalts von vermissten bzw. verschwundenen Personen (vom Bundesrat rechtlich wie auch mittels finanzieller Unterstützung anerkannt, vgl. Medienmitteilung des Bundesrates vom 24.06.2015).
SRK	VE-DSG	Art. 27/29 In Verbindung	3/2	c/c	Analog zu den vorangehenden Ausführungen schlagen wir vor, in die Erläuterungen ebenfalls einen Passus einzufügen, wonach die Bearbeitung von Personendaten durch Bundesorgane für humanitäre Zwecke und gestützt auf die Genfer Konventionen notwendig sein kann, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es

		mit den Erläuterungen			nicht möglich ist, rechtzeitig eine Einwilligung einzuholen. Dies würde klären, dass es Bundesorganen (z.B. dem SEM) möglich ist, in solchen Fällen Angaben zu gesuchten Personen bekanntzugeben auch wenn keine ausdrückliche gesetzliche Grundlage für eine solche Bekanntgabe vorliegt.
SRK	VE-DSG	50ff.			Das geltende DSG kennt, von der Übertretungsnorm gemäss Art. 34 DSG abgesehen, keine nennenswerten Strafbestimmungen. Dieser Zustand soll nun durch Einführung scharfer Sanktionen geändert werden. Die neuen Strafbestimmungen von Art. 50 ff. E-DSG richten sich gegen private Personen, bei Vereinen und Stiftungen in der Regel also gegen Organe und vor allem die verantwortlichen Mitarbeitenden selbst. Erfasst werden auch fahrlässige Datenschutzverstösse, was zu einer stossenden Kriminalisierung von Organen und Mitarbeitenden führen wird. Die Bussenobergrenze bei der Verletzung von Sorgfaltspflichten von CHF 500'000 für vorsätzliches Verhalten und CHF 250'000 für fahrlässiges Verhalten auch einzelner Mitarbeitender ist massiv und unverhältnismässig. Dies insbesondere auch gegenüber Mitarbeitenden im NPO-Bereich, deren Löhne erheblich niedriger sind als bei Mitarbeitenden grosser Konzerne. Die strafrechtliche Verantwortung der natürlichen Personen geht weit über die notwendige Verschärfung und über die europäischen Regelungen hinaus. Auch dürfte die flächendeckende Kriminalisierung dazu führen, dass sich Organe und Mitarbeitende davor hüten werden, ohne externe Beratung Entscheide im Bereich der Datenbearbeitung zu treffen. Dies führt wiederum zu einem Kostenschub mit dem Ergebnis, dass Stiftungs- oder Vereinsmittel nicht mehr für die Erfüllung des gemeinnützigen Zwecks zur Verfügung stehen. Der persönliche, strafrechtliche Charakter der Sanktionen wird dazu führen, dass Personen, welche Daten bearbeiten, ja selbst betriebliche Datenschutzbeauftragte mit der Schaffung eines persönlichen Strafbarkeitsrisikos unnötig exponiert werden. Wir sind aber auch hier, wie bereits erwähnt, der Meinung, dass Datenschutz primär Chefsache bzw. eine Sache des obersten Leitungsorgans ist und nicht der Marketingassistentin oder des IT-Mitarbeitenden. Daher ist deren persönliche strafrechtliche Erfassung stossend. Insbesondere, weil sie auch die Arbeitgeberpflichten, speziell die gute Führung und die Sorgfaltspflichten gegenüber dem

					Arbeitnehmer unterminiert. Das SRK beantragt, die Strafbestimmungen in dem Sinn zu überarbeiten, dass sie hinsichtlich Anwendungsbereich und Sanktionshöhe auf ein vernünftiges Mass reduziert werden. Die Fahrlässigkeitsdelikte sind ersatzlos zu streichen. Art. 52 E-DSG führt schliesslich eine neue berufliche Schweigepflicht ein, deren Missachtung mit Freiheitsstrafe bis zu drei Jahren pönalisiert ist. So untersteht jeder Berufstätige (Nebenbemerkung: was ist mit den Freiwilligen oder ehrenamtlich Tätigen?) neu einer sanktionierten Schweigepflicht und zwar unabhängig davon, ob die Daten selbst einer Geheimhaltung unterliegen. Diese Regelung ist übertrieben. Abgesehen davon, dass die meisten Unternehmen die berufliche Schweigepflicht, die NPO darüber hinaus auch diejenige für Freiwillige, in ihren firmeninternen Personalerlassen, Arbeitsverträgen oder Standards regeln. Wir beantragen mit Nachdruck, Art. 52 E-DSG zu streichen und durch die bisherige Regelung von Art. 35 DSG zu ersetzen.

Wir danken Ihnen, sehr geehrte Frau Bundesrätin, für die aufmerksame Prüfung unserer Kommentare und Anträge. Wir hoffen, dass diese Eingang in die neue Vorlage finden.

Mit hochachtungsvollen Grüssen

Markus Mader
Direktor

Ruth C. Voggensperger
Stv. Leiterin Rechtsdienst

Amstutz Jonas BJ

Von:	snocera@ssphplus.ch
Gesendet:	Freitag, 31. März 2017 09:01
An:	Amstutz Jonas BJ
Cc:	'Nino.Kuenzli@unibas.ch'; dominique.sprumont; Luca Crivelli; Tanner Marcel; Ursula Erni
Betreff:	Stellungnahme SSPH+ zu Vernehmlassung "Loi sur la protection des données/Datenschutzgesetz"
Anlagen:	SSPH_Révision LPD_prise de position_31032017.doc

Sehr geehrter Herr Amstutz

Im Anhang sende ich Ihnen die Stellungnahme der SSPH+ zur Totalrevision des Datenschutzgesetzes.

Besten Dank für Ihre Kenntnisnahme.

Mit freundlichen Grüssen
Sandra Nocera
--
Dr. Sandra Nocera
Head of Administration

SWISS SCHOOL OF PUBLIC HEALTH (SSPH+)
Hirschengraben 82
8001 Zurich
ph: +41 44 634 47 93
fax: +41 44 634 49 09
snocera@ssphplus.ch
www.ssphplus.ch

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Avis donné par

Nom / société / organisation : Swiss School of Public Health

Abréviation de la société / de l'organisation : SSPH+

Adresse : Hirschengraben 82, 8001 Zurich

Personne de référence : Sandra Nocera

Téléphone : +41 44 634 47 93

Courriel : snocera@ssphplus.ch

Date : 31.03.2017

Remarques importantes :

1. Nous vous prions de ne pas modifier le formatage de ce formulaire !
2. Utilisez une ligne par article, alinéa et lettre ou par chapitre du rapport explicatif.
3. Veuillez faire parvenir votre avis au **format Word** d'ici au 4 avril 2017 à l'adresse suivante : jonas.amstutz@bj.admin.ch

Nous vous remercions de votre collaboration!

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Table des matières

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Remarques générales

nom/société	remarque / suggestion :
SSPH+	La SSPH+ salue la volonté de réviser la loi fédérale sur la protection des données. Celle-ci est devenue non seulement nécessaire en raison du développement du droit international et communautaire, mais également en raison du développement des nouvelles technologies de l'information et de la communication. Il est par conséquent essentiel d'adapter le cadre légal applicable aux contraintes actuelles et futures.
SSPH+	De manière générale, l'avant-projet de révision de la LPD a été judicieusement conçu. La SSPH+ émet toutefois des réserves, en particulier en lien avec la protection des données relatives à la santé. Les données personnelles relatives à la santé constituent une catégorie de données particulièrement sensibles en tant qu'elles permettent, directement ou indirectement, de tirer des conclusions sur l'état de santé, physique, mental ou psychique d'une personne (MEIER, Protection des données, Berne 2011, N 486). Avec l'évolution de la science, les données collectées en lien avec la santé sont devenues de plus en plus pointues et intimes (ex. : encodage génétique). Par ailleurs, les méthodes de collectes et de stockage développées permettent aujourd'hui de traiter un nombre immense de données concernant la santé des individus. Accumulées, ces données peuvent être utilisées à de multiples fins (assurances, recherche scientifique, réseaux sociaux, habitudes de consommation, etc.) qui présentent un haut potentiel de nuisance pour les individus. Si les collectes de données sur la santé peuvent présenter des avantages pour la société (ex. : résultats de recherche bénéfiques), elles présentent aussi des risques de préjudices graves à l'égard des personnes dont les données sont collectées. Ainsi, le traitement illicite de données génétiques à des fins malveillantes est susceptible de mettre au ban de la société les personnes concernées. De tels agissements peuvent avoir des conséquences graves sur la vie des personnes concernées, en particulier du point de vue des assurances, du travail ou de la vie privée. Au regard de la nature et du nombre de données relatives à la santé qui sont aujourd'hui collectées, ainsi que des risques encourus par un traitement illicite de ces données, il est primordial d'encadrer strictement le traitement des données personnelles relatives à la santé. De ce point de vue, l'avant-projet de révision de la LPD devrait mieux prendre en compte les risques liés à cette question.
SSPH+	Le concept d'anonymisation des données doit être appréhendé de manière très prudente, en particulier en matière de données personnelles relatives à la santé. Avec le développement des techniques génétiques, il est actuellement aisé de relier un échantillon biologique à un individu. En d'autres termes, il n'est plus possible d'anonymiser des données génétiques. Ce qui est vrai pour le domaine génétique l'est par ailleurs de plus en plus pour les données physiologiques d'un patient. Grâce au développement des techniques d'analyse des données physiologiques, il est

	maintenant fréquemment possible de rattacher des données physiologiques à un patient. Ce constat appelle l'adoption de règles particulièrement protectrices en matière de traitement de données relatives à la santé et une prudence toute particulière lorsqu'il est fait recours à l'anonymisation. Par ailleurs, l'utilisation des *big data* remet sérieusement en cause le principe même d'anonymisation puisque ces techniques permettent, par recoupement, d'identifier un grand nombre d'individus sur la base d'informations banales et a priori anonymes.
SSPH+	A l'heure actuelle, les échantillons biologiques humains se trouvent en partie placés dans un vide juridique. Dans la mesure où ceux-ci ne font pas l'objet d'une recherche au sens de la LRH, leur traitement n'est pas réglé par la loi. Or, en pratique, les collectes et la conservation d'échantillons humains ne sont pas forcément réalisées dans un objectif de recherche, ou alors le sont sans objectif prédéterminés (différents types de biobanques). Inclure les échantillons biologiques dans le champ d'application de la LPD renforce la proposition de traiter à part les données de santé sous l'angle de la protection des données. L'occasion de la révision de la LPD pourrait être saisie pour combler ce vide juridique. Cela pourrait se traduire par une extension du champ d'application de la LPD aux échantillons biologiques dont la collecte et la conservation permettraient de tirer des données personnelles. Une telle extension permettrait de garantir une protection minimale en attendant l'adoption d'une loi fédérale sur les biobanques (cf. Motion 17.3170 de Rebecca Ruiz déposée le 16 mars 2017 au Conseil national).
SSPH+	En ce qui concerne le champ d'application territorial de la LPD, le Tribunal fédéral a admis une application assez large de la LPD pour des traitements illicites de données collectées en Suisse, commis depuis l'étranger. La révision de la LPD offre une occasion particulièrement propice d'inscrire clairement dans la loi que tout traitement illicite de données collectées en Suisse, même commis depuis l'étranger, est soumis à la LPD et peut être condamné en Suisse en application de cette loi. Cette proposition est d'autant plus importante que la question du *big data* demeure traitée de manière trop vague.
SSPH+	Du point de vue des sanctions, il est regrettable que l'avant-projet n'octroie pas au PFPDT un véritable pouvoir de punir les contrevenants à la LPD au moyen d'amendes administratives, à l'instar de ce que prévoit le Règlement UE 2016/679. Privilégier les sanctions pénales, comme le fait l'avant-projet, présente des inconvénients de taille. En effet, les sanctions pénales visent prioritairement les personnes physiques au sein des entreprises privées plutôt que les personnes morales elles-mêmes. Cela ouvre le champ à une impunité malvenue des entreprises qui traiteraient des données personnelles de manière illicite. Face à des entreprises aux capitaux importants, dont le business repose principalement sur les collectes de données (géants du net, réseaux sociaux, société spécialisée dans la médecine personnalisée ou le *big data*, etc.), il est primordial de se doter d'un cadre légal fort, assorti de sanctions importantes et dissuasives. Ainsi, il est nécessaire de doter le PFPDT d'un pouvoir de condamner les contrevenants à des amendes administratives d'un montant dans l'ordre de grandeur

	de ce que prévoit l'article 83 du Règlement (UE) 2016/679, à savoir des amendes administratives pouvant s'élever jusqu'à 20 millions d'euros, ou dans le cas d'entreprise, jusqu'à 4% du chiffre d'affaires mondial total de l'exercice précédent si ce montant dépasse 20 millions d'euros. En l'absence de sanctions administratives fortes, la Suisse pourrait rapidement devenir un paradis pour les sociétés souhaitant être soumises à des réglementations légères, avec le risque que les pays voisins de la Suisse considèrent que cette dernière ne bénéficie plus d'un niveau adéquat de protection. Cela pourrait s'avérer préjudiciable à la recherche en santé publique qui a besoin d'accéder à de larges quantités de données liées à la santé. Pour cela, il est indispensable que le public puisse avoir confiance dans le fait que la confidentialité de ses données est bien garantie.
SSPH+	La problématique du *big data* a probablement été sous-estimée dans l'avant-projet de révision de la LPD. Alors que le *big data* pose des questions nouvelles, l'avant-projet ne semble connaître aucune évolution majeure sur point, malgré les objectifs affichés dans le rapport explicatif. Dans les grandes lignes, l'avant-projet se contente en effet d'assimiler les activités liées au *big data* au profilage. Ce faisant, il n'apporte malheureusement pas de règles spécifiques à l'appréhension du *big data*. L'adoption de règles spécifiques dans ce domaine paraît pourtant judicieuse, car les principes généraux de la LPD ne semblent plus adéquats pour répondre aux défis posés par le *big data*. Par exemple, dans le contexte du *big data*, les collectes de données sont souvent menées sans que la finalité du traitement ne soit nécessairement connue. Cela pose des problèmes sérieux du point de vue du consentement des personnes concernées, dans la mesure où il n'est alors pas possible de leur offrir une information précise sur le but du traitement. Par ailleurs, toujours dans ce contexte, l'utilisation de données *a priori* anonymes (et donc non soumises à la LPD) permettent fréquemment, par recoupement, de procéder à l'identification d'une personne. Face à ce phénomène, il paraît donc judicieux de requestionner la notion même de données personnelles et d'examiner si le champ d'application matériel de la LPD ne devrait pas être redéfini. Parmi d'autres problématiques, le principe d'exactitude est également mis à mal avec l'utilisation des *big data*. Dans ce contexte, on fait en effet usage d'algorithmes pour identifier des corrélations de données. Les résultats aboutissent à des informations/données nouvelles liées à des personnes, qu'il n'est pas possible de vérifier dans la mesure où elles sont le résultat de probabilités ou d'interprétations (pour plus de détails sur les problématiques mentionnées ci-dessus, voir notamment : FANTI S., *Big data & protection des données dans le domaine de la santé*, in : SPRUMONT D. (édit.), Nouvelles technologies et santé publique, 22ème Journée de droit de la sa santé, Berne 2016 ; JACCARD *M., De la protection des données à la sécurisation des données connectées ?*, in : Regards de marathoniens sur le droit suisse, Mélanges publiés à l'occasion du 20ème « Marathon du droit », Genève 2015, p. 491 ss.) L'environnement des *big data* évolue rapidement et il est capital d'appréhender juridiquement ce phénomène avant qu'il ne s'impose « de fait ». En raison des dangers potentiels qui entourent une utilisation malveillante des *big data*, la révision de la LPD constitue une occasion qui doit être saisie pour mener une réflexion large sur cette question et adopter des règles adaptées aux contraintes nouvelles auxquelles nous devons aujourd'hui faire face. Il convient de ne plus attendre pour aborder la question.

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

SSPH+	On peut se demander si la LPD doit offrir une protection particulière aux données personnelles relatives à la santé ou si cette protection n'est pas déjà offerte par un certain nombre de lois spéciales. En effet, la future loi fédérale sur le dossier électronique sur le patient ou la future loi fédérale sur l'enregistrement des maladies oncologiques offrent des garanties de protection particulières aux données médicales. Par ailleurs, les données médicales sont protégées par le dispositions relatives au secret médical (not. : art. 321 et 320 CP, différentes lois fédérales sur les professions médicales, lois cantonales sur la santé) ou au secret de la recherche. Malgré le cadre légal existant, il est selon nous primordial que la loi fédérale sur la protection des données assure des garanties spécifiques de protection aux données personnelles relatives à la santé. En effet, les données relatives à la santé ne sont plus seulement collectées par des soignants, mais par un grand nombre de sociétés susceptibles de les utiliser à des fins commerciales (géants du net, assurances, etc.) par le biais des réseaux sociaux ou d'objet connectés notamment. Or, ces acteurs ne sont pas soumis aux dispositions sur le secret médical et collectent les données médicales d'individus sur la base d'un consentement souvent discutable. Par ailleurs, les risques encourus aujourd'hui par une utilisation illicite de données de la santé est susceptible de déboucher sur des préjudices toujours plus graves. Il est primordial que les personnes dont les données personnelles relatives à la santé sont collectées puissent garder un contrôle sur ces données. Or, à l'exception de la loi fédérale sur la protection des données, aucune loi fédérale ne protège ce type de données en tout type de situations. La loi fédérale sur le dossier électronique du patient ne s'applique en effet qu'aux communautés certifiées et seulement si le patient a souhaité constituer un dossier électronique. Par ailleurs, les règles applicables en matière de secret médical se bornent en grande majorité à punir la violation du secret, mais ne règlent pas les modalités de traitement des données médicales. La loi laisse ainsi subsister des lacunes importantes en matière de protection des données de la santé. En l'absence d'une loi fédérale sur la santé, cette question devrait être réglée de manière spécifique dans la LPD. La révision de la LPD devrait ainsi être saisie pour intégrer des considérations relatives à cette question. Il conviendrait dans ce sens d'évaluer la possibilité d'identifier les données de santé comme une catégorie à part dans la LPD au même niveau que les données sensibles. Cela permettrait de fixer, le cas échéant, un régime particulier pour ces données de santé qui tiennent compte des nombreuses lois spéciales en la matière (LDEP, LRMO, LAGH, LRH, etc).
SSPH+	Dans le cadre de la présente prise de position, l'absence de remarque sur une disposition ne vaut pas approbation de la part de la SSPH+.

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

nom/société	loi	art.	al.	let.	remarque / suggestion :
SSPH+	LPD	2			Dans sa jurisprudence « Google Street View » (ATF 138 II 346, c. 3), le Tribunal fédéral a appliqué la théorie des effets. Il a ainsi considéré la prise d'images en Suisse et la publication de celles-ci de façon à pouvoir être utilisées en Suisse créaient un point de rattachement prépondérant avec la Suisse, mêmes lorsque ces images étaient traitées depuis l'étranger. Dans ce cas, le Tribunal fédéral a reconnu l'application de la LPD ainsi que la compétence du Préposé fédéral à la protection des données (PFPDT). L'occasion devrait être saisie ici de codifier clairement cette pratique et de la renforcer. Il serait ainsi bienvenu de soumettre le traitement de toutes les données collectées en Suisse à la LPD et au pouvoir de contrôle du PFPDT. Une telle réglementation permettrait d'éviter les hésitations relatives au critère du « rattachement prépondérant » et encouragerait les collecteurs de données étrangers à agir en conformité avec la LPD. Nous proposons la modification suivante de l'article 2 al. 1 LPD : « *La présente loi régit le traitement de données concernant des personnes physiques,* ***collectées en Suisse ou à partir de la Suisse****, effectué par : (…)* » Nous proposons par ailleurs d'étendre le champ d'application de la loi aux échantillons biologiques, dans la mesure où ils sont collectés et conservés de telle sorte qu'il est possible d'en tirer des données personnelles. Un alinéa 1bis pourrait être ajouté avec la teneur suivante : « *^{1bis} Elle régit également la collecte et la conservation de matériel biologique humain dans la mesure où il est possible d'en tirer des données personnelles. Sont réservées les dispositions de la loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain.* »

SSPH+	LPD	5			Le transfert de la compétence de déterminer si une législation assure un niveau protection adéquat en faveur du Conseil fédéral (et non plus au maître du fichier) est à saluer.
SSPH+	LPD	10			Il est indispensable que les organismes suisses ou étrangers qui traitent à grande échelle des données sur la santé collectées en Suisse soient soumis à une forme de contrôle. La certification obligatoire semble être l'instrument le plus adapté pour assurer ce contrôle. Elle permet en effet d'assurer que toutes les personnes soumises à la certification, suisses ou étrangères, prennent connaissance et respectent les dispositions réglementaires applicables au traitement de données de santé, en particulier lors de la collecte de telles données. Le cercle des personnes ou institutions soumises à l'exigence de certification obligatoire devrait toutefois être soigneusement déterminé. Il faudrait en effet éviter de soumettre les cabinets médicaux ou les hôpitaux à l'exigence de certification. Il serait également judicieux d'exempter d'une telle obligation les personnes privées ou organes fédéraux qui sont amenées, de par la loi, à traiter des données sur la santé. On vise notamment ici les assurances maladies. Toutes les autres personnes ou institutions, à l'instar des entreprises qui collectent des informations sur la santé de personnes ou autres hébergeurs de données sur la santé, seraient soumis à une obligation de certification. Nous proposons ainsi l'ajout d'un article 10 al. 1bis dont la teneur pourrait être la suivante : « *[1bis] Le traitement de données sur la santé est soumis à une certification obligatoire. Sont exemptés d'une telle certification :* *a. les professionnels de la santé au bénéfice d'une autorisation de pratique à titre indépendant;* *b. les institutions de santé au bénéfice d'une autorisation d'exploitation ;* *c. les organisations qui, de par la loi, sont amenées à traiter des données sur la santé.* »
SSPH+	LPD	18			**La SSPH+ salue l'introduction d'un devoir de protection des données dès la conception et par défaut. Cette disposition doit absolument être maintenue.**

SSPH+	LPD	30			Il serait bienvenu de préciser que la personne qui s'oppose à la communication de données personnelles par l'organe fédéral ne subira pas de conséquences négatives du simple fait de cette opposition.
SSPH+	LPD	**51a**			L'avant-projet en consultation ne comprend de sanctions administratives propres à dissuader les entreprises actives dans le domaine. Nous proposons ainsi d'adopter une disposition analogue à celle de l'art. 83 du Règlement (UE) 2016/679 sur la protection des données et dont les sanctions devraient être analogues, à savoir ***Art. 51a Sanctions administratives*** *Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 CHF ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu:* - *…* - *…* -

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2016/680 relative à la protection des données personnelles traitées à des fins de poursuite pénale ou d'entraide en matière pénale

nom/société	remarque / suggestion :
SSPH+	

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

nom/société	remarque / suggestion :
SSPH+	

Rapport explicatif : chap. 8 « Commentaire des dispositions »

nom/société	art.	remarque / suggestion :
SSPH+		

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz BJ
Bundesrain 20
3003 Bern

Per Mail: jonas.amstutz@bj.admin.ch

Bern, 28. März 2017

Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz: Vernehmlassung

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, zur oben genannten Vernehmlassung Stellung nehmen zu können. Der Schweizerische Städteverband vertritt die Städte, städtischen Gemeinden und Agglomerationen in der Schweiz und damit gut drei Viertel der Schweizer Bevölkerung.

Allgemeine Einschätzung

Die Mitglieder des Schweizerischen Städteverbandes begrüssen die Totalrevision des Datenschutzgesetzes ausdrücklich. Kommentare zu den einzelnen Punkten entnehmen Sie bitte dem beigefügten Formular.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Schweizerischer Städteverband

Präsident

Kurt Fluri, Nationalrat
Stadtpräsident Solothurn

Direktorin

Renate Amstutz

Kopie Schweizerischer Gemeindeverband

Monbijoustrasse 8, Postfach, 3001 Bern
Telefon +41 31 356 32 32
info@staedteverband.ch, www.staedteverband.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schweizerischer Städteverband

Abkürzung der Firma / Organisation : SSV

Adresse : Postfach, Monbijoustrasse 8, 3001 Bern

Kontaktperson : Julia Imfeld

Telefon : 031 356 32 32

E-Mail : julia.imfeld@staedteverband.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Städteverband	Die Mitglieder des Schweizerischen Städteverbandes begrüssen die Totalrevision des Datenschutzgesetzes ausdrücklich. Die Anpassung des schweizerischen Rechtes an die rasante technologische Entwicklung bedingt eine wesentliche Stärkung des Datenschutzes.
Städteverband	Das revidierte Datenschutzrecht bildet durch die Übernahme des europäischen Rechtsrahmens Basis dafür, dass Schweizer Unternehmen auf dem europäischen Markt wettbewerbsfähig bleiben und unnötige Hemmnisse für die Bearbeitung und den Austausch von Daten verhindert werden können. Die Mitglieder des Städteverbandes sehen in einem starken Datenschutz denn auch keinen Wettbewerbsnachteil für die Schweiz, sondern vielmehr einen Standortvorteil. Voraussetzung dafür ist jedoch, dass den betroffenen Unternehmen genügend Vorlaufzeit eingeräumt wird und sie die nötige Unterstützung bei der Umsetzung der neuen Vorschriften erhalten.
Städteverband	Der Städteverband schliesst sich grundsätzlich der Vernehmlassungsantwort der Vereinigung der schweizerischen Datenschutzbeauftragten, Privatim, vom 9.März 2017 an.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Städteverband	DSG	3		a/c	In der Praxis zeigt sich, dass es für Personendaten, die nicht in die Kategorie der besonders schützenswerten Personendaten (Lit. c) gehören, keinen gesetzlichen Begriff gibt. Wir regen deshalb an, den bereits weitgehend genutzten Begriff «gewöhnliche Personendaten» ins Gesetz aufzunehmen.
Städteverband	DSG	3		c	Wir regen an, die Liste um die Kategorie «Daten über Minderjährige» zu ergänzen, um die Rechtslage etwa in Ausbildungsbetrieben und Schulen für die inhärent schwächere Partei zu verbessern.
Städteverband	DSG	13 ff.			Die Verschärfung der Informationspflicht wird von den Mitgliedern des Städteverbandes positiv bewertet.
Städteverband	DSG	13	1		Die Sanktionierung (in Verbindung mit Art. 50 Abs. 1 lit. a und b VE-DSG) soll auch bei der Videoüberwachung durch Private zur Anwendung kommen. Es stellt sich durchaus die Frage, ob die vorgeschlagene Regelung auch tatsächlich dazu führt, dass eine unzulässige Videoüberwachung des öffentlichen Raumes durch Private entsprechend strafrechtlich sanktioniert wird. Die vorgenannten Bestimmungen zeigen u.E. betroffenen Privatpersonen unzureichend auf, dass sie sich mit dem Einsatz ihrer Geräte strafbar machen. Der Städteverband beantragt daher, einen eindeutigen Strafbestand zu schaffen, um der Praxis zunehmender Videoüberwachung des öffentlichen Grundes durch Private entgegenzuwirken.
Städteverband	DSG	14	2	b	Das Entfallen der Informationspflicht, wenn die Information nachweislich nicht oder nur mit unverhältnismässigem Aufwand möglich ist, erscheint uns problematisch. Aus Sicht des Städteverbandes genügt es nicht, dass im erläuternden Bericht festgehalten ist, dass diese Bestimmung restriktiv ausgelegt werden muss. Ausserdem können die betroffenen Personen die Datenbearbeitung nur anfechten, wenn sie von dieser per Zufall erfahren, hier wäre möglicherweise eine Mitteilungspflicht an die zuständige Datenschutzbehörde sinnvoll.

Städteverband	DSG	15	2		Die Ausnahme, wodurch die Informations- und Anhörungspflicht nicht gilt, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht, ist unglücklich formuliert, da dies suggeriert, dass bei automatisierten Verfügungen den Betroffenen kein rechtliches Gehör gewährt werden muss. Eine solche Auslegung widerspräche indes in fundamentaler Weise den allgemeinen Verfahrensgarantien von Art. 29 BV.
Städteverband	DSG	16			Die Stossrichtung ist zu begrüssen, da auch auf Bundesebene die Frage der rechtlichen Zulässigkeit der Bearbeitung von Daten mit den Grundrechten verknüpft ist. Insbesondere bedeutet dies, dass unter den genannten Bedingungen die Bearbeitung von Daten, deren Personenbezug nicht offensichtlich ist (beispielsweise anonymisierte Daten) in den Geltungsbereich des DSG zurückgeholt werden können. Allerdings sorgt die Konstruktion im Zusammenspiel mit Art. 27 VE für eine gewisse Verwirrung, da insbesondere nicht klar ist, ob sich die Ausnahme in Art. 27 Abs. 2 Bst. b VE jeweils auf das ursprüngliche Risiko oder auf das Restrisiko nach der Anordnung von sichernden Massnahmen bezieht. Es bleibt unklar, zu welchem Zweck gemäss Art. 16 eine Folgeabschätzung durchgeführt wird.
Städteverband	DSG	18			Die Mitglieder des Städteverbandes erachten es als wichtig, dass die Verantwortung für den Datenschutz nicht ausschliesslich bei den Bürgerinnen und Bürgern liegen soll. Die vorgesehene Verpflichtung der Hersteller, den Datenschutz bereits bei der Konzeption und Entwicklung von Produkten und Anwendungen zu beachten und werkstellige Voreinstellungen immer dem höchstmöglichen Datenschutzniveau anzupassen, wird deshalb ausdrücklich begrüsst.
Städteverband	DSG	20 ff.			Die Änderungen im Bereich Auskunftspflicht werden ebenfalls begrüsst.
Städteverband	DSG	51			Der vorgesehene Paradigmenwechsel bei den Sorgfaltspflichten findet bei den Mitgliedern des Städteverbandes Unterstützung.
Städteverband	ZPO	113	2	g	Effektiver Datenschutz soll nicht nur auf dem Papier bestehen, sondern auch effektiv und wirkungsvoll durchgesetzt werden. Ob der Verzicht auf die Erhebung von Gerichtskosten hierfür ausreicht, ist u.E. zumindest fraglich. Im Falle eines Unterliegens, sind die anfallenden Parteikosten für eine einzelne Person kaum tragbar. Bedauert wird, dass geeignete Mittel wie das Instrument der Sammelklage oder die Beweislastumkehr nicht in die Vorlage aufgenommen sind.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Städteverband	Keine Bemerkungen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Städteverband	Keine Bemerkungen

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Städteverband		Keine Bemerkungen

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Städteverband		Keine Bemerkungen

Amstutz Jonas BJ

Von: Michel Heeb Astrid (SST) <Astrid.Michel@zuerich.ch>
Gesendet: Dienstag, 4. April 2017 11:19
An: Amstutz Jonas BJ
Betreff: Vernehmlassung Totalrevision des Datenschutzgesetzes
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_der_STSTK.doc

Sehr geehrte Damen und Herren

Im Auftrag der Städtischen Steuerkonferenz sende ich Ihnen die Antwort zu dieser Vernehmlassung.

Freundliche Grüsse
Astrid Michel Heeb
Direktionsassistentin

Direktwahl +41 44 412 33 26
Direktfax +41 44 412 37 96
astrid.michel@zuerich.ch

Stadt Zürich
Steueramt
Direktion
Werdstrasse 75
Verwaltungszentrum Werd
Postfach, 8010 Zürich

Telefon +41 44 412 33 11
Fax +41 44 212 17 03
http://www.stadt-zuerich.ch/steueramt

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Städtische Steuerkonferenz

Abkürzung der Firma / Organisation : STSTK

Adresse : c/o Steueramt der Stadt Zürich, Werdstrasse 75, 8004 Zürich

Kontaktperson : Herr Dr. Bruno Fässler

Telefon : 044 412 33 00

E-Mail : bruno.faessler@zuerich.ch

Datum : 31.03.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Städtische Steuerkonferenz	Auch wenn die Städtische Steuerkonferenz nicht in der Liste der Vernehmlassungsadressaten aufgeführt ist, hat sie sich dennoch dazu entschieden, eine kurze Stellungnahme zur Totalrevision des Bundesdatenschutzgesetzes, in concreto zum abzuschaffenden Art. 19 Abs. 3 DSG, zu verfassen. Die städtischen Steuerämter sind im Rahmen ihrer Tätigkeit immer wieder mit Fragen zum Abrufverfahren konfrontiert. Die diesbezüglichen Regelungen auf kantonaler Ebene sind teilweise unklar und wenig kohärent. Eine Anpassung auf Bundesebene dürfte voraussichtlich auch auf die kantonalen Entwicklungen einen nicht unmassgeblichen Einfluss haben und auch die städtischen Steuerämter in ihrer täglichen Arbeit betreffen. Wir danken bereits im Vorfeld für die Berücksichtigung unserer Stellungnahme
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Städtische Steuerkonferenz	DSG	19	3		Auf Basis von Art. 19 Abs. 3 DSG ist für die Datenbekanntgabe im Abrufverfahren eine spezifische gesetzliche Grundlage erforderlich. Die Totalrevision des Bundesdatenschutzgesetzes sieht neben zahlreichen weiteren Neuerungen nun die Abschaffung von Art. 19 Abs. 3 DSG vor. Dies wird insbesondere damit begründet, dass das Erfordernis einer spezifischen gesetzlichen Grundlage für die Datenbekanntgabe im Abrufverfahren dem technologieneutralem Charakter des Datenschutzgesetzes widerspreche. Die Städtische Steuerkonferenz teilt die bereits in der Botschaft zum Bundesdatenschutzgesetz geäusserte Auffassung, dass ein Datenschutzgesetz nicht den Zweck hat, «die Entwicklungsmöglichkeiten im Bereich der Informationstechnologien zu verhindern oder einzuschränken», sondern dass vielmehr gewisse Leitplanken für die Datenbearbeitung zu setzen sind, «die garantieren, dass die Entfaltung der Persönlichkeit nicht durch unnötige und unerwünschte Informationstätigkeiten beeinträchtigt wird» (vgl. BBl 1988 II 417-418). Aus aktuellem Anlass hat sich die Städtische Steuerkonferenz dazu entschlossen, sich im Rahmen dieser Vernehmlassung auf die Frage der Notwendigkeit einer gesetzlichen Grundlage für die Datenbekanntgabe im Abrufverfahren zu beschränken. Dabei beziehen sich die Ausführungen ausschliesslich auf die Datenbekanntgabe unter Behörden. Die Frage der Notwendigkeit einer gesetzlichen Grundlage für die Datenbekanntgabe im Abrufverfahren war in den vergangenen Jahren immer wieder Gegenstand von Diskursen und Auseinandersetzungen. Während verschiedene Kantone das Erfordernis einer gesetzlichen Grundlage in ihren Datenschutzgesetzen vorsehen, haben andere, so der Kanton Zürich, in ihrer Datenschutzgesetzgebung auf eine entsprechende Regelung verzichtet. Insbesondere mit Verweis auf die Notwendigkeit einer gesetzlichen Grundlage auf Bundesebene sowie mit dem erhöhten Risiko von Grundrechtsverletzungen durch die Datenbekanntgabe im Abrufverfahren wurde jedoch auch im Kanton Zürich vereinzelt die Forderung nach einer spezifischen gesetzlichen Grundlage für die Datenbekanntgabe im Abrufverfahren laut. Argumentiert wurde insbesondere damit, dass im Rahmen der Datenbekanntgabe im Abrufverfahren

					die datenbesitzende Stelle jedwede Prüfungsbefugnis betreffend einen gerechtfertigten oder ungerechtfertigten Datenzugriff aus der Hand gibt. Die Städtische Steuerkonferenz vertritt die Ansicht, dass der durch das Datenschutzgesetz gewährleistete Schutz technologieneutral sein muss und insbesondere nicht von der Art der Datenbekanntgabe abhängen kann. Unter einem Abrufverfahren versteht man ein automatisches Verfahren, welches es den informationssuchenden Organen ermöglicht, sich die gewünschten Informationen selbst anhand eines Datenbestands ohne Mitwirkung der datenbesitzenden Stelle zu beschaffen. Bei der Datenbekanntgabe im Abrufverfahren handelt es sich um eine Bekanntgabe im Sinne von Art. 17 DSG. Eine solche ist dann möglich ist, wenn eine Rechtsgrundlage im Sinne von Art. 17 DSG besteht, die zur Datenbearbeitung legitimiert, oder wenn einer der weiteren Fälle von Art. 19 Abs. 1 DSG gegeben ist. Hierbei ist zu beachten, dass der Zugriff jeweils nur im Umfang des zugrundeliegenden Gesetzes erfolgen darf. Die Möglichkeit einer Datenbekanntgabe im Abrufverfahren legitimiert die zugreifende Behörde indes nicht, bedingungslos und vollumfänglich Zugriff auf jedwede Daten von jedermann zu nehmen. Die Frage, ob eine Datenbekanntgabe im Abrufverfahren das Risiko eines Grundrechtseingriffs erhöht, soll im Folgenden anhand verschiedener Konstellationen betrachtet werden. Diese Vernehmlassung beschränkt sich dabei auf die Betrachtung von «einfachen» Personendaten und bezieht sich insbesondere nicht auf die Bekanntgabe besonders schützenswerter Personendaten im Abrufverfahren. **Unbedingte Pflicht zur Datenbekanntgabe:** In gewissen Fällen sind Behörden gegenüber anderen Behörden ohne weitere Voraussetzungen zur Auskunft verpflichtet. Diese Verpflichtung gilt unbedingt und ist insbesondere nicht von einer vorgängigen Prüfung eines etwaigen zugrundeliegenden rechtlichen Interesses an der Datenbekanntgabe durch die angefragte oder auskunftspflichtige Behörde abhängig. Nach Auffassung der Städtischen Steuerkonferenz kann in Fällen, in denen eine unbedingte Pflicht zur Datenbekanntgabe besteht, diese ohne dass das Risiko eines Grundrechtseingriffs erhöht würde auch im Rahmen eines Abrufverfahrens stattfinden. In einer solchen Konstellation vergrössert sich die Gefahr einer Grundrechtsverletzung bereits deshalb nicht, da der datenbesitzenden Stelle ohnedies keine Prüfungsbefugnis zukommt, sondern der

					Gesetzgeber vielmehr bereits im Voraus eine Prüfung bzw. Interessenabwägung vorgenommen hat. Ein Beispiel, in dem eine unbedingte Pflicht zur Datenbekanntgabe besteht, ist die Ausgabe von Steuerausweisen im Kanton Zürich. Hier hat der Gesetzgeber eine grundsätzliche Öffentlichkeit vorgesehen und so bereits im Vorfeld eine Abwägung zwischen dem Einsichts- und dem Geheimhaltungsinteresse getroffen, so dass dem Steueramt als auskunftserteilende Behörde eine Interessenabwägung von vornherein verwehrt ist. Der auskunftserteilenden Behörde ist es nicht möglich, gegenüber anderen Behörden den unmittelbaren und unbedingten Auskunftsanspruch einzuschränken. In einer derartigen Konstellation betrifft das Abrufverfahren lediglich die Art bzw. Technik der Datenbekanntgabe. Zu klären wären vorrangig jedoch allfällige technischen Fragen. Gegebenenfalls wäre durch die datenbesitzende Stelle sicherzustellen, dass die Datenbezüger im Rahmen des Abrufverfahrens lediglich auf jene Informationen zugreifen können, die der Gesetzgeber im Rahmen des Steuerausweises vorgesehen hat, in dieser konkreten Konstellation also auf das aktuelle steuerbare bzw. satzbestimmende Einkommen und Vermögen. Es wäre jedoch auch denkbar, die Verantwortung dahingehend, dass der Zugriff lediglich auf die gesetzlich vorgesehenen Informationen erfolgt, den datenbeziehenden Stellen auferlegt würde. Sämtliche über die gesetzlich vorgesehenen Daten hinausgehenden Informationen wären von der zugrunde gelegten gesetzlichen Grundlage nicht mehr gedeckt, ein Zugriff auf die weiteren Daten wäre somit rechtswidrig und zumindest aufsichtsrechtlich zu ahnden. Die bestehenden gesetzlichen Grundlagen liefern bereits einen hinreichenden Schutz vor allfälligem missbräuchlichem Datenbezug. **Bedingte Pflicht zur Datenbekanntgabe:** In gewissen Fällen sieht das Gesetz vor, dass eine Auskunft nur unter gewissen Umständen erfolgen darf. So sieht Art. 91 SchKG eine Auskunftspflicht von Behörden gegenüber den Betreibungsämtern im Pfändungsverfahren vor. In derartigen Konstellationen besteht im Rahmen eines Abrufverfahrens möglicherweise das Risiko, dass die datenabrufende Behörde auch ausserhalb der gesetzlich vorgesehenen Umstände auf die Daten zugreift. Dieses Risiko bestünde jedoch auch dann, wenn eine weitere gesetzliche Grundlage die Bekanntgabe der Daten im Rahmen des Pfändungsverfahrens im Abrufverfahren regeln würde. In jedem Fall sind die Betreibungsämter nur zum Zugriff auf jene von Art. 91 SchKG Abs. 5 SchKG umfassten Daten legitimiert. Da ein darüber hinausgehender Datenbezug den Betreibungsämtern bereits auf Basis von Art. 91 SchKG nicht gestattet ist, würde das Betreibungsamt im Falle eines Abrufs von nicht von Art. 91 Abs. 5 SchKG gedeckten Daten ausserhalb der gesetzlichen

					Legitimation handeln, ganz gleich, ob dieses Handeln im Rahmen eines Abrufverfahrens oder im Rahmen einer Anfrage erfolgen würde. Die zugrundeliegende gesetzliche Grundlage im Sinne von Art. 17 DSG gewährleistet somit bereits einen hinreichenden Schutz. Nach Auffassung der Städtischen Steuerkonferenz ist auch in Fällen einer bedingten Pflicht zur Datenbekanntgabe eine solche über ein Abrufverfahren denkbar, wenn im Rahmen von Vereinbarungen etc. sichergestellt wird, dass die entsprechenden Behörden nur im Rahmen des gesetzlich Vorgegebenen agieren. **Einwilligung im Einzelfall durch die betroffene Person:** In gewissen Konstellationen können Daten dann weiteregegeben werden, wenn die betroffene Person im Einzelfall eingewilligt hat (vgl. Art. 19 Abs. 1 lit. b DSG). Fraglich ist, ob ein Zugriff in einem derartigen Fall auch im Abrufverfahren denkbar wäre und ob eine gesetzliche Grundlage allenfalls geeignet bzw. notwendig wäre, (um) das Risiko von Grundrechtseingriffen zu minimieren. Nach Auffassung der Städtischen Steuerkonferenz lässt die erwähnte Konstellation nur Zugriff auf solche Daten zu, die von der Einwilligung der betroffenen Person gedeckt sind. Würde eine Behörde auf weitere als die von der Einwilligung gedeckten Daten im Rahmen eines Abrufverfahrens zugreifen oder auf Daten solcher Personen zugreifen, die keine Einwilligung gegeben haben, so wäre dies ein Verstoss gegen Art. 19 Abs. 1 lit. b DSG und damit ein widerrechtliches Bearbeiten von Personendaten. Eine spezifische gesetzliche Grundlage zum Abrufverfahren könnte dieses Risiko nicht minimieren, da Art. 19 Abs. 1 lit. b DSG bereits klarstellt, dass nur auf die Daten zugegriffen werden darf, die von der Einwilligung des Betroffenen umfasst sind. Missbraucht die Amtsperson seine Befugnis und greift über Gebühr auf weitere Daten zu, so wäre dieses Verhalten von den gesetzlichen Bestimmungen nicht gedeckt und zumindest aufsichtsrechtlich relevant. Nach Auffassung der städtischen Steuerkonferenz sind mit den gesetzlichen Vorgaben von Art. 17 und Art. 19 Abs. 1 DSG die Anforderungen an das Legalitätsprinzip betreffend die Datenbekanntgabe gewahrt und es bedarf keiner weiteren spezifischen gesetzlichen Grundlage für die Datenbekanntgabe im Abrufverfahren. Die Regelungen über die Datenbekanntgabe selbst halten klar fest, welche Art von Informationen die betroffenen Amtsstellen in welchem Umfang einsehen können. In Konstellationen, in denen dem bekannt gebenden Organ eine spezifische Prüfungspflicht zukommt, ist eine Bekanntgabe im Abrufverfahren eher schwer vorstellbar, da die bekannt gebende Behörde in einem

					Abrufverfahren ihrer Prüfungspflicht nicht nachkommen könnte. Denkbar wäre jedoch, dass eine abstrakte Prüfung einzelner Fallgruppen im Vorfeld stattfindet und eine Zugriffsberechtigung nur für bestimmte Konstellationen erteilt wird. Ein Risiko von Grundrechtseingriffen wäre auch in einer derartigen Konstellation lediglich dann gegeben, wenn die abrufende Behörde über ihre Legitimation hinausgehend Daten abrufen würde. Hierbei würde es sich jedoch ebenfalls um ein widerrechtliches Verhalten der Behörde mit zumindest aufsichtsrechtlichen Konsequenzen handeln. Die Städtische Steuerkonferenz weist zudem darauf hin, dass die Datenbekanntgabe im Abrufverfahren nach ihrer Auffassung sogar dazu beitragen kann, allfällige Grundrechtseingriffe zu vermeiden. Sie gewährleistet beispielsweise, dass anders als im Rahmen von Einzelanfragen die Anonymität der Person, auf welche zugegriffen wird, gewahrt bleibt. Zudem trägt sie dazu bei, dass den verschiedenen Behörden kohärente und aktuelle Informationen vorliegen und trägt somit zu einer rechtsgleichen Behandlung auf behördlicher Ebene bei. Abschliessend sei erwähnt, dass sich die Städtische Steuerkonferenz zwar auf den Standpunkt stellt, dass auf das Erfordernis einer spezifischen gesetzlichen Grundlage für die Datenbekanntgabe im Abrufverfahren verzichtet werden kann, dass jedoch – möglicherweise auf Verordnungsebene – gewisse Anforderungen an Ausgestaltung, Sicherheit, Aufsicht und Verfahren betreffend die Datenbekanntgabe im Abrufverfahren festgelegt werden sollten. Nur so lässt sich vermeiden, dass aufgrund einer undurchdachten oder unsicheren Gestaltung von Abrufverfahren ein neues Risiko von Grundrechtsverletzungen entsteht.
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht					

gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden	

werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler!		

Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Amstutz Jonas BJ

Von: Bernhard Wittweiler <bernhard.wittweiler@suisa.ch>
Gesendet: Freitag, 31. März 2017 12:14
An: Amstutz Jonas BJ
Betreff: Stellungnahme zum VE DSG
Anlagen: DSG_Vernehml_VE-2016-12_17-4-4.doc

Sehr geehrter Herr Amstutz

In der Beilage senden wir Ihnen unsere Stellungnahme zum Vorentwurf eines neuen Datenschutzgesetzes.

(See attached file: DSG_Vernehml_VE-2016-12_17-4-4.doc)

Freundliche Grüsse

Bernhard Wittweiler
Leiter Rechtsdienst

SUISA
Genossenschaft der Urheber und Verleger von Musik

Bellariastr. 82, Postfach, CH-8038 Zürich
T +41 44 485 66 66, F +41 44 483 06 66
bernhard.wittweiler@suisa.ch, www.suisa.ch | www.suisablog.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von SUISA

Name / Firma / Organisation : SUISA, Genossenschaft der Urheber und Verleger von Musik

Abkürzung der Firma / Organisation : SUISA

Adresse : Bellariastrasse 82, Postfach, 8038 Zürich

Kontaktperson : Bernhard Wittweiler, Leiter Rechtsdienst

Telefon : 044 485 65 40

E-Mail : bernhard.wittweiler@suisa.ch

Datum : 31. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SUISA	Obwohl wir der Auffassung sind, dass das bestehende Datenschutzrecht grundsätzlich genügt, anerkennen wir das Bedürfnis, die internationalen Rechtsentwicklungen – die Revision der Europarats-Konvention 108 (E-SEV 108) sowie die EU-Datenschutz-Grundverordnung 2016/679 (DSGVO) und die EU-Richtlinie 2016/680 (RL 2016/680) – im Schweizer Recht nachzuvollziehen. Erstgenannte Aussage bedeutet, dass man sich beim Nachvollzug an die internationalen Vorgaben halten und nicht ohne zwingende Notwendigkeit darüber hinausgehen sollte. Dieses Ziel ist mit dem Vorentwurf (VE) über weite Strecken erreicht worden. Positiv zu würdigen ist auch, dass der VE einige unsinnige Regelungen des europäischen Rechts nicht übernommen hat. Doch leider hält sich der VE nicht ganz an die erwähnte Devise. Einmal mehr ist an einigen Stellen ein fataler Hang zu einem „Swiss Finish“ zu erkennen, der unnötig und kontraproduktiv ist. Nach dem Erläuternden Bericht wollte man Überregulierung vermeiden – ein Ziel, das nur teilweise erreicht worden ist. Wir werden bei den Bemerkungen zu den einzelnen Bestimmungen darauf zurückkommen. Die vorgeschlagene Revision des Datenschutzes besteht vor allem aus vielen neuen öffentlich-rechtlichen Pflichten, über deren Einhaltung der Beauftragte wacht, und bei deren blosser Nichteinhaltung man sanktioniert wird, unabhängig davon, ob die Persönlichkeit der betroffenen Person verletzt worden ist oder nicht. Damit führt die Revision vor allem zu einer weiteren Bürokratisierung des Datenschutzes, und dessen eigentlicher Sinn und Zweck drohen unterzugehen. Abgesehen von dieser grundsätzlichen Kritik ist eine Reihe von nicht durchdachten, unnötigen und teilweise kontraproduktiven Bestimmungen festzustellen, siehe unsere untenstehenden Bemerkungen zu den einzelnen Bestimmungen. Entschieden abzulehnen ist der völlig verfehlte Systemwechsel bei der Aufsicht und den Sanktionen. Alles in allem bedarf der VE in einigen Punkten einer gründlichen Überarbeitung. Zu den vorgeschlagenen Änderungen im Zusammenhang mit Schengen (RL 2016/680 und deren Umsetzung, v.a. im StGB) äussern wir uns nicht, soweit das DSG nicht betroffen ist.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SUISA	DSG	2	1		Die Beschränkung des Geltungsbereichs des Datenschutzes auf Daten von natürlichen Personen begrüssen wir ausdrücklich.
SUISA	DSG	5	2 + 7		Neu sollen nicht mehr die Verantwortlichen selber abklären und entscheiden (und dafür auch die Verantwortung übernehmen) müssen, ob ein bestimmter Staat einen angemessenen Datenschutz gewährleistet, sondern sie können sich auf die entsprechenden publizierten Vorgaben des Bundesrates abstützen. Diese Neuerung ist zu begrüssen, denn sie führt zu einer erheblichen Erhöhung der Rechtssicherheit.
SUISA	DSG	5	3	b + c	Unklar ist der Unterschied zwischen den „spezifischen Garantien“ und den „verbindlichen unternehmensinternen Datenschutzvorschriften“. Die Unklarheit hat umso gravierendere Auswirkungen, als erstere dem Beauftragten nur notifiziert, letztere jedoch von ihm genehmigt werden müssen.
SUISA	DSG	5	5		Die Genehmigungsfrist von 6 Monaten ist viel zu lang. Sie kann ausserdem fast beliebig verlängert werden, weil der Beauftragte immer wieder neue Unterlagen anfordern kann. Die Frist sollte auf höchstens 2 Monate begrenzt werden.
SUISA	DSG	5	6		Nicht einzusehen ist, was die in Satz 1 vorgesehene Informationspflicht über den Einsatz von vom Beauftragten ausgestellten oder anerkannten standardisierten Garantien zu einem wirksamen Datenschutz beizutragen vermag. Diese Pflicht ist in der DSGVO nicht vorgesehen und sollte gestrichen werden.
SUISA	DSG	6	1	c/2	Die durch die Ergänzung des Wortlauts um die „Verwaltungsbehörden“ beabsichtigte Erweiterung dieser Bestimmung ist zu begrüssen. Allerdings ist absehbar, dass die Auslegung des Begriffs, namentlich wenn es um ausländische Behörden geht, zu unfruchtbaren Kontroversen führen wird. Wir empfehlen

					diesbezüglich eine Angleichung an Art. 49 Abs. 1 lit. e DSGVO: Streichung der Begriffe „vor einem Gericht oder einer Verwaltungsbehörde“ und Ersatz des Wortes „unerlässlich“ im Ingress durch „erforderlich“.
SUISA	DSG	6	2		Diese Meldepflicht zwingt die Rechtsunterworfenen zur Bekanntgabe u.U. sensibler Informationen über Vertragsinhalte, Gerichtsverfahren, Untersuchungen usw., die nach dem Öffentlichkeitsgesetz für jedermann einsehbar sind, was wiederum datenschutzrechtlich höchst fragwürdig ist. Die Kautelen zum Schutz von Geheimnissen sind unzureichend. Salopp ausgedrückt schiesst sich der Datenschutz damit selbst ins Bein. Wir empfehlen, diesen Absatz zu streichen.
SUISA	DSG	8/9			Die Beibehaltung des prinzipienbasierten Regelungsansatzes im Datenschutz durch den VE ist grundsätzlich zu begrüssen. Doch dieser Ansatz hat auch seine Schattenseiten: Die Prinzipien des Datenschutzes im geltenden DSG und auch im VE sind sehr allgemein und vage gehalten, was eine ausserordentlich grosse Rechtsunsicherheit zur Folge hat. Es gibt kaum ein Rechtsgebiet mit systembedingt grösserer Rechtsunsicherheit als den Datenschutz. Folglich sind Vorkehren, welche den Datenschutz konkretisieren und die Rechtsunsicherheit reduzieren, im Prinzip willkommen zu heissen. Solche Vorkehren sieht der VE mit den Empfehlungen der guten Praxis vor, die der Beauftragte entweder selbst aufstellen kann oder genehmigt. Wie erwähnt ist das prinzipiell positiv zu würdigen. Doch die im VE vorgeschlagene Umsetzung dieses Instruments ist in hohem Masse problematisch, und das aus mehreren Gründen: Nach dem Wortlaut von Art. 9 Abs. 1 VE wird implizit die Fiktion der Datenschutzkonformität der Empfehlungen aufgestellt, die auch für die Gerichte bindend wäre (entgegen dem Erläuternden Bericht). Die Empfehlungen unterliegen keiner rechtsstaatlichen Kontrolle: Die Überprüfung im Einzelfall ist infolge der Fiktion ausgeschlossen; die vom Beauftragten selbst aufgestellten Empfehlungen sind nach VE nicht anfechtbar; unklar ist, ob die Genehmigung bzw. deren Ablehnung der von Dritten aufgestellten Empfehlungen durch den Beauftragten in Form einer anfechtbaren Verfügung ergeht oder ob eine solche verlangt werden kann. Hinzu kommt, dass das Amt des Beauftragten faktisch ein anwaltliches für einen maximalen Datenschutz ist. Das steht zwar nicht ausdrücklich im Gesetz, doch ist das Amt bisher von allen Amtsinhabern so verstanden und auch so gelebt worden. Mit anderen Worten verschaffen die Art. 8 und 9 VE dem Beauftragten eine Machtfülle, die es in einem Rechtsstaat wie der Schweiz nicht geben

					darf. Zur Behebung dieses rechtsstaatlichen Mankos schlagen wir folgende Änderungen vor: • Statt einer Fiktion besteht die (widerlegbare) Vermutung der Datenschutzkonformität der Empfehlungen. Noch zurückhaltender sind Art. 24 Abs. 3 und 28 Abs. 5 DSGVO („kann als Gesichtspunkt herangezogen werden"). • Die vom Beauftragten selbst erlassenen Empfehlungen sind gerichtlich überprüfbar (bis zum Bundesgericht). Das gleiche gilt für die Genehmigung resp. Ablehnung der Genehmigung von durch Dritte vorgelegten Empfehlungen (so auch Art. 12bis Ziff. 6 E-SEV 108 und Art. 58 Abs. 4 und 78 DSGVO). • Für den Erlass von Empfehlungen ist nicht der Beauftragte, sondern ein unabhängiges Gremium zuständig, das aus Praktikern aller Betroffenen besteht und das verpflichtet ist, eine Abwägung der Interessen aller Betroffenen vorzunehmen.
SUISA	DSG	13			Die Informationspflichten sollen erheblich ausgebaut werden. Indem nur Mindestangaben vorgeschrieben sind, soll den Verantwortlichen eine flexible Handhabung dieser Pflicht ermöglicht und damit die Vermittlung zu vieler und unnötiger Informationen verhindert werden. Die daraus folgende Unklarheit, welche Informationen im Einzelfall gegeben werden müssen, in Verbindung mit den massiven Sanktionen wird allerdings genau das Gegenteil bewirken: Um sich auch ja nicht strafbar zu machen werden alle erdenklich möglichen Informationen geliefert, was nicht sinnvoll ist, sondern sich kontraproduktiv auswirkt. Wenn man wirklich Flexibilität erreichen und Überinformation vermeiden will, genügen letztlich die Art. 4 Abs. 3 und 6 VE. In diesem Zusammenhang ein ganz wesentlicher Punkt ist, ob Informationen in allgemeiner Form (z.B. in ABG's, Datenschutzerklärung auf einer Website) oder individuell bei jeder Beschaffung, Bekanntgabe oder jedem anderen Bearbeitungsakt vermittelt werden müssen. Dazu schweigt sich der Wortlaut von Art. 13 VE aus. Nach dem erläuternden Bericht sollen allgemeine Informationen genügen, doch wird einschränkend dazu auch ausgeführt, eine betroffene Person solle „ohne eigenes Dazutun darauf aufmerksam werden" und dürfe „nicht erst nach der Information suchen müssen" (Ziff. 8.1.3.1, S. 56). Wir empfehlen, in Art. 13 festzuhalten, dass Information in allgemeiner Weise, wie z.B. auf einer Website, sowie Hinweise darauf bei der Datenbeschaffung genügen. Dies empfiehlt auch die Mehrheit der zum VE

					befragten Experten, siehe Erläuternder Bericht Ziff. 1.7.5, S. 24.
SUISA	DSG	13	4		Die vorgeschriebene Information über Auftragsbearbeiter wird abgelehnt. Sie ist unnötig, bringt angesichts der umfassenden Verantwortung der Verantwortlichen nach Art. 7 VE keinen Mehrwert und geht über die DSGVO hinaus. Die Aufnahme der Informationen über Auftragsbearbeiter in den Katalog von Art. 20 Abs. 2 VE genügt vollkommen.
SUISA	DSG	14			Die Ausnahmen von den Informations- und Auskunftspflichten (siehe Art. 21 Abs. 1 VE) sind sehr eng formuliert, enger jedenfalls als es die E-SEV 108 und die DSGVO erfordern. Unverständlich ist, dass auch allgemein anerkannte Verweigerungsgründe fehlen, wie z.B.: • zulässige Verweigerung der Mitwirkung an Beweiserhebungen in zivil-, straf- und verwaltungsrechtlichen Verfahren, z.B. Art. 163, 165 und 166 ZPO, Art. 168-173 StPO; • Daten zur internen Meinungsbildung; • Sicherheitsinteressen; • Informationen, welche die betroffene Person schon hat oder ihr schon gegeben worden sind; • eigene Geheimhaltungsinteressen.
SUISA	DSG	14	4	a	Keinen Sinn macht und daher abzulehnen ist, die Bekanntgabe von Personendaten an Dritte von der Abwägung der Interessen von privaten Verantwortlichen auszuschliessen. Datenschutz beruht fundamental auf der Abwägung der auf dem Spiel stehenden Interessen. Eine bestimmte Art der Datenbearbeitung davon von vorneherein auszuschliessen geht nicht an. Es versteht sich von selbst, dass bei der Bekanntgabe von Daten an Dritte den Interessen der betroffenen Person(en) allenfalls ein erhöhtes Gewicht zukommt.
SUISA	DSG	16	1		Die vorgeschlagene Ausgestaltung des Instruments der Datenschutz-Folgenabschätzung wird in Verbindung mit der massiven Strafandrohung in der Praxis dazu führen, dass für *jede* Datenbearbeitung eine Folgenabschätzung durchgeführt und dem Beauftragten mitgeteilt wird. Denn jede Datenbearbeitung führt zu einem „erhöhten“ Risiko für die Persönlichkeit der betroffenen Person im Vergleich zum Zustand ohne Datenbearbeitung. Um diese unerwünschte Auswirkung zu vermeiden, ist es angebracht, sich an

					der DSGVO zu orientieren: Diese sieht eine Folgenabschätzung nur bei „hohen“ Risiken vor und gibt dafür auch drei Beispiele (Art. 35 Abs. 1 und 3).
SUISA	DSG	16	3		Die ausnahmslose Weiterleitung der Folgenabschätzungen an den Beauftragten schiesst bei weitem über das Ziel hinaus. Auch hier sollte man sich an die DSGVO halten: Diese sieht eine Konsultation des Beauftragten nur vor, wenn trotz der vorgesehenen Schutzmassnahmen ein Risiko verbleibt (Art. 36).
SUISA	DSG	16	4		Die vorgesehene Reaktionsfrist für den Beauftragten von drei Monaten ist viel zu lang bemessen. Sie sollte 6 Wochen nicht überschreiten.
SUISA	DSG	17	1		Gemäss Wortlaut und Erläuterndem Bericht soll sich die Regelung der Data Breach Notifications am europäischen Recht ausrichten. Doch angesichts der in sich widersprüchlichen Ausnahmebestimmung („es sei denn ...“) bestehen erhebliche Zweifel, ob die Regelung nicht doch dazu führt, dass ausnahmslos alle Verstösse gemeldet werden müssten: Nach Art. 23 VE führt jede Datenschutzverletzung per se zu einer Persönlichkeitsverletzung. Wir empfehlen, sich am Wortlaut der E-SEV 108 zu orientieren: Eine Meldung von „Verstössen gegen die Datensicherheit“ ist nur erforderlich, wenn die Rechte und Grundfreiheiten der betroffenen Person „erheblich“ beeinträchtigt werden könnten (Art. 7 Ziff. 2). Auch dieser Regelungsvorschlag hat in Verbindung mit den strafrechtlichen Sanktionen rechtsstaatlich höchst bedenkliche Konsequenzen: Die Strafbarkeit der Unterlassung einer Meldung und die Anzeigepflicht des Beauftragten (Art. 45 VE) haben einen Zwang zur Selbstanzeige resp. zur Anzeige von Mitarbeitern des eigenen Unternehmens zur Folge. Ersteres ist der Fall, wenn die für den Datenschutzverstoss und dessen Meldung verantwortliche Person identisch ist – der Konflikt mit dem strafprozessualen Verbot der Selbstbelastung (nemo tenetur) ist unabwendbar. Zweiteres ist der Fall, wenn die für die Meldung verantwortliche Person (z.B. ein Datenschutzbeauftragter eines Unternehmens) Datenschutzverstösse von Mitarbeitern seines Unternehmens anzeigen muss – dass dies verheerende Folgen für jede Unternehmenskultur und jedes Arbeitsklima hat, braucht wohl nicht weiter ausgeführt zu werden. Aus diesen Gründen sollte unbedingt von der Strafbarkeit der Unterlassung solcher Meldungen oder – noch besser – von der Strafbarkeit der gemeldeten Verstösse abgesehen werden. Unrealistisch und praxisfremd ist es schliesslich, die unverzügliche Meldung von Verstössen zu verlangen. Auch hier sollte die E-SEV 108 übernommen werden (Art. 7 Ziff. 2): Meldung „ohne

					übermässige Verzögerung“.
SUISA	DSG	19		a	Die Dokumentationspflicht ist vorgeschrieben, jedoch nicht näher geregelt, d.h. der Verordnung überlassen. Es ist sicherzustellen, dass diese Regelung nicht über das in Art. 30 DSGVO Geforderte hinausgeht.
SUISA	DSG	19		b	Die Ausgestaltung der Pflicht, jede Berichtigung, Löschung oder Vernichtung von Daten den Empfängern mitzuteilen, führt zu Uferlosigkeit. Sie würde selbst dann gelten, wenn der Verantwortliche nur im Interesse der betroffenen Person seinen allgemeinen datenschutzrechtlichen Pflichten nachkommt. Die Pflicht sollte dahingehend eingegrenzt werden, dass die betroffene Person ein schützenswertes Interesse an der Mitteilung hat oder sie aus berechtigten Gründen verlangt. In einem Punkt geht die Regelung unnötigerweise über die DSGVO hinaus: Den Empfängern sind auch Verletzungen des Datenschutzes zu melden. Diese zusätzliche Verpflichtung ist zu streichen.
SUISA	DSG	20			Allgemein bekannt ist, dass das Auskunftsrecht häufig zur Beweisausforschung missbraucht wird und dass das geltende Recht dagegen keine Handhabe bietet. Unverständlich ist, warum der VE diesen Missbräuchen keinen Riegel schieben will. Wir empfehlen dringend, hier eine Missbrauchsschranke einzubauen. Dass Auskünfte ohne Ausnahme kostenlos gegeben werden müssen, geht über die DSGVO hinaus. Hier könnte die Kompetenz Ausnahmen vorzusehen dem Verordnungsgeber eingeräumt werden.
SUISA	DSG	20	2 3	e	Die Auskunftsrechte im Zusammenhang mit Einzelentscheidungen gehen über die DSGVO hinaus und sind mit Art. 15 VE nicht kongruent (namentlich wird die betroffene Person schon nach dieser Bestimmung über das „Ergebnis“ informiert). Wir empfehlen, Abs. 2 lit. e mit dem Zusatz „... nach Art. 15 Abs. 1“ zu ergänzen und Abs. 3 wie folgt zu fassen: „Wird aufgrund einer Datenbearbeitung eine automatisierte Einzelentscheidung gefällt, erhält die davon betroffene Person auf Anfrage Informationen über das Zustandekommen und die Auswirkungen der Entscheidung.“
SUISA	DSG	37-55			Die einschneidendsten Neuerungen des VE liegen im Systemwechsel der Aufsicht durch den Beauftragten und in der massiven Verschärfung der strafrechtlichen Sanktionen.

					Das bisherige System der Aufsicht durch den Beauftragten – Abklärungen, Empfehlungen und Klagen vor BVGer. – soll, obwohl es sich bewährt hat, abgeschafft und durch die umfassende Verfügungskompetenz des Beauftragten ersetzt werden. Dagegen erheben wir keine grundsätzlichen Einwände. Völlig verfehlt und entschieden abzulehnen ist jedoch die massive Verschärfung der strafrechtlichen Sanktionen gegen private Personen. Auf die Gründe, warum das der falsche Weg ist, wird weiter unten zurückzukommen sein. An dieser Stelle soll ausgeführt werden, dass das alleinige Setzen auf das Strafrecht gegen Private nicht alternativlos ist. Nach den europarechtlichen Vorgaben – E-SEV 108 und DSGVO – sind strafrechtlichen Sanktionen nicht zwingend erforderlich – im Gegenteil: Nach diesen beiden Erlassen stehen verwaltungsrechtliche Sanktionen eindeutig im Vordergrund (Art. 12bis Ziff. 2 lit. c E-SEV 108, Art. 83 DSGVO). Verwaltungssanktionen gegen Unternehmen sind bereits heute u.a. im Fernmelde- und Kartellgesetz vorgesehen. Im Erläuternden Bericht (Ziff. 8.1.8, S. 83) wird denn auch als einziger Grund gegen diese angeführt, dafür müsste die Organisation des Beauftragten ausgebaut werden, was aus Kostengründen abgelehnt wird. Mit anderen Worten wird die Anwendung der Sanktionen an die Kantone abgeschoben (Art. 54 VE). Doch bei einer Gesamtbetrachtung ist das kostenmässig die teuerste Lösung, weil in der Regel zwei Behörden – der Beauftragte und die kantonale Staatsanwaltschaft – zwei verschiedene Verfahren durchführen müssen. Auch das Argument, die strafrechtliche Sanktionierung sei wegen der Garantien des Strafprozessrechts „vorteilhafter“, überzeugt in keiner Weise: Die Verfahrensrechte nach VwVG (Art. 44 Abs. 1 VE) sind dem Strafprozessrecht praktisch ebenbürtig. Ausserdem wird ein eines Datenschutzverstosses verdächtigter Verantwortlicher zwei Verfahren ausgesetzt, mithin in jeder Hinsicht doppelt belastet. Im Zusammenhang mit Schengen hat gemäss Erläuterndem Bericht (Ziff. 1.2.2.3, S. 15) der EU-Evaluationsausschuss der Schweiz den Ausbau der Sanktionsbefugnisse des Beauftragten, nicht der Strafbehörden empfohlen. Nach dem Erläuternden Bericht (a.a.O.) sei es unangemessen und widerspreche der schweizerischen Rechtstradition, Verwaltungssanktionen gegen Bundesorgane zu verhängen. Doch im Fokus steht die Datenbearbeitung durch Private und Unternehmen. Warum Unternehmen und Bundesorgane beim Sanktionsregime nicht unterschiedlich behandelt werden können, ist nicht einzusehen.

					Ein zielführendes, angemessenes und wirksames Sanktionsregime sieht unseres Erachtens wie folgt aus (in folgender Prioritätenreihenfolge): 1. Der Beauftragte erlässt die erforderlichen Verwaltungsmassnahmen nach Art. 42/43 VE. Solche Verfügungen sind mit Ungehorsamsstrafe nach Art. 292 StGB bedroht, wobei das Bussenmaximum dieser Bestimmung im DSG angemessen erhöht werden könnte. Ergänzend dazu können die bisherigen strafrechtlichen Sanktionen nach Art. 34 DSG beibehalten werden. 2. Der Beauftragte erlässt die erforderlichen Verwaltungsmassnahmen nach Art. 42/43 VE. Solche Verfügungen sind mit Ungehorsamsstrafe nach Art. 292 StGB bedroht, wobei das Bussenmaximum dieser Bestimmung im DSG angemessen erhöht werden könnte. Ergänzend dazu können gegen Unternehmen und Organisationen im Rahmen von Verwaltungsverfahren Geldbussen verhängt werden, wobei die Maxima gemäss DSGVO wesentlich zu reduzieren sind. Gegen private Personen können die bisherigen strafrechtlichen Sanktionen nach Art. 34 DSG beibehalten werden.
SUISA	DSG	44	3		Der gesetzliche Ausschluss der aufschiebenden Wirkung von Beschwerden gegen vorsorgliche Massnahmen ist entschieden abzulehnen. Derartige Massnahmen haben ein enormes – auch volkswirtschaftliches – Schädigungspotential, indem sie ganze Unternehmen lahmlegen können. Deshalb ist die Interessenabwägung durch ein unabhängiges Gericht, ob eine vorsorgliche Massnahme während der Dauer des Beschwerdeverfahrens aufrechterhalten bleibt oder nicht, unabdingbar.
SUISA	DSG	45			Die Anzeige*pflicht* des Beauftragten wird abgelehnt. Es ist kein Grund ersichtlich, über die E-SEV 108 und die DSGVO hinauszugehen, die lediglich eine Anzeige*befugnis* vorsehen.
SUISA	DSG	50-55			Die Durchsetzung des Datenschutzes zu einem wesentlichen Teil mit massiven strafrechtlichen Sanktionen gegen private Personen zu bewerkstelligen, halten wir für völlig verfehlt und lehnen wir entschieden ab. Die einzelnen Organe und Mitarbeiter eines Unternehmens oder einer Organisation als alleinige Adressaten strafrechtlicher Sanktionen ins Visier zu nehmen, ist unverhältnismässig, ja stossend und nicht zielführend. Die Handhabung des Datenschutzes ist Sache der Unternehmen als Ganzes, die dafür auch die Verantwortung übernehmen sollen. Datenschutz ist ein Unternehmensrisiko, das nicht auf die einzelnen Mitarbeiter abgewälzt werden darf. Dem Datenschutz wird ein denkbar schlechter Dienst

					erwiesen, wenn einzelne Mitarbeiter kriminalisiert werden. Die vorgeschlagene Regelung trifft besonders jene Mitarbeiter in Unternehmen, die sich speziell mit dem Datenschutz befassen, namentlich die betrieblichen Datenschutzbeauftragten. Statt dass man diese Personen schützt und stärkt, werden sie durch die strafrechtlichen Sanktionen unnötigerweise unter Druck gesetzt. Aus Angst vor strafrechtlichen Sanktionen – sogar bei fahrlässiger Tatbegehung (!) – werden einerseits die simpelsten unternehmerischen Verrichtungen durch interne oder externe Datenschutzspezialisten geprüft und abgesegnet werden müssen, was zu einer enormen Kostensteigerung der Datenbearbeitung führt, und werden anderseits die an sich bestehenden gesetzlichen Spielräume nicht mehr ausgeschöpft. Art. 53 VE bietet keine wirksame Entlastung, weil dessen Anwendungsvoraussetzungen unbestimmt sind und den Strafverfolgungsbehörden einen sehr weiten Ermessensspielraum lassen. Ausserdem können Bussen nach Art. 50/51 VE wahrscheinlich weder versichert noch dürfen sie vom Arbeitgeber bezahlt werden, damit sich dieser nicht noch der Verfolgungsbegünstigung (Art. 305 StGB) schuldig macht. Unter Strafe gestellt wird die Verletzung praktisch aller verwaltungsrechtlicher Pflichten des Gesetzes, unabhängig davon, ob im Einzelfall die Persönlichkeitsrechte der betroffenen Person(en) verletzt worden sind oder nicht. Das heisst, es ist möglich, strafrechtlich zur Verantwortung gezogen zu werden, ohne dass eine Rechtsgutverletzung vorliegt. Das darf es in einem Rechtsstaat nicht geben. Zu welch unhaltbaren Ergebnissen das führt, zeigt sich z.B. daran, dass nicht derjenige gebüsst wird, der bewusst Personendaten missbräuchlich verwendet, sondern der andere Mitarbeiter im Unternehmen, der es aus Unachtsamkeit unterlässt, diesen Datenschutzverstoss dem Beauftragten zu melden. Die vorgeschlagene Regelung erweist sich auch unter dem Aspekt des strafrechtlichen Legalitätsprinzips (Art. 1 StGB) als höchst fragwürdig. Wie oben in den Bemerkungen zu Art. 8/9 dargelegt, wird das Datenschutzrecht durch sehr allgemein und vage formulierte Gebote und Verbote und damit durch ausserordentlich hohe Rechtsunsicherheit geprägt. Wenn nun diese unbestimmten Normen gleichzeitig zu Straftatbeständen erhoben werden, wie das Art. 50/51 VE tut, können die Rechtsunterworfenen kaum abschätzen, was sie tun dürfen und was nicht. Die Höhe der vorgeschlagenen strafrechtlichen Sanktionen wird im wesentlichen durch die europarechtlichen Vorgaben begründet (Erläuternder Bericht Ziff. 8.1.8, S. 83f.): Die Sanktionen sollen „abschreckend“ sein, damit die Schweiz nicht des Angemessenheitsbeschlusses der EU verlustig geht.

					Dabei gingen die Überlegungen offenbar dahin, die hohen Verwaltungssanktionen (Geldbussen) der DSGVO irgendwie im Strafrecht abzubilden. Doch ein solcher „Transfer" funktioniert nicht. Funktionsweise und Adressaten der beiden Sanktionensysteme sind derart unterschiedlich, dass ein Vergleich der beiden gar nicht möglich ist. Einige der Straftatbestände sind als Antragsdelikte ausgestaltet. Teilweise ist jedoch unklar, wer zum Antrag berechtigt ist, weil es an einer Person fehlt, deren Rechtsgüter verletzt werden (Art. 50 Abs. 1 lit. c, Art. 51 Abs. 1 lit. c-f VE).
SUISA	DSG	52			Der bisherige Art. 35 DSG soll hinsichtlich Tatbestand wie der Sanktionen erheblich ausgebaut werden. Die Norm schafft sozusagen aus dem Nichts eine umfassende berufliche Schweigepflicht. Voraussetzung seiner Anwendung ist nicht eine vorbestehende gesetzliche oder vertragliche Geheimhaltungspflicht, sondern lediglich die Tatsachen der „Kenntnis" von Personendaten und deren Bearbeitung zu kommerziellen Zwecken. Dadurch wird diese Strafbestimmung uferlos. Wir lehnen sie ab. Wenn überhaupt kann Art. 35 DSG ohne Verschärfung der Sanktionen an die Gegebenheiten des VE angepasst werden.
SUISA	DSG	59			Der VE sieht eine Übergangsfrist von zwei Jahren nur für die Datenschutz-Folgenabschätzung, die Massnahmen der privacy by design und by default sowie die Dokumentation der Datenbearbeitung vor. Unerfindlich ist, warum nicht auch zu den zahlreichen sonstigen Neuerungen des VE eine Übergangsbestimmung bzw. -frist vorgeschlagen wird. Wir empfehlen, generell eine Übergangsfrist von zwei Jahren vorzusehen, zumal die DSGVO die gleiche Umsetzungsfrist gewährt.
SUISA	StGB	179^{novies}			Diese Strafbestimmung soll im Tatbestand beträchtlich erweitert werden, indem alle Personendaten darunter fallen. Angesichts der hohen Strafdrohung halten wir das für unverhältnismässig und empfehlen, weiterhin nur die unbefugte Beschaffung von nicht frei zugänglichen besonders schützenswerten Personendaten und das unbefugte Profiling unter Strafe zu stellen.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		

SUISSEDIGITAL

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

(vorab per Email in Word- und PDF-Fassung an: jonas.amstutz@bj.admin.ch)

Bern, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DDSG)

Sehr geehrte Frau Bundesrätin

Sie haben am 21. Dezember 2016 interessierte Kreise eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nimmt SUISSEDIGITAL als Wirtschaftsverband der Schweizer Kommunikationsnetze gerne wahr.

SUISSEDIGITAL vertritt rund 200 privatwirtschaftlich und öffentlich-rechtlich organisierte Unternehmen aus der ganzen Schweiz von unterschiedlichster Grösse, welche aber mehrheitlich zum Kreis der KMU zu zählen sind. Diese versorgen mit ihren Kommunikationsnetzen und -dienstleistungen zahlreiche Geschäftskunden und über 2,5 Millionen Privathaushalte nicht nur in städtischen Gebieten, sondern auch in ländlichen Regionen. Wir leisten damit einen grossen Beitrag an die digitale Vernetzung der Schweiz und deren Bevölkerung. Unser Kerngeschäft ist die Datenverarbeitung. Diese Daten erfüllen zunehmend und überwiegend die Voraussetzungen von Personendaten bzw. Daten, die zu einer Identifikation einer Person führen könnten. Datenschutz und Datensicherheit, sowie die entsprechenden Regulierungen sind daher für uns eine der wichtigsten Geschäftsgrundlagen. Entsprechend besteht eine hohe Betroffenheit, wenn diesbezüglich neue Regulierungen zur Diskussion stehen.

Gerne nehmen wir gestützt auf die zahlreich eingegangenen Inputs unserer Mitglieder wie folgt Stellung, wobei wir zunächst auf einige grundsätzliche Punkte eingehen, ehe wir – wie verlangt – zu den einzelnen Bestimmungen des VE-DSG Stellung beziehen und Anträge stellen:

Verband für Kommunikationsnetze – Association des réseaux de communication
Kramgasse 5 – Postfach 515 – CH-3000 Bern 8 – T +41 31 328 27 28 – F +41 31 328 27 38 – info@suissedigital.ch – www.suissedigital.ch

A. Grundsätzliche Bemerkungen

1. Chancen der Digitalisierung und damit auch Chancen der Datenbearbeitung

Die Digitalisierung bietet für die Zukunft ein enormes Entwicklungspotential und sollte durch unterstützende Rahmenbedingungen – gerade im Bereich Datenbearbeitung – gefördert werden. Die Schweiz sollte ein Wirtschaftsstandort für digitale Geschäftsmodelle sein und grösstmögliche Freiräume für die Datenbearbeitung zulassen. Grundsätzlich sollte jede Form von Datenbearbeitung zulässig sein und die informelle Selbstbestimmung sollte über Auskunfts- und Kontrollrechte realisiert werden. Ein Regulierungskonzept darf nicht der Vorstellung folgen, eine „Datenbearbeitung" durch Unternehmen sei *per se* anrüchig. Ein modernes Datenschutzgesetz ist weiter auch kein spezielles Konsumentenschutzrecht.

Die im Vorentwurf vorherrschende „Verbots- und Bestrafungskultur" sollte deshalb so nicht umgesetzt werden. Die Datenschutzgesetzgebung ist bisher – und gemäss VE-DSG noch mehr – als Konsumentenschutzgesetzgebung stark von gesetzlichen Einschränkungen für Unternehmen geprägt, die jedoch in der Praxis durch Einwilligungserklärungen der Datensubjekte übersteuert werden können. Dies führt heute gesamthaft nicht zu mehr Datenschutz, sondern nur zu aufwendigeren Einwilligungsverfahren und damit höheren Transaktionskosten bei der Geschäftsabwicklung.

Wir begrüssen eine Stärkung des Rechts auf informelle Selbstbestimmung, lehnen jedoch die Stossrichtung ab, dass zukünftig einzelfallbezogene Zustimmungserklärungen eingeholt werden müssen. Für eine wirtschaftliche Geschäftsabwicklung muss es möglich sein, in einem Vertragsverhältnis eine pauschale Einwilligung über allgemeine Geschäftsbedingungen abzuschliessen. Die Grundlagen dazu genügen im UWG.

2. Gleichwertigkeit des Datenschutzes in der CH und in der EU

Datenschutzregulierung ist heute kein nationales Thema mehr. Die modernen Kommunikationsnetze und die technologischen Entwicklungen machen den Datenverkehr zu einem globalen Thema. Ein freier Datenverkehr ist aus unserer Sicht unbedingt zu erreichen, insbesondere durch eine gegenseitige institutionelle Anerkennung eines gleichwertigen Datenschutzes mit möglichst vielen Ländern. Allen voran natürlich mit der Europäischen Union und den USA. Damit können für Unternehmen hohe administrative Hürden und Kosten vermieden werden. Dabei sind die notwendigen Bestimmungen für eine Gleichwertigkeit im Datenschutz umzusetzen.

2.1 Unnötiger „Swiss Finish"

Ein Grund für die Revision des DSG ist gemäss Erläuterungsbericht des EJPD/BJ die Entwicklung des Datenschutzes im europäischen Raum. Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) EuDSGVO in Kraft. Zudem gilt die EU-Richtlinie 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen. Die DSG-Revision soll die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Die Annäherung würde zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür bilden, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht (obschon unserer Ansicht nach dies auch das bestehende DSG

weiterhin tun würde). Die Revision des Schweizer DSG geht aber in mehreren Fällen über das Schutzniveau der EU hinaus, was nicht nachvollziehbar ist. Beispiele für diesen Swiss Finish sind:

a) Art. 13 Abs. 3 und 4 VE-DSG sehen eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister) sowie bei der Weitergabe von jeglichen Personendaten vor. Für den Adressaten solcher Informationen führt dies in einer zunehmend über digitale Geschäftsprozesse gesteuerten Gesellschaft zu einer Informationsflut. Nicht einmal die EU-Richtlinie 680/2016 vom 27. April 2016 sieht diesen Detaillierungsgrad vor.

b) Art. 16 Abs. 3 VE-DSG sieht eine Informationspflicht des Datenschutzbeauftragten über die Datenschutz-Folgeabschätzungen in jedem Fall vor. Die EU-Richtlinie 680/2016 hingegen fordert dies in Art. 27 und 28 nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen.

c) Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung (Art. 25). Diese besagt lediglich, dass gewisse Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen.

d) Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EuDSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell.

e) Auch der Ansatz des VE-DSG betreffend Profiling geht über die Bestimmungen der EuDSGVO und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der EuDSGVO noch der Konvention. Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren. Die Bedingung einer vorgängigen ausdrücklichen Einwilligung bei jeder Art von Profiling schiesst über das Ziel hinaus. Profiling soll nicht bereits bei dessen Erstellung schutzrelevant werden.

f) Überschiessende Informationspflichten (z.B. Art. 6 Abs. 2 oder Art. 13 Abs. 5 VE-DSG), die Geschäftsgeheimnisse betreffen können (gemäss Art. 6 Abs. 2 VE-DSG informiert der EDÖB über heikle Verfahren und Geschäftsgeheimnisse, ohne dass ein datenschutzrechtlicher Tatbestand dazu vorliegen müsste). Diese Pflicht ist dem EU Recht (inkl. E-SEV 108) fremd.

Wir lehnen Bestimmungen ab, die über das Mass der europäischen Regelungen hinausgehen. Es besteht keine Notwendigkeit für einen «Swiss Finish». Entsprechende Vorschläge sind ersatzlos zu streichen oder auf ein supranationales Mass zurückzunehmen.

2.2 Keine Doppelspurigkeiten bei der Aufsicht

Da viele Schweizer Unternehmen eine Tätigkeit in der Europäischen Union ausüben, werden diese auf der Grundlage von Art. 3 DSGVO i.V.m. Art. 55 Abs. 1 DSGVO auch der Aufsicht der nationalen Datenschutzbehörden unterstehen. Diese Doppelaufsicht bringt einerseits zahlreiche Rechtsunsicherheiten mit sich und andererseits verursacht sie eine massive administrative Zusatzbelastung der Schweizer Unternehmen. Es ist mit der Europäischen Union eine Gleichbehandlung auszuhandeln, damit die Schweizer Datenschutzaufsicht gegenseitig in das Konzept des „One-Stop-Shop“ nach Art. 56 DSGVO einbezogen werden kann. Heute steht diese für Unternehmen ausserhalb der EU nicht zur Verfügung.

3. Fehlende verfassungskonforme Regulierungskosten Folgeabschätzung (RFA)

Die Bundesverfassung verpflichtet in Art. 170 die Bundesversammlung, die Massnahmen des Bundes auf ihre Wirksamkeit zu prüfen („Die Bundesversammlung sorgt dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden.“). Nach Art. 141 Abs. 2 Bst. f) ParlG müssen in der Botschaft an das Parlament eine Kosten-Nutzen Abschätzung sowie nach Bst. g) die Folgen für die Wirtschaft und die Gesellschaft erläutert werden.

Auf Seite 23 des Erläuterungsberichts zum VE-DSG werden die Regulierungskosten als unbedeutend eingestuft. **Diese Einschätzung ist falsch**. Alle Unternehmen bearbeiten heute in zunehmendem und komplexem Mass Personendaten bzw. Rohdaten für Persönlichkeitsprofile und sind damit von den Bestimmungen direkt betroffen. **Die Regulierungskosten sind für alle Unternehmen massiv höher als beschrieben!**

3.1 Mangelhafte Durchführung der Regulierungsfolgeabschätzung

Wir stellen die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG grundsätzlich in Frage. Die Unternehmensbefragung basiert auf einer völlig ungenügenden Nettostichprobe von lediglich 95 (!) Fragebogen, wovon keines der Unternehmen den Fragebogen vollständig beantwortet hat. Insbesondere wurden die spezifischen Daten zu den Folgen nur von wenigen Unternehmen beantwortet. Keines der angefragten Unternehmen machte bei einer Interviewerhebung mit.[1] Die Studienverfasser – immerhin eine renommierte Revisionsgesellschaft – erklären dazu ohne jeden Interpretationsspielraum selbst:

> „Die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten waren sowohl in Bezug auf Quantität als auch Qualität unzureichend; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands.“[2]

[1] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

[2] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 8.

> „Die Quantität und die Qualität des Rücklaufs aus der Unternehmensbefragung ermöglichte es nicht, in repräsentativer Weise eine Hochrechnung zur Schätzung der finanziellen Auswirkungen zu erstellen.“[3]

Eine korrekte Aussage ist daher aufgrund dieser Angaben nicht möglich und es ist erstaunlich, dass das EJPD in ihrem Erläuterungsbericht zum Ergebnis kommt, die zu erwartenden Regulierungskostenfolgen seien unbedeutend. Im Bericht wird lediglich angegeben, dass die fehlenden statistischen Erhebungen durch Gespräche mit Fachpersonen ausgeglichen worden sind. Auch das ist falsch: Die angeblichen Gespräche sind ein dreistündiges Gespräch vom 4. Mai 2016 mit neun Fachpersonen, wo auch der Geschäftsführer von SUISSEDIGITAL anwesend war. Die anwesenden Vertreter haben bei der mündlichen Erörterung der Fragen wiederholt darauf hingewiesen, dass eine verbindliche Beurteilung der „statistischen“ Ergebnisse aufgrund der unzureichenden Quantität und Qualität der Umfrageergebnisse absolut unmöglich sei. Wir finden die sehr kritischen Aussagen der angeblich befragten Fachpersonen im Bericht heute mit keinem Wort erwähnt. In der Studie wird lediglich vermerkt, dass diese Aussagen nicht repräsentativ sind.[4] Über den Verlauf der Sitzung vom 4. Mai 2016 wurde durch den Geschäftsführer von SUISSEDIGITAL ein internes Protokoll erstellt; dort ist auch die – für die desaströse Datenqualität – von einem Berater des Bundes vorgebrachte Begründung vermerkt, für die Untersuchung wären halt lediglich CHF 80‘000.- Budget zur Verfügung gestellt worden.

Wir sind der Meinung, dass damit die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt wurde. Das ist für einen Vorentwurf von derartiger wirtschaftlicher Tragweite nicht akzeptabel und wir behalten uns diesbezüglich alle rechtlichen Massnahmen ausdrücklich vor, sollte dieser Umstand im Zuge der Abwicklung des weiteren Gesetzesprojekts keine Beachtung finden.

3.2 Methodisch fehlerhafte Durchführung der Regulierungsfolgeabschätzung

Die Einteilung der Unternehmen in drei Kategorien scheint völlig willkürlich und basiert nicht auf der tatsächlichen Betroffenheit. So werden zum Beispiel die Mehrheit der gewerblichen KMU-Betriebe (wie Metzgerei, Schreinerei, Papeterie, Spenglerei, Elektriker, lokale Transporteure, Baubetriebe, Bauernbetriebe, Velomechaniker, Coiffeur etc.) in das Segment A als Unternehmen mit geringer datenschutzrechtlicher Exponierung und keinem oder geringem Einsatz von Web-IT-Technologien eingeteilt.

Dabei wird verkannt, dass heute – und vor allem in Zukunft – jedes Unternehmen moderne Informatikmittel einsetzt, eine Internetseite und Social Media-Profile betreibt und damit Personendaten bearbeitet. Gerade kleine Unternehmen nutzen überdurchschnittlich viel cloudbasierte Internetapplikationen oder beziehen ihre gesamte Geschäftssoftware aus der Cloud. Als Beispiel deinen Cloud-Angebote wie „Microsoft 365“ für kleinere und mittlere Unternehmen mit einer Datenspeicherung im Ausland, u.a. auch in den USA. Damit müssen diese 335'000 (55.1%) Unternehmen korrekterweise dem Segment B als Unternehmen mit mittlerer bis grosser datenschutzrechtlicher Exponierung (innerhalb der Schweiz und weltweit tätige Unternehmen und/oder Einsatz von

[3] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

[4] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 25.

Web-IT-Technologien wie Webseiten für Marketing oder Nutzung von Cloud Services) zugeordnet werden.[5]

3.3 Falsche Angaben zur Regulierungsfolgeabschätzung im VE-DSG

Die Folgekosten für die Wirtschaft werden überhaupt nicht quantifiziert. Vielmehr wird behauptet:

> „Die Analyseergebnisse zeigen, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen generell nur geringfügig betroffen sind. Die Auswirkungen der Revision auf dieses Segment sind somit verhältnismässig gering. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im VE vorgesehenen Massnahmen stärker betroffen als Grossunternehmen, da sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei.“[6]

Nur schon durch das Zusammenziehen der in der Studie vorhandenen – ungenügenden – Schätzungen, wird der massive Umsetzungsaufwand sichtbar, entsprechend unerklärlich es ist, dass dies im Erläuterungsbericht mit keinem Wort erwähnt wird:[7]

Handlungspflichten nach VE-DSG	**Einmalig**	**Wiederkehrend**	**Kosten CHF**
Informationspflichten			
Pflicht zur Information der betroffenen Person	60 – 100 Stunden	30 Stunden	3000 – 40‘000
Auskunft über Aufbau der Datenbearbeitung	4- 12 Stunden	1.6 h – 3 Tage pro Fall	Keine Angabe
Informationspflicht Automatisierte Entscheidungen	30 – 50 Stunden	3 Stunden pro Fall	10‘000
Meldung Data Breach	5 – 20 Stunden	2 – 5 Stunden pro Fall	5‘000 – 10‘000
Datenherrschaft			
Mitteilung, Löschung, Beschränkung	14 – 20 Stunden	3 Stunden pro Fall	100 – 5‘000
Pflichten auf Datenübertragbarkeit	12 Stunden	2 Stunden pro Fall	7‘500
Unternehmensinterne Datenschutzorganisation			
Datenschutz-Folgeabschätzung[8]		20 – 160 h pro Fall	5‘000 – 30‘000
Privacy by Default	1 – 40 Stunden		500 – 5‘000
Betriebliche Datenschutzbeauftragter		500 – 2‘000 h pro Jahr	
Grenzüberschreitender Datenverkehr			
Genehmigung Standard Datentransfervereinbarung	50 Stunden		5‘000

[5] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 5.

[6] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetze und Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 23.

[7] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 27 ff.

[8] In einer Studie der Europäischen Union zur Datenschutz-Folgeabschätzung (Privat Impact Analysis) wurden die Kosten pro Durchführung auf € 14‘000 – 149‘000 geschätzt. Quelle: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, Seite 70.

Auch wenn man nur die Aufgaben einbezieht, die alle Unternehmen beachten müssen, und als Basis Minimalschätzungen als Grundlage für eine Hochrechnung annimmt, ergeben sich Umsetzungskosten für die Schweizer Wirtschaft von über CHF 1‘532‘160‘000, resp. im Durchschnitt von CHF 2‘520 pro Unternehmen.[9] In der Praxis dürften diese noch wesentlich höher liegen.

Es muss heute nämlich davon ausgegangen werden, dass alle Unternehmen von diesen vorgeschlagenen Bestimmungen betroffen sind, insbesondere da auch alle ohne jede *de minimis*-Schwelle den exzessiven Strafbestimmungen unterliegen. Selbst die Studienverfasser gehen von einer vergleichsweise hohen Belastung der Unternehmen aus:

> „Gleichsam haben mehrere Fachpersonen im Rahmen der Fachgespräche vorgebracht, dass bei gleicher Datenbearbeitungstätigkeit KMU stärker von der Revision oder generell von den datenschutz-rechtlichen Verpflichtungen betroffen sind als grosse Unternehmen, da ihnen die notwendige Compliance-Infrastruktur fehle resp. sie im Verhältnis teurer sei. In Bezug auf die Unternehmen der Segmente B und C ist demgegenüber von einer vergleichsweise hohen Belastung durch die Revision des Datenschutzgesetzes auszugehen.“[10]

Aufgrund der methodischen Fehlbeurteilung wird in Verbindung mit der ungenügenden Datenerhebung bei den Unternehmen sichtbar, dass einerseits die Regulierungsfolgenabschätzung nicht korrekt durchgeführt wurde und andererseits die Regulierung für die gesamte Wirtschaft massiv höhere Kosten zur Folge hat.

Bislang wurde die korrekte Durchführung eines Vernehmlassungsverfahrens oder sogar die Vorlage einer Botschaft an das Parlament ohne solche Regulierungskostenfolgenabschätzung nie durch die Judikative überprüft. Wir und mit uns die gesamte Schweizer KMU-Wirtschaft müssen darauf vertrauen, dass dieses Manko vor einer Parlamentsvorlage unbedingt und professionell korrigiert wird. Andernfalls muss diese Korrektur spätestens vom Parlament bzw. den entsprechenden Rechtskommissionen vorgenommen werden. Sollte diese nicht gelingen, würden die neuen Regulierungen spätestens beim Vollzug einer auf den VE-DSG gestützten Verordnung über die akzessorische Normenkontrolle Fälle für Gerichte.

B. Forderungen

Wir stellen weiter folgende Forderungen grundsätzlicher Natur an das revidierte Datenschutzgesetz:

a) Eine klare Regelung der Einwilligung und eine gesetzliche Vermutung der Einwilligung bei definierten Vorgängen, wie zum Beispiel einem Vertragsverhältnis würden den Unternehmen wesentlich mehr Rechtssicherheit und weniger administrativen Aufwand bringen. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten.

b) Auf die unüberschaubare Menge von Informations- und Dokumentationspflichten der Unternehmen sowie der rein administrativen Meldungen an den Beauftragten ist

[9] 608‘000 Unternehmen mit einem Aufwand von 84 Stunden zu einem Stundenkostensatz von CHF 30.

[10] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 53.

grundsätzlich zu verzichten. Hingegen sollten Unternehmen vom Beauftragten innerhalb von 30 Tagen eine verbindliche Beurteilung einer Datenbearbeitung verlangen können (Negativattest, *Comfort Letter* oder dergleichen).

c) Auf eine Ausweitung des Strafenkatalogs ist zu verzichten. Insbesondere sind nur materielle Datenschutzverletzungen zu sanktionieren und keinesfalls Verletzungen von Dokumentations- oder Meldepflichten an den Beauftragten. Es bestehen heute genügend Möglichkeiten bei tatsächlichen Verstössen, Sanktionen gegen fehlbare Unternehmen zu verhängen. Der Verweis auf das Persönlichkeitsrecht für Ansprüche von betroffenen Personen hat sich ebenfalls bewährt und muss nicht geändert werden.

C. Stellungnahme zu den einzelnen Artikeln

Im Übrigen finden Sie unsere Anträge und Bemerkungen zu den einzelnen Artikeln wie verlangt in der nachfolgenden tabellarischen Übersicht:

VE-DSG	Anträge und Bemerkungen
1. Abschnitt: Zweck, Geltungsbereich und Begriffe	
Art. 1 Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.	**Antrag zu Art. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. Wenn nicht im Gesetzestext (Art. 1 oder Art. 2 Abs. 1 VE-DSG) selbst, so ist diese Klarstellung spätestens in der Botschaft unmissverständlich anzubringen.
Art. 2 Geltungsbereich [1] Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen durch: a. private Personen; b. Bundesorgane. [2] Es ist nicht anwendbar auf: a. Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden; b. Personendaten, die durch die Eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden; c. Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden; d. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007, die in der Schweiz Immunität geniessen, wie das Internationale Komitee vom Roten Kreuz. [3] Dieses Gesetz ist nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Für die Bearbeitung der übrigen Daten sind sie von	**Antrag zu Art. 2 Abs. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. **Antrag zu Art. 2 Abs. 2 lit. c)**: Beibehaltung des geltenden Wortlauts. Der VE will neu nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung nicht mehr gelten. Das ist weder sachgerecht, noch nachvollziehbar, und führt zu schwerwiegenden Konsequenzen im Zusammenhang mit der Führung von Gerichtsverfahren (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).

VE-DSG	Anträge und Bemerkungen
der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ausgenommen. [4] Die Bundesversammlung und der Bundesrat sind von der Aufsicht durch den Beauftragten ausgenommen.	**Antrag zu Art. 2 Abs. 5 (<u>neu</u>)**: Der im Erläuterungsbericht erwähnte Allgemeincharakter des VE (*Lex Generalis*) ist in einem neuen Abs. 5 ausdrücklich vorzusehen. Es ist festzustellen, dass datenschutz- bzw. datenbearbeitungsrelevante Regelungen in kantonalen und anderen Erlassen des Bundes dem allgemeinen DSG vorgehen (*Lex Specialis*). Damit können entsprechende Einzelhinweise im VE gestrichen werden. Solche Einzelerwähnungen sind nicht sinnvoll und gefährlich, weil diese das im Erläuterungsbericht erwähnte, selbstverständliche Wirkungsprinzip „*Lex Specialis derogat Lex Generalis*“ grundsätzlich in Frage stellen. Diese generelle Klarstellung ist aber vor allem deshalb wichtig, weil das Prinzip beim Anspruch auf Information über bearbeitet Personendaten schon nach geltendem Recht immer wieder in Frage gestellt worden (<u>Beispiel</u>: Ein Teil der allgemeinen Datenschutz-Lehre meint unzutreffend, dass Art. 8 DSG auch im Bereich von fernmelderechtlich geschützten Personendaten anwendbar bleibt, ergo die spezifischen fernmelderechtlichen Datenschutzbestimmungen in Art. 43 bis 46 FMG und 9. Kapitel „Fernmeldegeheimnis und Datenschutz“, Art. 80 ff. FDV, den Datenschutz bei der Datenherausgabe im Zusammenhang mit der Erbringung von Fernmeldediensten nicht als „Lex Specialis“ abschliessend regelt.)
2. Abschnitt: Allgemeine Datenschutzbestimmungen	
Art. 3 Begriffe Die folgenden Ausdrücke bedeuten: a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; b. *betroffene Person:* natürliche Person, über die Daten bearbeitet werden; c. *besonders schützenswerte Personendaten:* 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,	**Antrag zu Art. 3 lit. c Ziff. 4**: Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die <u>zum Zweck</u> der Identifizierung bearbeitet werden. Der im Erläuterungsbericht enthaltene Hinweis, wann auch Fotos als biometrische Personendaten gelten, ist unverständlich. Es ist klarzustellen, wann Fotos als Personendaten gelten; dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biometrische Daten gelten.

VE-DSG	Anträge und Bemerkungen
5. Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe; d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten; e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten; f. *Profiling:* jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;	**Bemerkung zu Art. 3 lit. c Ziff. 5**: Die Bestimmung ist in dieser allgemeinen Form problematisch; etwa wenn Vermögensdelikte zur Diskussion stehen, von welchen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste. **Antrag zu Art. 3 lit. f)**: Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes „Daten“. Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um „Personendaten“. Andere Daten werden gemäss Erläuterungsbericht durch den Begriff „Personendaten“ konsumiert. Der Begriff des „Profiling“ ist zu unbestimmt und gefährdet damit die Rechtssicherheit mit nicht ermittelbaren Kostenfolgen für die gesamtschweizerische Wirtschaft. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem „Persönlichkeitsprofil“ des geltenden Rechts abzulehnen. **Generelle Bemerkung zu Art. 3 lit. f)**: Die nicht reflektierte Übernahme von Begriffen des ausländischen Rechts führt dazu, dass sich die Anwendung und Auslegung von Schweizer Recht zukünftig primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und hier vor allem deshalb nicht sachgerecht. weil der Begriff des „Profiling“ gegenüber dem EU-Recht sogar nicht mit einem „Swiss Finish“ versehen und inhaltlich ausgeweitet wird. Die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich schädlich, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als „Voraussage“ eines späteren Verhaltens interpretiert werden könnten. Die Revision schiesst hier

VE-DSG	Anträge und Bemerkungen
	weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen, ohne alle erheblichen Verpflichtungen einzuhalten, die der VE mit dem „Profiling“ verknüpft. Es gäbe zahlreiche Beispiele von sicherlich nicht beabsichtigten und unbedachten Konsequenzen in längst etablierten und von Konsumenten akzeptierten digitalisierten Wirtschaftsprozessen: Man denke nur an die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind. So etwas Selbstverständliches würde plötzlich problematisch.
g. *Bundesorgan:* Behörde und Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist; h. *Verantwortlicher*: Bundesorgan oder private Person, das oder die – alleine oder zusammen mit anderen – über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet;	**Antrag zu Art. 3 lit. h und i**: Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), *eventualiter* zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu einer unklaren – teilweise unsinnigen – Aufteilung der Verantwortung und zu Doppelspurigkeiten. Zudem wird übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen *kann*. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für wen?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den Verantwortlichen?) geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den Verantwortlichen?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht, ergo auch hier nicht einmal das Generalargumente der Bundesverwaltung zieht, man müsse etwas so regeln, weil es ausländisches Recht so vorgebe und man andernfalls auf eine „Blacklist“ gesetzt werde. Dass „Arbeitnehmer mit einem Arbeitsvertrag“ (gibt es auch Arbeitnehmer ohne Arbeitsvertrag?) nicht unter den Begriff des "Auftragsbearbeiters" fallen, steht zwar im Erläuterungsbericht. In Anbetracht der merkwürdigen Formulierung „Arbeitnehmer mit Arbeitsvertrag“ wäre es aber dringend nötig, dies klar und deutlich im Gesetzestext zu normieren (Simpler Vorschlag: „Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter“).
i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	

VE-DSG	Anträge und Bemerkungen
Art. 4 Grundsätze [1] Personendaten müssen rechtmässig bearbeitet werden. [2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.	**Antrag zu Art. 4 Abs. 2**: In Absatz 2 ist zu ergänzen, dass nicht nur die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und verhältnismässig zu sein hat, sondern auch die Ausübung anderer Rechte und Pflichten gemäss diesem Gesetz.
[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.	**Antrag I zu Art. 4 Abs. 3**: Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Der Erläuterungsbericht argumentiert, es sei mit der redaktionellen keine materielle Änderung beabsichtigt (das steht im Übrigen – beschwichtigend – an zahlreichen anderen Stellen des Erläuterungsberichts). Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann in der Praxis eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. **Antrag II zu Art. 4 Abs. 3**: Im Erläuterungsbericht wird beim Beispielkatalog von nicht erkennbaren Datenbearbeitungen die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch Privatunternehmen erwähnt. Es wird dazu auf den sog. Logistep-Entscheid (BGE 136 II 508 E.4) verwiesen. Dieser Verweis und dieses Beispiel ist deplatziert, zumal das Bundesgericht in diesem Entscheid ausdrücklich festgehalten hat, seine Begründung beziehe sich auf geltendes Recht, welches durch den Gesetzgeber im Lichte der mit der Sammlung solcher IP-Adressen zusammenhängenden vertretbaren Absicht allenfalls zu korrigieren sei. Es ist unverständlich, weshalb nun gerade dieses Beispiel als „Nicht-Erkennbarkeit einer Bearbeitung von Personendaten“ aufgeführt ist. Vielmehr wäre gerade vorzusehen, dass die Beschaffung von IP-Adressen zum Zwecke der Strafverfolgung von diesem Grundsatz ausdrücklich nicht erfasst wird.
[4] Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.	**Antrag zu Art. 4 Abs. 4**: Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.
[5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten.	**Antrag zu Art. 4 Abs. 5**: Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Erläuterungsberichts sind auch hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten. *Eventualiter* ist Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind" zu beschränken (Streichung des Rests). Bekanntlich fängt die "Bearbeitung" schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE).
[6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von	

VE-DSG	Anträge und Bemerkungen
besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.	Eine fortdauernde Verpflichtung zur Nachführung ist nicht erfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Selbst wenn so etwas möglich wäre, ist dieses Konzept nicht finanzierbar. **Antrag zu Art. 4 Abs. 6**: Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f) vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (vgl. dazu auch die Bemerkungen zu Art. 3 lit. f VE). Die im Erläuterungsbericht vertretene Ansicht, mit der vorgeschlagenen Redaktion von Abs. 6 möge die in der Lehre ausgetragene Kontroverse über die „Ausdrücklichkeit“ einer Einwilligung beendet sein, ist die blosse Äusserung einer Hoffnung. Das Gegenteil wird der Fall sein und die Kontroverse verstärkt werden: Es lassen sich über die Begriffe „freiwillig“, „freiwillig und eindeutig“, „ausdrücklich“ und die Abgrenzung zur blossen „Einwilligung“ (vgl. z.B. Art. 6 Abs. 1 lit. a VE) vorzügliche juristische Publikationen schreiben.
Art. 5 Bekanntgabe ins Ausland [1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. [2] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz gewährleistet. [3] Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch: a. einen völkerrechtlichen Vertrag; b. spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde; c. standardisierte Garantien, insbesondere durch Vertrag: 1. welche der Beauftragte vorgängig genehmigt hat, oder 2. welche der Beauftragte ausgestellt oder anerkannt hat; d. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig genehmigt wurden: 1. durch den Beauftragten, oder 2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet. [4] Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 Buchstabe b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien informieren. [5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c	**Antrag zu Art. 5 Abs. 3 lit. d)**: Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG. **Antrag zu Art. 5 Abs. 4 bis 6**: Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt – wie aus dem Wort ersichtlich – nach den Weisungen des Verantwortlichen, dem – wiederum entsprechend seiner Bezeichnung – die Verantwortung für die Information des Beauftragten obliegt.

VE-DSG	Anträge und Bemerkungen
Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht. [6] Der Verantwortliche oder der Auftragsbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit. [7] Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.	**Antrag zu Art. 5 Abs. 7**: Es ist zu ergänzen, dass der Bundesrat die Liste quartalsweise aktualisieren muss und dazu ein ständiges Staaten-Monitoring etabliert. Heute ist die Liste von Staaten mit der Gewährleistung von angemessenem Schutz des EDÖB gut etabliert und ausreichend dynamisch. Wenn nun die Kompetenz zum Bundesrat hinaufgereicht wird, ist sicherzustellen, dass der Bundesrat diese sehr operative Rolle auch bedarfsgerecht wahrnehmen muss.
Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: a. die betroffene Person im Einzelfall eingewilligt hat; b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt; c. die Bekanntgabe im Einzelfall unerlässlich ist für: 1. die Wahrung eines überwiegenden öffentlichen Interesses, oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde; d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; e. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; f. die Daten aus einem gesetzlich vorgesehenen Register stammen, das zugänglich ist für die Öffentlichkeit oder für Personen mit einem schutzwürdigen Interesse, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. [2] Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.	**Antrag zu Art. 6 Abs. 1 lit. a)**: Es ist zu präzisieren, wie sich die hier ohne die Zusätze „freiwillig“, „eindeutig“ oder „ausdrücklich“ auskommende Einwilligung gestalten lässt. **Antrag zu Art. 6 Abs. 2**: Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1 lit. b, c oder d ins Ausland bekanntgegeben wird. Das gilt erst recht, wenn neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Es ist mit dieser Doppelnennung nicht klar, wer am Ende für die Erfüllung der Meldepflicht verantwortlich ist. Die Folge davon

VE-DSG	Anträge und Bemerkungen
	wird sein, dass sowohl der Verantwortliche, als auch der Auftragsbearbeiter Meldung erstatten müssen, um sich nicht einer Strafverfolgung auszusetzen. Die Bestimmung ist weiter auch deshalb heikel, weil solche Meldungen z.T. sensible Geschäftsinformationen betreffen (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetzen auch für Dritte einsehbar werden. Auch hier wurde offenbar in keiner Weise an den berechtigten Schutz von Geschäftsgeheimnissen gedacht.
Art. 7 Auftragsdatenbearbeitung [1] Die Bearbeitung von Personendaten kann durch Vereinbarung oder Gesetz einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. [2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters. [3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. [4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.	s **Antrag zu Art. 7 Abs. 2**: Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Die Pflichten des Auftragsbearbeiters ergeben sich aus den Pflichten des Verantwortlichen und des zwischen diesem und dem Auftragsbearbeiter abgeschlossenen Vertrags. **Antrag zu Art. 7 Abs. 3**: Schaffung der Möglichkeit einer generellen Einwilligung.
Art. 8 Empfehlungen der guten Praxis [1] Der Beauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen. [2] Der Verantwortliche sowie interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie. [3] Er veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.	**Antrag zu Art. 8**: Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der von diesem vordefinierten "interessierten Kreise" – erfahrungsgemäss ist die Zusammenstellung von solchen *Round Tables* „interessierter Kreise“ völlig willkürlich und intransparent – ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. Es ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen *tel quel* als Ermessensindikator zugrunde legen werden. Der Beauftragte wird damit im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich faktisch gemäss seinen Eindrücken Recht setzen. Dies wiegt umso schwerer, als der Beauftragte nicht einmal Jurist oder Anwalt sein oder über Erfahrungen in der Unternehmensjurisprudenz verfügen muss.
Art. 9 Einhaltung der Empfehlungen der guten Praxis [1] Befolgt der Verantwortliche die Empfehlungen der guten Praxis, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren. [2] Die Datenschutzvorschriften können auch auf andere Weise eingehalten werden, als in Empfehlungen der guten Praxis vorgesehen.	**Antrag zu Art. 9**: Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zu Lasten des Datenbearbeiters führen.

VE-DSG	Anträge und Bemerkungen
Art. 10 Zertifizierung [1] Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen. [2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.	Keine Bemerkungen
Art. 11 Sicherheit von Personendaten [1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden. [2] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.	Keine Bemerkungen
Art. 12 Daten einer verstorbenen Person [1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und: a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder b. keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen. [2] Ein schutzwürdiges Interesse wird bei Personen vermutet, die mit der verstorbenen Person in gerader Linie verwandt sind oder mit ihr bis zum Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten. [3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.	**Antrag I zu Art. 12**: Die Bestimmung ist aus dem VE zu entfernen und die Thematik in die aktuell laufende Revision des Erbrechts zu integrieren. Derart weitreichende, thematisch in einem allgemeinen Datenschutzgesetz nicht zu erwartende Regularien als Folge des Todes gehören dorthin, wo der Tod und dessen Folgen abgewickelt werden. Das ist das allgemeine Erbrecht. Die dort zu erlassenden datenschutzrechtlichen Bestimmungen sind *lex specialis* zum DSG. Weiter ist die gesamte Bestimmung voll von schwerwiegenden Unklarheiten: Wer urteilt über das Vorliegen überwiegender Interessen der verstorbenen Person? Wer über die überwiegenden Interessen Dritter? Wie verhält sich das schutzwürdige Interesse zum überwiegenden Interesse Dritter? Weiter ist die Verknüpfung des schutzwürdigen Interesses mit Verwandtschaftsgraden unbegründet und willkürlich. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären. Es gäbe unzählige weitere Beispiele. Art. 4 Abs. 1 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen. **Antrag II zu Art. 12 Abs. 3**: Die Bestimmung ist gerade umzukehren. Sie ist abzuändern, dass im Zusammenhang mit dem Vollzug dieser Bestimmung Amts- und Berufsgeheimnisse von Geheimnisträgern jederzeit geltend gemacht werden können. Alles andere wäre absurd: Es gäbe zahlreiche Beispiele, die dramatische Konsequenzen zur Folge hätten. Man denke nur an den Fall, in

VE-DSG	Anträge und Bemerkungen
[4] Jeder Erbe kann verlangen, dass der Verantwortliche Personendaten des Erblassers kostenlos löscht oder vernichtet, ausser: a. der Erblasser hat dies zu Lebzeiten ausdrücklich untersagt; oder b. der Löschung oder Vernichtung stehen überwiegende Interessen des Erblassers oder von Dritten entgegen. [5] Vorbehalten bleiben spezielle Bestimmungen anderer Bundesgesetze.	welchem ein Mitglied einer zerstrittenen Erbengemeinschaft den Vertrauensanwalt des Verstorbenen nötigen würde, ihm Einsicht in die Personendaten zu geben, die er dann auch noch auf Geheiss vernichten müsste. **Antrag zu Art. 12 Abs. 4**: Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und Löschungsrecht völlig ausreichen. **Bemerkung zu Art. 12 Abs. 5**: Es ist bezeichnend, dass genau bei dieser Bestimmung noch einmal explizit betont wird, was gemäss Art. 2 VE ohnehin generell gilt. Diese Bestimmung steht mit zahlreichen spezialgesetzlichen Regelungen komplett im Widerspruch. Insofern ist der Sinn einer solchen allgemeinen Datenschutzklausel im Zusammenhang mit Verstorbenen nicht ersichtlich.
3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters	**Vorbemerkungen**: - Es fehlt an Übergangsbestimmungen, welche regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar und führt über Jahre hinweg zu grossen Unsicherheiten in der Praxis. - Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention – und nicht die DSGVO – den Massstab für die Angemessenheit des Datenschutzes zu liefern haben.
Art. 13 Informationspflicht bei der Beschaffung von Personendaten [1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. [2] Er teilt der betroffenen Person spätestens bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten; c. den Zweck der Bearbeitung.	**Antrag zu Art. 13 Abs. 1 und 2:** Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird zwar festgehalten, es genüge eine solche "allgemeine Information". Das ist allerdings im Wortlaut der Bestimmung nicht ersichtlich. In der vorliegenden Form ist die Bestimmung nicht praktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. In der Telekommunikationsbranche ist dies selbst mit solchen Massenschreiben nicht möglich, weil regelmässig Personendaten bearbeitet werden, mit welchen ein Dienstanbieter nie in einem direkten Kontakt

VE-DSG	Anträge und Bemerkungen
	steht. Die Bestimmung ist schlicht nicht umsetzbar und schiesst über das Ziel hinaus: Selbst die insgesamt absolut ungenügende Analyse der Regulierungskostenfolgeabschätzung von PWC hält dies so fest.
[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.	**Antrag zu Art. 13 Abs. 3** Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist nicht akzeptierbar. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, in welchen persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger jeder Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen.
[4] Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die er bearbeitet, mit.	**Antrag zu Art. 13 Abs. 4**: Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
[5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden; werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.	**Antrag zu Art. 13 Abs. 5**: Ersatzlos streichen. *Eventualiter* ist die aktive Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten zu beschränken. Die vorgesehene uferlose Informationspflicht ist schlicht nicht umsetzbar und – selbst wenn diese umsetzbar wäre – völlig unverhältnismässig. Hinzu kommt, dass die Bestimmung sogar noch weiter geht als die DSGVO, die immerhin noch einen Monat Frist gewährt. Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird. Weiter muss man sich bei diesem Konzept auch die Auswirkungen auf Konsumentenseite vor Augen führen: Da in Zukunft praktisch kein Wirtschaftszweig mehr ohne die Beschaffung und Bearbeitung von Personendaten auskommen wird, wird der Konsument mit solchen Informationen regelrecht zugespamt werden. Die einzelne Information versinkt im Informationsmeer. Der Adressat wird abgestumpft und negiert die diesem Informationswahn zu Grunde gelegten Absichten, den Adressaten vor „bösen“ Datenbearbeitern zu schützen.
Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen [1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt.	**Bemerkung**: Wurde unnötigerweise enger als die SEV 108 gefasst. **Antrag zu Art. 14 Abs. 1:** Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung),

VE-DSG	Anträge und Bemerkungen
[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn: a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.	in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist. **Antrag zu Art. 14 Abs. 2**: 1. Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der VE für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
[3] Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn: a. ein Gesetz im formellen Sinn dies vorsieht; oder b. dies aufgrund überwiegender Interessen Dritter erforderlich ist.	
[4] Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten: a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt; b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls eine der folgenden Voraussetzungen erfüllt ist: 1. es ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich; oder 2. die Übermittlung der Information stellt den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage.	**Antrag zu Art. 14 Abs. 4 lit. a**: Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns (der als Dritter gilt) unnötig erschwert.
II. [5] Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	
Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung [1] Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.	**Antrag zu Art. 15 Abs. 1**: Streichen. *Eventualiter* ist die Bestimmung um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a DSGVO EU (2016/679) zu ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als untauglicher Versuch, Konsumenten vor jeder Art automatisiert getroffener Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche“ Auswirkung ist, dürfte letztlich von der Sensibilität des Be-

VE-DSG	Anträge und Bemerkungen
	troffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte. Die saloppe Begründung im Erläuterungsbericht „denn solche Entscheidungen sind in allen Wirtschaftsbereichen immer häufiger und werden teilweise auf der Grundlage falscher Daten getroffen“ reicht jedenfalls nicht aus, einer solchen weitreichenden Bestimmung ein öffentliches Interesse mitzugeben. Art. 22 DSGVO nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor. Eine von der DSGVO abweichende Regelung wäre demnach zweifellos auch für die Schweiz zulässig. Es ist nicht nachvollziehbar, weshalb hier ein „Swiss Finish“ erfolgt. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung seit der Gründung des Bundesstaates frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Das hat nichts damit zu tun, ob die Grundlage für einen solchen Entscheid aus Papier, aus Menschen oder aus Algorithmen stammt.
[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.	**Antrag zu Art. 15 Abs. 2**: Streichen. Wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand für die gesamte Schweizer Wirtschaft. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens.
[3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.	**Antrag zu Art. 15 Abs. 3**: Streichen. Es ist nicht nachvollziehbar, weshalb gerade der Staat automatisierte Entscheidungen ohne Informations- und Anhörungspflicht durchführen darf. Das Handeln des Staates ist an die Einhaltung von Grundrechten geknüpft. Diese Bestimmung zeugt von einem sehr gefährlichen Grundverständnis der Gesetzesredaktoren: Hier der gute Staat, dort die böse Wirtschaft. Es ist daran zu erinnern, dass solche Ausnahmen für staatliches Handeln vor allem Mittel totalitärer Staaten sind, sich für nichts rechtfertigen zu müssen.
Art. 16 Datenschutz-Folgenabschätzung [1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen. [2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern.	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschätzungen bei jeder beliebigen Datenbearbeitung vornehmen zu müssen; abgesehen davon muss die Abschätzung ohnehin durchgeführt werden, um herauszufinden, ob die Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit führt. Die Kosten sind angefallen, selbst wenn man zum Schluss käme, dass gar keine Risiken bestehen. Hier wird ein bürokratisches Monstrum freigesetzt,

VE-DSG	Anträge und Bemerkungen
[3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen. [4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit.	das in der Privatwirtschaft im Ergebnis nichts ausser gigantischen Kosten bringen wird. Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier, Zeit und Geld dafür aufwenden müssen. Denn anders als der Bund, der – wie im vorliegenden Fall – meint, mit wenig Geld eine verfassungskonforme Regulierungskostenfolgenabschätzung machen zu können, hat der private Datenbearbeiter mit seiner Existenz gerade zu stehen, wenn er einer solchen Verpflichtung nicht im Sinne des Gesetzes nachkommen sollte. **Antrag zu Art. 16 Abs. 3 und 4**: Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist ist weiter viel zu lang und zeugt nicht von einem Verständnis wirtschaftlicher Prozesse. Wenn es bei solchen Folgeabschätzungen Beanstandungen gibt, dann hat der Beauftragte Einwände innert 7 Tagen zu adressieren, ansonsten Geschäftsprozesse während Monaten blockiert bleiben müssen. Wir weisen dazu auch darauf hin, dass allein die Überprüfung der zu erwartenden Schwemme solcher Meldungen, ein Herr von neuen Beamten erforderlich machen wird, die nichts anderes tun, als solche Folgeabschätzungen zu prüfen.
Art. 17 Meldung von Verletzungen des Datenschutzes [1] Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.	**Antrag zu Art. 17**: Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien unseres Rechtsstaates. Es ist nicht zu rechtfertigen, dass diese Garantie gerade im Datenschutzrecht nicht mehr gewährleistet werden soll; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer Flut von Selbstanzeigen zu rechnen, die erneut nur den Apparat des Beauftragten übermässig aufblähen würde. Diese aus den USA bekannten Regulierungsmechanismen sollten in der Schweiz nicht angefasst werden. Der Druck auf die Verantwortlichen wäre enorm und würde ein pragmatisches und/oder vernunftgetriebenes Handeln von vornherein ausschliessen. Die Selbstanzeige ist in einem solchen System immer die sicherste Art, sich prophylaktisch „compliant“ zu verhalten.

VE-DSG	Anträge und Bemerkungen
[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. [3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. [4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung.	**Antrag zu Art. 17 Abs. 2**: Streichung; In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen. **Bemerkung zu Art. 17 Abs. 4**: Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen [1] Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. [2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.	**Antrag zu Art. 18**: Streichung. Die Bestimmung ist redundant. Der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Art. 19 Weitere Pflichten Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie dokumentieren ihre Datenbearbeitung; b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.	**Antrag zu Art. 19**: Streichung; Die Bestimmung ist nicht nur überflüssig, sondern teilweise nicht umsetzbar. Die stipulierte Dokumentationspflicht würde insbesondere für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b ist von vornherein nicht umsetzbar. Teilweise lassen sich dagegen auch absurde Beispiele vorbringen: Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine allfällige Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gemäss Art. 25 machen zu müssen. Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Auch hier gilt es, sich auch in die Situation der Informationsadressaten zu versetzen. Dass Millionen unnützer Mitteilungen versandt werden ist das eine; dass aber jeder Einzelne tausende solcher Informationen von allen Datenbearbeitern erhält, das andere. Diese Informationen sind die neuen „Spam Waves“ und werden bei den Adressaten keinerlei Wirkung erzielen, geschweige denn, diese in ihren Persönlichkeiten schützen.
4. Abschnitt: Rechte der betroffenen Person	
Art. 20 Auskunftsrecht	

VE-DSG	Anträge und Bemerkungen
[1] Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. [2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten; c. der Zweck der Bearbeitung; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; e. das Vorliegen einer automatisierten Einzelentscheidung;	**Antrag zu Art. 20 Abs. 2 lit e)**: Streichen; in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich(vgl. auch den Antrag zu Art. 15).
f. die verfügbaren Angaben über die Herkunft der Personendaten;	**Antrag zu Art. 20 Abs. 2 lit. f)**: Streichen; die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntgeben zu müssen, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen.
g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4.	
[3] Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.	**Antrag zu Art. 20 Abs. 3**: Streichen; *eventualiter* ist Abs. 3 auf die Pflicht zu beschränken, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt: Entweder wird ein Vertrag geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, eine Begründungspflicht für den Nicht-Abschluss von Verträgen über das Datenschutzrecht einzuführen. Das kann nicht das Ziel des Datenschutzes sein. Die Verweigerung von Geschäftsbeziehungen ist ausschliesslich ein wettbewerbs- und lauterkeitsrechtlicher Tatbestand. Es ist lebensfremd, wenn man heute meint, allein durch eine modernere Datenbearbeitung würden Fehler bei der Einschätzung von geschäftlichen Tätigkeiten verursacht. Die Frage, ob zwei Personen miteinander kontrahieren, basierte seit jeher auf der Einschätzung von „Personendaten“ und „Persönlichkeitsprofilen“. Es kam bislang niemand auf die Idee, im allgemeinen oder im besonderen Teil des OR eine Begründungspflicht für den Nicht-Abschluss eines Vertrages zu fordern. Vielfach wird gerade deshalb kein Vertrag geschlossen, weil die persönliche Chemie nicht stimmt. In den seltenen Fällen wird dies der anderen Seite so direkt mitgeteilt. Wieso es weiter für den Schutz der Persönlichkeit erforderlich sein soll, dem Betroffenen die Auswirkungen eines Nicht-Entscheids zu erläutern, ist völlig unerfindlich, wenn

VE-DSG	Anträge und Bemerkungen
[4] Personendaten über die Gesundheit können der betroffenen Person durch einen von ihr bezeichneten Arzt mitgeteilt werden. [5] Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat. [6] Niemand kann im Voraus auf das Auskunftsrecht verzichten.	nicht gleichzeitig eine Rechtsmittelmöglichkeit besteht, die am Ende in einen Vertragszwang münden könnte. Beides wird zum Glück und konsequenterweise (jedoch im Kontext aller anderen Ideen fast schon überraschend) nicht gefordert.
Art. 21 Einschränkung des Auskunftsrechts [1] Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. [2] Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.	Keine Bemerkungen
Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende [1] Werden Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben: a. Die Daten geben Aufschluss über die Informationsquellen; b. Es müsste dafür Einsicht in Entwürfe für Publikationen gewährt werden; c. Die freie Meinungsbildung des Publikums würde gefährdet. [2] Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.	Keine Bemerkungen
5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen	
Art. 23 Persönlichkeitsverletzungen [1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. [2] Eine Persönlichkeitsverletzung liegt insbesondere vor: a. wenn Personendaten entgegen den Grundsätzen nach den Artikeln 4-6 und 11 bearbeitet werden; b. wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden; c. wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden; d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.	**Antrag zu Art. 23 Abs. 2 lit d)**: Streichung; zum Profiling vgl. Bemerkungen zu Art. 3 lit. f VE.

VE-DSG	Anträge und Bemerkungen
[3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	**Bemerkung zu Art. 23 Abs. 3**: Streichung des zweiten Teils „und eine Bearbeitung nicht ausdrücklich untersagt hat“. Was einmal allgemein zugänglich gemacht worden ist, kann später nicht mehr widerrufen werden.
Art. 24 Rechtfertigungsgründe [1] Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. [2] Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere: a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet; b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben; c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn: 1. es sich dabei nicht um besonders schützenswerte Personendaten handelt, 2. Dritten nur Daten bekanntgegeben werden, welche diese für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen, 3. die betroffene Person volljährig ist; d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet; e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet, soweit: 1. die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt, 2. Dritten besonders schützenswerte Personendaten so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind, 3. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind; f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.	**Antrag I zu Art. 24 Abs. 2, erster Satz**: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit. **Antrag II zu Art. 24 Abs. 2. lit a)**: Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft Abgrenzungsfragen auf, für welche der VE keine Antworten liefert. **Antrag zu Art. 24 Abs. 2 lit. c) Ziff. 3**: Streichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar (Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft). Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit Sicherheit bestimmbar.
Art. 25 Rechtsansprüche [1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs. Die klagende Partei kann insbesondere verlangen, dass:	

VE-DSG	Anträge und Bemerkungen
a. die Datenbearbeitung verboten wird; b. die Bekanntgabe von Personendaten an Dritte untersagt wird; c. Personendaten berichtigt, gelöscht oder vernichtet werden. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die klagende Partei verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird. Sie kann darüber hinaus verlangen, dass die Bearbeitung der bestrittenen Daten eingeschränkt wird. [3] Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.	**Antrag Art. 25 lit. a) bis c)**: Es müsste klargestellt werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. Ansonsten kann die Bestimmung nicht umgesetzt werden. **Antrag Art. 25 Ziff. 2**: Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", *eventualiter* Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis schiefe Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat. **Antrag Art. 25 Ziff. 3**: Ziff. 3. streichen. Lit. a) bis c) reichen völlig, um die Interessen der Betroffenen zu wahren. Auch die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor.
6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane	
Art. 26 Verantwortliches Organ und Kontrolle [1] Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt. [2] Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.	Keine Bemerkungen
Art. 27 Rechtsgrundlagen [1] Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. [2] Für die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Eine Grundlage in einem Gesetz im materiellen Sinn ist ausreichend, wenn die folgenden Voraussetzungen erfüllt sind: a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn klar festgelegte Aufgabe unentbehrlich; und b. Die Bearbeitung birgt für die Persönlichkeit und die Grundrechte der betroffenen Person keine besonderen Risiken. [3] In Abweichung von den Absätzen 1 und 2 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Der Bundesrat bewilligt die Bearbeitung, sofern die Rechte der betroffenen Person nicht gefährdet sind; b. Die betroffene Person hat in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt;	**Antrag zu Art. 15 Abs. 2**: Streichen „oder den Erlass einer automatisierten Einzelfallentscheidungen nach Artikel Art. 15 Absatz 1“ (vgl. dazu den Kommentar zu Art. 15 Abs. 2): Damit würde jede Prozessautomatisierung und -optimierung in der Verwaltung massiv erschwert. Es stellt sich grundsätzlich auch die Frage, ob als Grundlage für die Datenbearbeitung nicht auch Regelungen auf Verordnungsstufe ausreichen sollten.

VE-DSG	Anträge und Bemerkungen
c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.	
Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen [1] Der Bundesrat kann vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling bewilligen, wenn: a. die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz im formellen Sinn geregelt sind; b. ausreichende Massnahmen getroffen werden, um eine Verletzung der Grundrechte der betroffenen Person zu verhindern; und c. eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, zwingend erforderlich ist. [2] Er holt vorgängig die Stellungnahme des Beauftragten ein. [3] Das zuständige Bundesorgan legt dem Bundesrat spätestens innerhalb von zwei Jahren nach Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor. [4] Die automatisierte Datenbearbeitung oder das Profiling müssen in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage umfasst.	**Antrag zu Art. 28 Abs. 1 und 2**: Die Bestimmung ist entweder zu streichen, oder die entsprechenden Möglichkeiten ist auch Privaten zu eröffnen.
Art. 29 Bekanntgabe von Personendaten [1] Bundesorgane dürfen Personendaten bekannt geben, wenn eine Rechtsgrundlage im Sinne von Artikel 27 Absätze 1 und 2 dies vorsieht. [2] In Abweichung von Absatz 1 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten bekannt geben, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich; b. Die betroffene Person hat in die Bekanntgabe eingewilligt; c. Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; d. Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt; e. Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben, wenn: a. die betreffenden Daten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen; und b. an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. [4] Name, Vorname, Adresse und Geburtsdatum einer Person dürfen Bundesorgane auf Anfrage auch bekannt geben, wenn die Voraussetzungen von Absatz 1 oder 2 nicht erfüllt sind. [5] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 3 bekannt geben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst gelöscht. [6] Sie lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn: a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.	
Art. 30 Widerspruch gegen die Bekanntgabe von Personendaten [1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen. [2] Das Bundesorgan weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist: a. es besteht eine Rechtspflicht zur Bekanntgabe; b. die Erfüllung seiner Aufgabe wäre sonst gefährdet. [3] Artikel 29 Absatz 3 bleibt vorbehalten.	Keine Bemerkungen
Art. 31 Angebot von Unterlagen an das Bundesarchiv [1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998 bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen. [2] Sie vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese: a. anonymisiert sind; b. zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.	Keine Bemerkungen
Art. 32 Datenbearbeitung für Forschung, Planung und Statistik [1] Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn: a. die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt;	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
b. das Bundesorgan privaten Personen besonders schützenswerte Personendaten so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind; c. die Empfängerin oder der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und d. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. [2] Die Artikel 4 Absatz 3, 27 Absätze 1 und 2 sowie Artikel 29 Absatz 1 sind nicht anwendbar.	
Art. 33 Privatrechtliche Tätigkeit von Bundesorganen [1] Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen. [2] Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.	Keine Bemerkungen
Art. 34 Ansprüche und Verfahren [1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es: a. die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt; b. die Folgen einer widerrechtlichen Bearbeitung beseitigt; c. die Widerrechtlichkeit der Bearbeitung feststellt. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so muss das Bundesorgan bei den Daten einen Bestreitungsvermerk anbringen und deren Bearbeitung einschränken. [3] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan: a. die betreffenden Personendaten berichtigt, löscht oder vernichtet; b. seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, das Verbot der Bearbeitung, den Widerspruch gegen die Bekanntgabe nach Artikel 30 oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht. [4] Die Berichtigung, Löschung oder Vernichtung von Personendaten kann nicht verlangt werden in Bezug auf die Bestände öffentlich zugänglicher Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderer öffentlicher Gedächtnisinstitutionen. Wenn die Gesuchstellerin oder der Gesuchsteller ein überwiegendes Interesse nachweisen kann, kann sie oder er jedoch verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt. [5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.	Keine Bemerkungen
Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Öffentlichkeitsgesetzes hängig, so kann die betroffene Person im Rahmen dieses Verfahrens diejenigen Rechte geltend machen, die ihr nach Artikel 34 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.	Keine Bemerkungen
Art. 36 Register [1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [2] Der Beauftragte führt ein Register der Datenbearbeitungstätigkeiten. Das Register ist öffentlich.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.	
7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte	
Art. 37 Ernennung und Stellung [1] Die oder der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen. [2] Das Arbeitsverhältnis der oder des Beauftragten richtet sich, soweit dieses Gesetz nichts anderes vorsieht, nach dem Bundespersonalgesetz vom 24. März 2000 (BPG). [3] Die oder der Beauftragte übt ihre bzw. seine Funktion unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder zu erhalten. Sie oder er ist administrativ der Bundeskanzlei zugeordnet. [4] Sie oder er verfügt über ein ständiges Sekretariat und ein eigenes Budget. Sie oder er stellt sein Personal an. [5] Die oder der Beauftragte unterstehen nicht dem Beurteilungssystem nach Artikel 4 Absatz 3 BPG.	**Antrag zu Art. 37 Abs. 1**: Dem Bundesrat soll ein Vorschlagsrecht zukommen und die Wahl soll durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Amtsdauer von 4 Jahren gewählt". Was die blosse Genehmigung einer Wahl bringen soll, ist nicht ersichtlich. Die Person des Beauftragten soll über grosse Kompetenzen und einen Wirkungsgrad mit erheblichen finanziellen Auswirkungen auf die Schweizer Wirtschaft verfügen. In Anbetracht des zukünftigen, angedachten Gewichts dieses Posten, ist eine Wahl durch das Parlament gerechtfertigt. **Antrag zu Art. 37 Abs. 4**: Das Budget wird durch das Parlament genehmigt.
Art. 38 Wiederwahl und Beendigung der Amtsdauer [1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden. [2] Verfügt der Bundesrat nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl, so ist der oder die Beauftragte für eine neue Amtsdauer wiedergewählt. [3] Die oder der Beauftragte kann den Bundesrat unter Einhaltung einer Frist von sechs Monaten um Entlassung auf ein Monatsende ersuchen. [4] Der Bundesrat kann die Beauftragte oder den Beauftragten vor Ablauf der Amtsdauer des Amtes entheben, wenn diese oder dieser: a. vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder b. die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.	**Antrag zu Art. 38 Abs. 2**: Der oder die Beauftragte ist für jede Amtsperiode neu zu wählen. Das Verfahren über eine Verfügung kommt einem Kündigungsverfahren gleich, das in der Praxis nur aus wichtigen Gründen möglich ist. Das Wahlorgan soll in seiner Wahl wirklich frei sein.
Art. 39 Nebenbeschäftigung [1] Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, der Verwaltung, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein. [2] Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1 auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.	**Antrag zu Art. 39 Abs. 2**: Solche Bewilligungen von Nebenbeschäftigung sind offenzulegen. Für die Vermeidung von Interessenkonflikten ist absolute Transparenz unabdingbar.
Art. 40 Aufsicht	Keine Bemerkungen.

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte überwacht die Einhaltung der Datenschutzvorschriften des Bundes. [2] Bundesverwaltungsbehörden, die nach einem anderen Bundesgesetz Private oder Organisationen ausserhalb der Bundesverwaltung beaufsichtigen, laden den Beauftragten zur Stellungnahme ein, bevor sie eine Verfügung treffen, die Fragen des Datenschutzes berührt. [3] Führt der Beauftragte gegen die gleiche Partei ein eigenes Verfahren, so haben die beiden Behörden ihre Verfahren zu koordinieren.	
Art. 41 Untersuchung [1] Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.	
[2] Das Bundesorgan oder die private Person erteilt dem Beauftragten die von ihm verlangten Auskünfte und stellen ihm alle für die Untersuchung notwendigen Unterlagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes.	**Antrag zu Art. 41 Abs. 2**: Hier ist zu ergänzen, dass bei Untersuchungen gegen Private alle Untersuchungsakten nicht dem Öffentlichkeitsgesetz unterliegen, da ansonsten über diesen Umweg Betriebsgeheimnisse an Dritte gelangen könnten. Wenn Unternehmen verpflichtet sind, dem Beauftragten alle notwendigen Unterlagen zur Verfügung zu stellen, muss es die Garantie haben, dass diese nicht veröffentlicht werden. Der Beauftragte veröffentlicht bei Untersuchungen gegen private Personen nur die Empfehlung.
[3] Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte vergeblich versucht, Auskünfte und Unterlagen einzuholen, so kann der Beauftragte im Rahmen einer Untersuchung: a. ohne Vorankündigung Räumlichkeiten inspizieren; b. Zugang zu allen notwendigen Daten und Informationen verlangen.	**Antrag zur Art. 41 Abs. 3**: Diese Bestimmung ist nur akzeptabel, wenn das Unternehmen Rechtsmittel gegen die Auskunftsverfügung hat. Eine unbestimmte Verletzung von Mitwirkungspflichten darf nicht zu Strafsanktionen oder publizitätswirksamen Aktionen des Beauftragten gegen Unternehmen führen. Bevor solche Massnahmen ergriffen werden, muss eine Editionsverfügung des Beauftragten einer gerichtlichen Überprüfung zugänglich sein.
[4] Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten.	**Antrag zu Art. 41 Abs. 4**: Streichen „private Personen“. Ein Tätigwerden des Beauftragten gegenüber Privaten ohne Anzeige einer Datenschutzverletzung ist strikt abzulehnen. Wenn Anhaltspunkte vorliegen, kann der Beauftragte nach Art. 41 Abs. 1 formell vorgehen. Es dürfen hier keine mehrgleisigen Verfahren ohne Rechtsschutz für die betroffenen Parteien eingefügt werden. Im Gegenteil, es müsste für Unternehmen möglich sein, Sachverhalte rechtsverbindlich durch den Beauftragten überprüfen und mittels Attest der Datenrechtskonformität genehmigen zu lassen.
[5] Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung.	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Parteistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte Abs. 5 auch gestrichen werden.
Art. 42 Vorsorgliche Massnahmen	

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern. [2] Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.	**Antrag zu Art. 42 Abs. 1**: Ändern: Der Beauftragte kann beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen. Vorsorgliche Massnahmen sind – auch im Persönlichkeitsschutz – immer Sache der Gerichte. Hier ist die bisherige Regelung mit dem Antrag beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts beizubehalten. Es sollte hier nicht von den bewährten rechtsstaatlichen Prozessen abgewichen werden. Jedenfalls gibt es dazu keine ausreichenden Rechtfertigungsgründe.
Art. 43 Verwaltungsmassnahmen [1] Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden. [2] Der Beauftragte kann zudem die Bekanntgabe ins Ausland aufschieben oder untersagen, wenn sie gegen die Voraussetzungen nach Artikel 5 oder 6 oder gegen spezifische Bestimmungen betreffend die Bekanntgabe von Personendaten ins Ausland in anderen Bundesgesetzen, verstösst.	**Antrag zu Art 43 Abs. 1**: Ändern: Anstelle der Empfehlung und des nachfolgenden Gerichtswegs wie im heutigen Recht wird hier auch die Klage- und Beweislast umgekehrt. Das ist abzulehnen. Der Beauftragte hat in der Verfügung die Rechtsverletzung nachzuweisen. Eine Verfügung sollte nur nach der Durchführung einer Untersuchung zulässig sein, in welchem dem betroffenen Datenbearbeiter selbstverständlich auch das rechtliche Gehör gewährt wurde. Eine Datenvernichtung darf nicht durch den Beauftragten angeordnet werden können, da dies nicht wieder gutzumachende Folgen hat (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 41 reicht zum Schutz Betroffener völlig aus.
Art. 44 Verfahren [1] Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz. [2] Partei sind lediglich das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wurde. [3] Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt keine aufschiebende Wirkung zu.	**Antrag zu Art. 44 Abs. 2**: Drittpersonen haben keine Parteistellung und kein Akteneinsichtsrecht, was zu begrüssen ist. Zu ergänzen ist weiter, dass Untersuchungsunterlagen nicht dem Öffentlichkeitsgesetz unterliegen dürfen. **Antrag zu Art. 44 Abs. 3**: Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Vielmehr wäre vorzusehen, dass die aufschiebende

VE-DSG	Anträge und Bemerkungen
[4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.	Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt nicht praktikable Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Art. 45 Anzeigepflicht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.	**Antrag zu Art. 45**: Streichen. Ein Recht zur Anzeige würde völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE).
Art. 46 Amtshilfe zwischen schweizerischen Behörden [1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses Gesetzes erforderlich sind. [2] Der Beauftragte gibt den folgenden Behörden die Informationen und Personendaten bekannt, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind: a. den für den Datenschutz zuständigen kantonalen Behörden; b. den zuständigen Strafverfolgungsbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 45 geht; c. den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss Artikel 41 Absatz 3, 42 und 43.	**Antrag zu Art. 46 Abs. 2**: Hier ist zu ergänzen, dass Informationen die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen.
Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden [1] Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen: a. die Identität des Verantwortlichen, des Auftragsbearbeiters oder anderer beteiligter Dritter; b. Kategorien von betroffenen Personen; c. die Identität der betroffenen Personen, falls: 1. die betroffenen Personen eingewilligt haben, oder 2. die Mitteilung der Identität der betroffenen Personen unumgänglich ist, um die gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde zu erfüllen; d. bearbeitete Personendaten oder Kategorien von bearbeiteten Personendaten; e. den Zweck der Datenbearbeitung; f. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern; g. technische und organisatorische Massnahmen. [2] Der Beauftragte kann der ausländischen Behörde Amtshilfe gewähren und ihr die Informationen gemäss Absatz 1 zur Verfügung stellen, wenn sie folgende Voraussetzungen erfüllt: a. Sie verpflichtet sich, die zur Verfügung gestellten Informationen und Personendaten, nicht für andere Zwecke zu verwenden, als im Amtshilfegesuch angegeben; b. Sie verpflichtet sich, ähnlichen Amtshilfegesuchen der Schweiz Folge zu leisten;	**Antrag zu Art. 47 Abs. 1**: Auch hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen, insbesondere auch für Informationen, die in der Schweiz dem Berufsgeheimnis unterliegen. Die Herausgabe vertraulicher Unternehmensdaten darf nicht im Ermessen des Beauftragten liegen, sondern – wenn überhaupt – nur mit Zustimmung des betroffenen Unternehmens zulässig sein.

VE-DSG	Anträge und Bemerkungen
c. Sie verpflichtet sich zur Wahrung des Amts- und Berufsgeheimnisses; d. Sie verpflichtet sich, die erhaltenen Informationen und Personendaten nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln; e. Sie verpflichtet sich, die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten.	
Art. 48 Information [1] Der Beauftragte erstattet der Bundesversammlung periodisch sowie bei Bedarf Bericht. Er übermittelt den Bericht gleichzeitig dem Bundesrat. Die periodischen Berichte werden veröffentlicht. [2] In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über seine Feststellungen und Verfügungen.	**Antrag zu Art. 48 Abs. 2**: Streichen des Begriffs „seine Feststellungen und Verfügungen“ und ersetzen mit „seine Untersuchungen“. Damit der Beauftragte die Persönlichkeitsrechte wahrt, soll er nur über die Tatsache einer Untersuchung informieren. Es ist nicht ersichtlich, weshalb der Beauftragte zur Profilierung von Amt und Person ein öffentliches Prangerrecht haben soll.
Art. 49 Weitere Aufgaben Der Beauftragte nimmt darüber hinaus insbesondere folgende Aufgaben wahr: a. Er informiert und berät die Organe des Bundes und der Kantone sowie private Personen bei Fragen des Datenschutzes. b. Er arbeitet mit schweizerischen und ausländischen Behörden, die für den Datenschutz zuständig sind, zusammen. c. Er sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz. d. Er erteilt der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann. e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen. f. Er nimmt die ihm durch das Öffentlichkeitsgesetz übertragenen Aufgaben wahr.	**Antrag zu Art. 49 lit. d**: Streichen. Wenn der Datenschutzbeauftragte eine Aufsichtsfunktion hat, kann er nicht gleichzeitig auch eine Konsumentenschutzaufgabe erfüllen dürfen.
8. Abschnitt: Strafbestimmungen	**Antrag zum 8. Abschnitt (Art. 50ff)**: Das gesamte Sanktionssystem ist zu überarbeiten. Es führt zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden und Unternehmen. Unverständlich ist zudem, dass gerade die Verwaltung von den Strafsanktionen ausgenommen werden soll. Es wird komplett vergessen und ausgeblendet, dass vor noch nicht langer Zeit, die Gefahr im Umgang mit Daten nicht von Privaten und nicht von Unternehmen, sondern vom Staat selbst ausgegangen ist (Stichwort: Fichen-Affäre). Es wäre naiv zu glauben, dass sich diese Bedrohung in den letzten 20 Jahren komplett verflüchtigt hätte. Mit einer zunehmend

VE-DSG	Anträge und Bemerkungen
	hohen Verwaltungsquote von gegen 40% wäre ein sehr hoher Anteil der Berufstätigen vom Sanktionssystem ausgenommen. Das ist höchst zweifelhaft und politisch nicht zu rechtfertigen. Alternative: Der Beauftragte soll als Aufsichtsbehörde untersuchen und verfügen können. Unternehmen sollen sich in diesem verwaltungsrechtlichen Verfahren wehren können. Erst wenn rechtskräftige Entscheide nicht umgesetzt worden sind, sollten Strafsanktionen greifen. Es besteht kein Rechtfertigungsgrund, von diesem in anderen Belangen des Bundesrechts verankerten Prinzip abzuweichen.
Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten [1] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft: a. die ihre Pflichten nach den Artikeln 13, 15 und 20 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;	**Antrag zu Art. 50**: Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen. Der Bussenrahmen ist auf eine maximale Höhe von CHF 5'000.- bzw. – im Wiederholungsfall – auf maximal CHF 10'000.- zu begrenzen. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen anzusetzen, sicher nicht Beträge bis CHF 500'000.-. Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.- für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Grössenordnungen. Bussenbeträge über CHF 100'000.- sind bislang in der Schweiz nicht bekannt. Die Erhöhung des Strafrahmens auf CHF 500‘000.- ist daher völlig überrissen und nicht nachvollziehbar.
b. die es vorsätzlich unterlassen: 1. die betroffene Person nach Artikel 13 Absätze 1 und 5, 15 und 17 Absatz 2 die betroffene Person zu informieren; oder 2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2, 3 und 4 zu liefern.	**Antrag zu Art. 50 Abs. 1 lit. b)**: Ändern. Art 13 ist vollständig von der Sanktionierung auszunehmen.
c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3).	**Antrag zu Art. 50 Abs. 1 lit. c)**: Streichen. Ist vollständig von der Sanktionierung auszunehmen.
[2] Mit Busse bis zu 500 000 Franken werden private Personen bestraft, wer vorsätzlich: a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b und Absatz 6 zu informieren; b. die es unterlassen, dem Beauftragten die standardisierten Garantien oder die verbindlichen unternehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d Ziff. 1);	**Antrag zu Art. 50 Abs. 2, lit. a) und b)**: Streichen. Da die Meldepflicht sowieso massiv reduziert werden müssen, ist auch diese Bestimmung zu streichen.

VE-DSG	Anträge und Bemerkungen
c. dem Beauftragten bei der Untersuchung (Art. 41 Abs. 2) falsche Auskünfte erteilen oder die Mitwirkung verweigern; e. es unterlassen, dem Beauftragten Verletzungen des Datenschutzes nach Artikel 17 Absatz 1 zu melden; f. einer Verfügung des Beauftragten nicht Folge leistet. [3] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft, die es vorsätzlich unterlassen: a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren; b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 zu informieren. [4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**Antrag zu Art. 50 Abs. 2, lit. e)**: Ändern. Diese Bestimmung ist auf Vorfälle zu beschränken, die schwerwiegend sind und mehr als 1‘000 Personen betreffen. **Antrag zu Art. 50 Abs. 2, lit. f**: Streichen. Hier genügt die bestehende Strafbestimmung im StGB. **Antrag zu Art. 50 Abs. 3, lit. a)**: Streichen. Die dem Bst. a) zugrundeliegende Bestimmung ist Art. 19 Bst. b) ist in der Praxis gar nicht umsetzbar. Daher ist auch die Strafbestimmung zu streichen. **Antrag zu Art. 50 Abs. 4**: Streichen. Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen.
Art. 51 Verletzung der Sorgfaltspflichten [1] Mit Busse bis zu 500'000 Franken werden private Personen auf **Antrag** bestraft, die vorsätzlich: a. unter Verstoss gegen Artikel 5 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln; b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 7 Absätze 1 und 2 erfüllt sind; c. es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder Verlust zu schützen (Art. 11); d. es unterlassen, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16); e. es unterlassen, die Vorkehren nach Artikel 18 zu treffen; f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert.	**Antrag zu Art. 51 Abs. 1**: Bei Vorsatz sind Bussen bis CHF 10'000.- angemessen. **Antrag zu Art. 51 Abs. 1 lit. a)**: Die Meldepflicht von Art. 6 Abs. 2 ist von der Busse auszunehmen, da ansonsten tausende von KMU unwissentlich kriminalisiert werden. **Antrag zu Art. 51 Abs. 1 lit. d)**: Streichen; erst die Folgeabschätzung kann ja zeigen, ob eine Folgeabschätzung notwendig wäre. Die Strafdrohung führt dazu, dass dieses Verfahren für jede Datenbearbeitung durchgeführt werden muss. In der Rechtsfolgeabschätzung werden Kosten von CHF 5‘000 – 30‘000.- pro Durchführung veranschlagt, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU führen würde. **Antrag zu Art. 51 Abs. 1 lit. e)**: Streichen; Hier handelt es sich um eine unbestimmte Handlungsdefinition, die dadurch kaum eine Strafbarkeit auslösen kann. **Antrag zu Art. 51 Abs. 1 lit. f)**: Streichen; die Strafdrohung führt dazu, dass alle Prozesse für die Datenbearbeitung vorsorglich dokumentiert werden müs-

VE-DSG	Anträge und Bemerkungen
[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	sen, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU, führen würde. In der RFA wurden diese Kosten nicht erhoben. **Antrag zu Art. 51 Abs. 2**: Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen.
Art. 52 Verletzung der beruflichen Schweigepflicht [1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf **Antrag** bestraft, wer vorsätzlich geheime Personendaten bekannt gibt: a. von denen er im Rahmen seiner beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat; b. welche er selbst zu kommerziellen Zwecken bearbeitet hat. [2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er bei der Tätigkeit für einen Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat. [3] Das Bekanntgeben geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.	**Antrag zu Art. 52**: Streichen; der bisherige Art. 35 DSG hat die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten geregelt. Die Ausweitung auf den unbestimmten Begriff „geheime Personendaten“ wird abgelehnt. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Damit würde jeder Bearbeiter von Personendaten einer strafbewehrten Schweigepflicht unterworfen. Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist völlig unverhältnismässig. *Eventualiter* wäre es sinnvoller, die Strafbarkeit in dieser Bestimmung auf Auftragsbearbeiter und Beauftragte zu beschränken.
Art. 53 Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.	**Antrag zu Art. 53**: Streichen; die bestehenden Regelungen im Verwaltungsstrafrecht und im Strafrecht sind ausreichend.
Art. 54 Anwendbares Recht und Verfahren Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.	**Antrag zu Art. 54**: Streichen; die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet werden und ist somit vom Bund zu führen.
Art. 55 Verfolgungsverjährung für Übertretungen Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.	**Antrag zu Art 55**: Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109) und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
9. Abschnitt: Abschluss von Staatsverträgen	
Art. 56 Der Bundesrat kann Staatsverträge abschliessen betreffend: a. die internationale Zusammenarbeit zwischen Datenschutzbehörden; b. die gegenseitige Anerkennung eines angemessenen Schutzes für die Bekanntgabe von Personendaten ins Ausland.	Titel fehlt zum Artikel fehlt.
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unterstehen den Artikeln 1-22, 26, 27, 29 bis 32, 34 Absätze 1-3 und 36 dieses Gesetzes, soweit sie nicht kantonalen Datenschutzvorschriften unterstehen, die einen angemessenen Schutz der Daten gewährleisten. [2] Die Kantone bestimmen ein Organ, das die Einhaltung der Datenschutzvorschriften überwacht. Die Artikel 41-43, 48 und 49 gelten sinngemäss.	
Art. 58 Aufhebung und Änderung anderer Erlasse Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.	Keine Bemerkungen
Art. 59 Übergangsbestimmung Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die für Verantwortlichen sowie der Auftragsbearbeiter in der Lage sein: a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen; b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.	**Antrag zu Art. 59**: Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, die nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken ist.
Art. 60 Referendum und Inkrafttreten [1] Dieses Gesetz untersteht dem fakultativen Referendum. [2] Der Bundesrat bestimmt das Inkrafttreten.	Keine Bemerkungen

Sammlung Änderungsvorschläge: Aufhebung und Änderung anderer Erlasse

VE-DSG	Anträge und Bemerkungen
11. Zivilprozessordnung *Art. 20 Bst. d* Für die folgenden Klagen und Begehren ist das Gericht am Wohnsitz oder Sitz einer der Parteien zuständig: d. Klagen und Begehren nach dem Datenschutzgesetz vom … *Art. 99 Abs. 3 Bst. d* [3] Keine Sicherheit ist zu leisten: d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom…. *Art. 113 Abs. 2 Bst. g* [2] Keine Gerichtskosten werden gesprochen in Streitigkeiten:	**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Da in Datenschutzfragen der Beauftragte eine Aufsichtsfunktion ausübt, kann er bei Verstössen aktiv werden. Es braucht hier keine weitere soziale Gerichtsbarkeit. Für zivilrechtliche Verfahren genügen die bestehenden Regeln. Das kostenlose Prozessieren könnte hier eine Flut – auch von mutwilligen – Klagen auslösen. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll – wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist – seine Kostenrisiken abwägen müssen, ehe Gerichte bemüht werden.

VE-DSG	Anträge und Bemerkungen
g. nach dem Datenschutzgesetz vom ……	
Art. 114 Bst. f Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom …….	
Art. 243 Abs. 2 Bst. d [2] Es gilt ohne Rücksicht auf den Streitwert für Streitigkeiten: d. zur Durchsetzung der Ansprüche nach den Artikeln 12 und 20 des Datenschutzgesetzes vom …	

VE-DSG	Anträge und Bemerkungen
13. Strafgesetzbuch *Art. 179novies* Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. *Art. 179decies* Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.	**Antrag zu Art. 179novies**: Die Strafbarkeit der Beschaffung ist zu beschränken auf Daten die einem Berufsgeheimnis unterliegen sowie auf besonders schützenswerte Personendaten. Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe zu bestrafen ist unverhältnismässig. Hier reicht eine Geldstrafe.
37. Fernmeldegesetz vom 30. April 1997 *Art. 13a Abs. 1 erster Satz* 1 Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, bearbeiten, sofern dies für die Erfüllung der ihnen durch die Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. ... *Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz* 1 … Zu diesen Daten gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten. 2 Unter Vorbehalt anders lautender internationaler Vereinbarungen dürfen die Kommission und das Bundesamt ausländischen Aufsichtsbehörden im Fernmeldebereich Daten, einschliesslich in Verwaltungs- oder Verwaltungsstrafverfahren beschaffter besonders schützenswerter Personendaten, nur übermitteln, sofern diese Behörden: 4 Schweizerische Behörden geben der Kommission und dem Bundesamt kostenlos diejenigen Daten weiter, die für die Durchsetzung der Fernmeldegesetzgebung von Bedeutung sein können, einschliesslich besonders schützenswerter Personendaten. ...	**Bemerkung zu datenschutzrechtlichen Regulierungen im Fernmeldegesetz**: Es ist klarzustellen, dass datenschutzrechtliche Regulierungen im Fernmeldegesetz und in dessen Ausführungsbestimmungen als *lex specialis* den allgemeinen Datenschutzbestimmungen des DSG und dessen Ausführungsbestimmungen vorgehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

SUISSEDIGITAL – Verband für Kommunikationsnetze

Dr. Simon Osterwalder
Geschäftsführer / Rechtsanwalt

Stefan Flück
Leiter Rechtsdienst / Fürsprecher LL.M.

Amstutz Jonas BJ

Von: Marc Epelbaum (Suva) <marc.epelbaum@suva.ch>
Gesendet: Dienstag, 4. April 2017 17:33
An: Amstutz Jonas BJ
Betreff: Vernehmlassung Datenschutzgesetz
Anlagen: 20170404_Vernehmlassungsantwort Suva.doc

Wichtigkeit: Hoch

Sehr geehrter Herr Amstutz

Wir bedanken uns für die Gelegenheit, am Vernehmlassungsverfahren zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz teilnehmen zu dürfen. Wunschgemäss senden wir Ihnen beiliegend auf elektronischem Weg unsere Stellungnahme als Word-Datei. Für die wohlwollende Prüfung und Berücksichtigung unserer Anliegen sind wir Ihnen sehr dankbar.

Zusammenfassend möchten wir festhalten, dass die Suva im Grundsatz die Stossrichtung des aufgelegten Gesetzesentwurfes zur Totalrevision des Datenschutzgesetzes, insbesondere den technologieneutralen Charakter sowie die Erleichterung beim grenzüberschreitenden Datenverkehr durch die Abschaffung des Schutzbereichs für juristische Personen begrüsst. Als positiv bewertet wird auch die teilweise Übernahme der Terminologie der Datenschutzgrundverordnung (DSGVO), um die Vereinbarkeit mit dem europäischen Recht zu verbessern.

Allerdings ortet die Suva in der bundesrätlichen Vorlage auch erhebliches Nachbesserungspotential. So wird – wie nachfolgend aufgezeigt – in etlichen Bestimmungen über die Anforderungen der DSGVO hinausgegangen, wofür kein Anlass besteht. Insbesondere erachtet die Suva die Regelungen betreffend das Profiling als nicht praktikabel. Ausserdem ist es für die Suva unerlässlich, dass sie für die Analyse und Weiterentwicklung der Unfallversicherung auch die Möglichkeit für den Einsatz von automatisierten Einzelentscheidungen zu erhalten hat, um damit die vorhandenen Daten einsetzen und auswerten zu können. Ein weiterer Kritikpunkt betrifft die neuen und stark erweiterten Informations- und Auskunftspflichten. Hier sollten Regelungen, welche für Unternehmen einen hohen administrativen Aufwand mit sich bringen, den Datenschutz für die betroffene Person faktisch jedoch nicht verbessern, gestrichen werden.

Ein dritter Kritikpunkt betrifft die massiv verschärfen Strafbestimmungen. Hintergrund für die vorgesehene Stärkung des strafrechtlichen Teils des Gesetzes ist die Befürchtung, dass ein zu mildes Strafsystem zur Folge haben könnte, dass die Europäische Union die schweizerische Regelung nicht mehr als angemessen erachten könnte (vgl. Erläuterungen VE DSG, S. 83). Allerdings verlangt die hier einschlägige Datenschutzkonvention 108 nicht zwingend eine Bussgeld-Ahndung (als Verwaltungs- oder Strafsanktion), zumal Art. 43 VE DSG bereits verschiedene andere Verwaltungsmassnahmen vorsieht, welche zumindest gemäss schweizerischer Verwaltungsrechtsdogmatik ebenfalls als verwaltungsrechtliche Sanktion qualifiziert werden können. Vor diesem Hintergrund ist deshalb zumindest die fahrlässige Begehung von einer Pönalisierung auszunehmen. Viele der Pflichten des VE DSG und damit auch die daraus abgeleiteten Straftatbestände sind zudem zu offen formuliert und widersprechen somit dem strafrechtlichen Prinzip „nulla poena sine lege certa“; auch sie sind aus dem Strafkatalog zu streichen.

Da zahlreiche Bestimmungen in der noch zu erlassenden Verordnung zum revidierten Datenschutzgesetz das Gesetz konkretisieren oder sich in der Verordnung überhaupt erst Regelungen finden werden (z.B. zum betrieblichen Datenschutzverantwortlichen), regt die Suva an, interessierte Kreise ebenfalls zu einer Vernehmlassung zur Verordnung zum revidierten Bundesgesetz über den Datenschutz einzuladen.

Gerne stehen wir für weitere Gespräche zu offenen Punkten zur Verfügung.

Freundliche Grüsse

Marc Epelbaum | Generalsekretär
Suva | Fluhmattstrasse 1 | 6002 Luzern
041 419 55 00

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schweizerische Unfallversicherungsanstalt Suva

Abkürzung der Firma / Organisation : Suva

Adresse : Fluhmattstrasse 1

Kontaktperson : Marc Epelbaum

Telefon : 041 419 55 00

E-Mail : marc.epelbaum@suva.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Suva	**Management Summary** Die Suva begrüsst im Grundsatz die Stossrichtung des aufgelegten Gesetzesentwurfes zur Totalrevision des Datenschutzgesetzes, insbesondere den technologieneutralen Charakter sowie die Erleichterung beim grenzüberschreitenden Datenverkehr durch die Abschaffung des Schutzbereichs für juristische Personen. Als positiv bewertet wird auch die teilweise Übernahme der Terminologie der Datenschutzgrundverordnung (DSGVO), um die Vereinbarkeit mit dem europäischen Recht zu verbessern. Allerdings ortet die Suva in der bundesrätlichen Vorlage auch erhebliches Nachbesserungspotential. So wird – wie nachfolgend aufgezeigt – in etlichen Bestimmungen über die Anforderungen der DSGVO hinausgegangen, wofür kein Anlass besteht. Insbesondere erachtet die Suva die Regelungen betreffend das Profiling als nicht praktikabel. Ausserdem ist es für die Suva unerlässlich, dass sie für die Analyse und Weiterentwicklung der Unfallversicherung auch die Möglichkeit für den Einsatz von automatisierten Einzelentscheidungen zu erhalten hat, um damit die vorhandenen Daten auch entsprechend einsetzen und auswerten zu können. Ein weiterer Kritikpunkt betrifft die neuen und stark erweiterten Informations- und Auskunftspflichten. Hier sollten Regelungen, welche für Unternehmen einen hohen administrativen Aufwand mit sich bringen, den Datenschutz für die betroffene Person faktisch jedoch nicht verbessern, gestrichen werden. Ein dritter Kritikpunkt betrifft die massiv verschärfen Strafbestimmungen. Hintergrund für die vorgesehene Stärkung des strafrechtlichen Teils des Gesetzes ist die Befürchtung, dass ein zu mildes Strafsystem zur Folge haben könnte, dass die Europäische Union die schweizerische Regelung nicht mehr als angemessen erachten könnte (vgl. Erläuterungen VE DSG, S. 83). Allerdings verlangt die hier einschlägige Datenschutzkonvention 108 nicht zwingend eine Bussgeld-Ahndung (als Verwaltungs- oder Strafsanktion), zumal Art. 43 VE DSG bereits verschiedene andere Verwaltungsmassnahmen vorsieht, welche zumindest gemäss schweizerischer Verwaltungsrechtsdogmatik ebenfalls als verwaltungsrechtliche Sanktion qualifiziert werden können. Vor diesem Hintergrund ist deshalb zumindest die fahrlässige Begehung von einer Pönalisierung auszunehmen. Viele der Pflichten des VE DSG und damit auch die daraus abgeleiteten Straftatbestände sind zudem zu offen formuliert und widersprechen somit dem strafrechtlichen Prinzip „nulla poena sine lege certa“; auch sie sind aus dem Strafkatalog zu streichen. Da zahlreiche Bestimmungen in der noch zu erlassenden Verordnung zum revidierten Datenschutzgesetz das Gesetz konkretisieren oder sich in der Verordnung überhaupt erst Regelungen finden werden (z.B. zum betrieblichen Datenschutzverantwortlichen), regt die Suva an, interessierte Kreise ebenfalls zu einer Vernehmlassung zur Verordnung zum revidierten Bundesgesetz über den Datenschutz einzuladen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Suva	VE DSG	3		c	**Antrag:** **„**4**.** biometrische Daten, **die bezwecken**, eine natürliche Person eindeutig zu identifizieren**“** **Begründung:** Die vorgesehene Regelung geht über die Konvention 108 hinaus. Als besonders schützenswert sollen biometrische Daten nur dann gelten, wenn mit ihnen gerade bezweckt wird, eine natürliche Person eindeutig zu identifizieren. Ohne diesen Zweck sind biometrische Daten nicht als besonders schützenswerte Daten zu klassifizieren.
Suva	VE DSG	3		f	**Antrag:** „f. *Profiling*: jede **automatisierte** Auswertung von ~~Daten oder~~ **Personendaten**…“ **Begründung:** Wie in Ziff. 8.1.1.2 des erläuternden Berichts zum Vorentwurf, S. 44, festgehalten, soll mit der Begriffsumstellung der Tatsache Rechnung getragen werden, dass es durch die technische Entwicklung (Big Data) vermehrt möglich wird, Daten ohne persönlichen Bezug so auszuwerten, dass anschliessend Personendaten vorliegen. Da im Rahmen von Big Data künftig wohl nur mit automatisierten Verfahren sinnvoll Profiling betrieben werden kann und insbesondere das automatisierte Auswerten einen besonderen Schutz der betroffenen Person erfordert, sollte sich der Begriff „Profiling“ nur auf die automatisierte Auswertung von Personendaten beziehen. Die DSGVO (Art. 4 Ziff. 4) versteht im Übrigen unter dem Begriff „Profiling“ ebenfalls nur die automatisierte Auswertung von personenbezogenen Daten, womit auch der Einbezug von anderen Daten in die Definition des Profiling abzulehnen ist.
Suva	VE DSG	3		h	**Antrag:**

					Neu wird nicht mehr vom „Inhaber der Datensammlung“ sondern vom „Verantwortlichen“ gesprochen. Das in Europa herrschende Begriffsverständnis vom „Verantwortlichen“ unterliegt einer finalen Betrachtungsweise; demgemäss ist nicht nur der, welcher über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet, ein Verantwortlicher, sondern bereits derjenige, der darüber entscheiden kann, auch wenn er es in der Folge nicht selbst tut, sondern den Entscheid einem Auftragsbearbeiter überlässt (vgl. auch ROSENTHAL, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter vom 20.02.2017, Rz. 10). Dieser Umstand kann zu Abgrenzungsschwierigkeiten führen, wenn z.B. der Outsourcer keinen Einfluss auf die konkreten Mittel hat, mit denen der Auftragsnehmer die Daten bearbeitet. Hier sollte **im Rahmen der Vernehmlassung eine Klärung** herbeigeführt werden.
Suva	VE DSG	4	3	Satz 1	**Antrag:** „Personendaten dürfen nur zu einem bestimmten und für die betroffene Person ~~klar~~ erkennbaren Zweck beschafft werden;“ **Begründung:** Das Wort „klar“ ist zu streichen, zumal die Formulierung bereits unter geltendem Recht nicht verwendet wird und es gemäss den Erläuterungen VE DSG, S. 46 keine materielle Änderung gegenüber dem heutigen Recht angestrebt wird.
Suva	VE DSG	4	3	Satz 2	**Antrag:** „…; sie dürfen nur so **weiter**bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.“ **Begründung:** Art. 4 Abs. 4 sieht zur terminologischen Annäherung an Art. 5 Abs. 1 Best. b DSGVO im 2. Satz vor, dass Daten nicht in einer Weise **weiter** bearbeitet werden dürfen, die mit dem anfänglichen Zweck nicht zu vereinbaren ist. Zur Klarstellung sollte dafür auch der Begriff „weiter bearbeitet“ verwendet werden.
Suva	VE DSG	4	4		**Antrag:**

					„….als der Zweck der Bearbeitung es bedingt, **ausser es bestehen gesetzliche oder regulatorische Aufbewahrungspflichten.“** **Begründung:** Die Ergänzung dient der Klarstellung, dass trotz Zweckerreichung aufgrund des Gesetzes oder anderen regulatorischen Vorgaben eine Pflicht zur Aufbewahrung der Daten in nicht anonymisierter Form bestehen kann.
Suva	VE DSG	4	5		**Antrag:** **„**Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind ~~und wenn nötig nachgeführt wurden.~~ Unrichtige und unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert werden oder ergänzt werden. Andernfalls sind die Daten zu vernichten. **Der Verantwortliche informiert Empfängerinnen und Empfänger von Personendaten über eine Berichtigung, Löschung oder Vernichtung von Daten, sofern eine betroffene Person eine solche Nachmeldung verlangt und sie ein schützenswertes Interesse daran hat.“** **Begründung:** Der Teilsatz („und wenn nötig nachgeführt werden“) ist zu streichen, denn Satz 2 stellt bereits sicher, dass unrichtige oder unvollständige Personendaten korrigiert oder ergänzt werden müssen. Wie bei Art. 19 lit. b ausgeführt ist die im VE-DSG dort vorgesehene, umfassende Informationspflicht an Dritte nach erfolgter Berichtigung, Löschung und Vernichtung von Daten Dritte zu streichen; stattdessen ist bei Art. 4 Abs. 5 eine reduzierte Informationspflicht im Falle, dass eine betroffene Person eine Information an einen Dritten verlangt, vorzusehen, wobei der Antragssteller über ein schützenswertes Interesse verfügen soll.
Suva	VE DSG	4	6		**Antrag 1:** „Ist für die Bearbeitung die Einwilligung der betroffenen Personen erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig ~~und eindeutig~~ erfolgt“. **Begründung:**

					Die Ergänzung, dass eine gültige Einwilligung eindeutig zu erfolgen hat, schafft keine Klarheit. Der erläuternde Bericht erklärt nicht, was genau damit gemeint ist. Die Erläuterungen weisen lediglich darauf hin, dass die terminologische Annäherung an den Entwurf der Konvention 108 und die DSGVO mit dieser Neuformulierung ermöglicht wird. Die Frage der Eindeutigkeit einer Willenserklärung ist bereits durch das geltende Recht geregelt und somit sollte in der Botschaft geklärt werden, dass der Schweizer Begriff der Einwilligung alle Voraussetzungen des Entwurfs der Konvention 108 erfüllt. **Antrag 2:** „…Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich sein." **Begründung:** Da in Art. 23 Abs. 2 lit. d beantragt wird, dass für das Profiling keine ausdrückliche Einwilligung vorausgesetzt wird, ist auch eine entsprechende Anpassung im Wortlaut von Art. 4 Abs. 6 VE DSG vorzunehmen**.** **Antrag 3:** Abs. 6 statuiert die Ausdrücklichkeit der Einwilligung für bestimmte Personendaten. Die Ausführungen in den Erläuterungen VE DSG, S. 47 sind – zumindest in Bezug auf den deutschen Text, welcher bezüglich der Ausdrücklichkeit nach wie vor gleich lautet wie heute – nicht klar. Inwiefern dadurch der in der Lehre ausgetragenen Kontroverse ein Ende gesetzt wird, ist nicht ersichtlich. In der noch zu erlassenden Botschaft sind dazu Klarstellungen nötig.
Suva	VE DSG	5	1		**Antrag:** Da der Bundesrat gemäss Art. 5 Abs. 2 VE DSG neu in einer verbindlichen Liste festlegt, welche Staaten einen angemessenen Datenschutz gewährleisten, führt der in Absatz 1 festgehaltene Grundsatz zu Unklarheiten (gilt Abs. 1 unabhängig von Abs. 2?) und sollte **gestrichen** werden.
Suva	VE DSG	5	3		**Antrag:** **„**Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten **nur dann** ins Ausland

					bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch:“ **Begründung:** Infolge der angeregten Streichung von Art. 6 Abs. 1 ist in Art. 6 Abs. 3 eine redaktionelle Präzisierung vorzunehmen.
Suva	VE DSG	5	5		**Antrag:** „Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiters spätestens ~~sechs Monate~~ **dreissig Tage** nach Erhalte der vollständigen Unterlagen mit, ob… “ **Begründung:** Die vorgesehene, 6-monatige Frist, innert welcher der EDÖB dem Verantwortlichen oder dem Datenbearbeiter mitteilt, ob er die standardisierten Garantien nach Abs. 3 lit. c Ziff. 1 oder Binding Corporate Rules (BCR) nach Abs. 3 lit. d Ziff. 1 genehmigt oder nicht, ist aus unternehmerischer Sicht zu lange und nicht praktikabel. Nach geltendem Recht musste die Prüfung selbst von BCR innert 30 Tagen durchgeführt sein. Die Frist von 6 Monaten ist deshalb auf 30 Tage zu kürzen.
Suva	VE DSG	5	6		**Antrag:** Absatz 6 sollte ersatzlos **gestrichen** werden. **Begründung:** Die in Abs. 6 enthaltenen Pflichten gehen über die DSGVO hinaus und sind deshalb zu streichen. Diese Informationspflichten stellen einen hohen administrativen Aufwand für Unternehmen dar; zudem war der Beitrag einer solchen Informationspflicht für den Datenschutz bereits unter geltendem Recht unklar und bei einer Verwendung von „Model-Clauses“ resultiert kein weiterer Nutzen bei einer Information des EBÖB (bspw. Zusätzlicher Schutz des Betroffenen).
Suva	VE DSG	6	1	a	**Antrag:** „…die betroffene Person ~~im Einzelfall~~ eingewilligt hat;“

					Begründung: Der Ausdruck „im Einzelfall“ hat in der Praxis zu Unklarheiten in der Anwendung geführt. Da die Einwilligung i.d.R. für einen bestimmten Bearbeitungszweck, und nicht für eine einzelne Übermittlung eingeholt wird, sollte auf das Erfordernis der Einwilligung im Einzelfall verzichtet werden.
Suva	VE DSG	6	1	b	**Antrag:** „…die Bearbeitung im ~~unmittelbarem~~ Zusammenhang mit dem Abschluss oder der Abwicklung eines im Interesse der betroffenen Person geschlossenen Vertrages steht…“ **Begründung:** Mit der vorgesehenen Regelung geht der VE DSG unnötigerweise über Art. 49 Abs. 1 lit. c DSGVO hinaus. Stattdessen sollte die die Formulierung von Art. 49 Abs. 1 lit. c DSGVO übernommen werden, mit welcher auch in „Dreiparteienverhältnissen“ eine Datenbekanntgabe gestützt auf Art. 6 Abs. 1 lit. b VE DSG sichergestellt werden kann.
Suva	VE DSG	6	1	c	**Antrag:** „Die Bekanntgabe im Einzelfall unerlässlich ist für: […] die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen ~~vor einem Gericht oder einer Verwaltungsbehörde~~“ **Begründung:** Die Begriffe „Gericht“ sowie „Verwaltungsbehörde“ sollten gestrichen werden, um schwierige Abgrenzungsfragen auszuschliessen. Massgebend ist, dass die Bearbeitungen zur „Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen“ vorliegen. Ausländische Behörden können anders organisiert sein sowie verschiedene Bezeichnungen tragen und sich u.U. nicht in eine der zwei Kategorien zuordnen lassen.
Suva	VE DSG	6	1	d	**Antrag:** „…die Bekanntgabe ~~im Einzelfall~~ notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Personen oder eines Dritten zu schützen…“

					Begründung: Siehe Ausführungen zu Art. 6 Abs. 1 lit. a VE-DSG.
Suva	VE DSG	6	2		**Antrag:** Absatz 2 sollte ersatzlos **gestrichen** werden. **Begründung:** Die in Abs. 2 enthaltenen Pflichten gehen über die DSGVO hinaus und sind deshalb ersatzlos zu streichen. Diese Informationspflichten, insbesondere bei einem Datenexport durch Vertragsabschluss oder –erfüllung oder bei einem Datenexport infolge Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen stellen einen hohen administrativen Aufwand für Unternehmen dar; zudem erscheint fraglich, ob der EDÖB überhaupt in der Lage sein wird, diese zahlreichen Meldungen (innert nützlicher Frist) zu verarbeiten. Im Übrigen sind Unternehmen durch diese Informationspflicht faktisch auch zur Offenlegung von Geschäftsgeheimnissen gegenüber dem EDÖB gezwungen.
Suva	VE DSG	7	2		**Antrag:** „Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit ~~und die Rechte der betroffenen Person~~ zu gewährleisten." **Begründung:** Neu hat sich der Verantwortliche nicht nur hinsichtlich der Datensicherheit sondern auch darüber zu vergewissern, dass Auftragsbearbeiter in der Lage ist, die Rechte der betroffenen Person zu gewährleisten. Es ist nicht klar, welche Pflichten damit dem Auftragsbearbeiter überbunden werden sollen und ausserdem kann der Auftraggeber nicht sämtliche Rechte der Betroffenen gewährleisten. Diese Anforderung ist zu streichen
Suva	VE DSG	7	3		**Antrag:** „Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger ~~schriftlicher~~ Zustimmung des

					Verantwortlichen einem anderen Auftragsbearbeiter übertragen." **Begründung:** Das Wort „schriftlich" ist zu streichen, da mit dieser Formulierung elektronische Prozesse nicht abgedeckt werden können (vgl. Art. 13 ff. OR).
Suva	VE DSG	8	1		**Antrag:** Absatz 1 sollte ersatzlos **gestrichen** werden. **Begründung:** Die in Abs. 1 dem EDÖB zugestandene Kompetenz, selbst Empfehlungen der guten Praxis zu erlassen, erscheint aus rechtsstaatlicher Sicht fragwürdig. Da gemäss Art. 9 Abs. 1 VE DSG die Einhaltung dieser Empfehlungen der guten Praxis die Einhaltung der Datenschutzvorschriften fingiert, könnte der EDÖB über seine eigenen Empfehlungen der guten Praxis strengere Anforderungen an ein datenschutzkonformes Verhalten einführen, als es das Gesetz verlangt und somit das Gesetz übersteuern. Auch rechtsstaatlicher Sicht kritisch zu beurteilen ist auch die Tatsache, dass der Erlass einer Empfehlung der guten Praxis durch den EDÖB offensichtlich nicht überprüft werden kann.
Suva	VE DSG	8	2		**Antrag:** **„Interessierte Kreise können Empfehlungen der guten Praxis ausarbeiten.** Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie." **Begründung:** Die interessierten Kreise (statt der EDÖB) werden für den Erlass von Empfehlungen der guten Praxis als zuständig erklärt; diese werden dem EDÖB anschliessend zur Genehmigung vorgelegt. Die „Empfehlungen der guten Praxis" sollten also analog zu den Regelungen in der EU als Mittel der Selbstregulierung von den interessierten Kreisen ausgehen und allenfalls durch den EDÖB genehmigt

					werden.
Suva	VE DSG	9	1-2		**Antrag:** Artikel 9 sollte **gestrichen** werden. **Begründung:** Die genauen Rechtswirkungen der Empfehlungen sind nach Art. 9 VE DSG unklar. Gemäss erläuterndem Bericht ist die Einhaltung der Empfehlungen freiwillig. Wer die Empfehlungen befolgt, hält diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren. Somit ist davon auszugehen, dass wer nachweisen kann, dass er sich an die Empfehlung hält, hier eine gesetzliche Vermutung besteht, dass der Verantwortliche sich gesetzeskonform verhalten hat. Dies sollte ausdrücklich so (unter Art. 8 VE DSG) festgehalten und geregelt werden.
Suva	VE DSG	12			**Antrag:** Artikel 12 sollte ersatzlos **gestrichen** werden. **Begründung:** Die bisherige (auf Verordnungsstufe) vorgesehene Regelung sollte beibehalten werden. Die Praktikabilität von Art. 12 VE DSG wird in Frage gestellt. So ist bei Abs. 1 lit. a z.B. unklar, wie der Verantwortliche feststellen können soll, ob die verstorbene Person die Einsicht zu Lebzeiten ausdrücklich untersagt hat. Ebenso ist unklar, wie post mortem ein überwiegendes Interesse einer verstorbenen Person, welches einer Datenherausgabe entgegenstehen könne, festzustellen wäre (Abs. 1 lit. b). Weiter wird diese Regelung zu grossen Aufwänden und Rechtsunsicherheit führen. Dies insbesondere auch, da Absatz 3 der Bestimmung besagt, dass Amts- und Berufsgeheimnisse nicht geltend gemacht werden können (Art. 33 ATSG). Durch diese Regelung sind auch Streitfälle mit Erben, die gegen oder unabhängig von der Erbengemeinschaft vorgehen, vorprogrammiert.

Suva	VE DSG	13	2		**Antrag:** **Präzisierung** in Absatz 2 „Er teilt der betroffenen Person spätestens bei der Beschaffung ~~diejenigen~~ **nachfolgende** Informationen mit, ~~die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere:…~~“ **Begründung:** Abs. 2 statuiert, dass der betroffenen Person diejenigen Informationen mitzuteilen sind, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Zwar sind in den nachfolgenden lit. a bis c einige konkrete Angaben aufgeführt. Gemäss den Erläuterungen VE DSG, S. 57 handelt es sich dabei jedoch um Mindestangaben, welche der betroffenen Person in jedem Fall mitgeteilt werden müssen. Auch aufgrund der Erläuterungen wird nicht klar, wie weit die Informationspflicht geht, was insofern problematisch ist, dass eine Verletzung der Informationspflicht strafrechtliche Sanktionen nach sich zieht, insbesondere auch bei fahrlässiger Begehung. Vor diesem Hintergrund und zwecks Rechtssicherheit sind die Angaben, über die informiert werden muss, klar und abschliessend im Gesetz zu nennen.
Suva	VE DSG	13	4		**Antrag:** Ersatzlose **Streichung von** Absatz 4 **Begründung:** Absatz 4 geht über Art. 13 und 14 der DSGVO hinaus und ist ersatzlos zu streichen. Eine Informationspflicht zur Identität und den Kontaktdaten sämtlicher Auftragsbearbeiter führt zu einem immensen Mehraufwand und schützt die Persönlichkeit der Betroffenen nicht. Eine Offenlegung der Identität und Kontaktdaten der Auftragsbearbeiter gegenüber den Kunden ist schliesslich auch wegen Geschäftsgeheimnissen kritisch. Es gibt diesbezüglich auch keine Vorgabe im revidierten Übereinkommen Nr. 108 des Europarates (siehe Art. 7bis E-SEV 108).

Suva	VE DSG	14	3+4		**Antrag:** Klarstellung der Begriffe. **Begründung:** Es ist unklar, was genau mit dem Begriff der „Übermittlung" gemeint ist und wie sich die „Übermittlung der Informationen" nach Abs. 3 von der „Übermittlung von Informationen" nach Abs. 4 unterscheidet.
Suva	VE DSG	14	4	a	**Antrag:** **„a.** wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern ~~und er die Personendaten nicht Dritten bekannt gibt~~;" **Begründung:** Auch wenn gemäss bisheriger Regelung in Art. 9 Abs. 4 DSG eine Einschränkung des Auskunftsrechts unter Berufung auf überwiegende private Interessen nur dann möglich war, wenn die Personendaten nicht Dritten bekannt gegeben wurden, sollte der letzte Teilsatz gestrichen werden, da die revidierte Konvention 108 diese Anforderung nicht voraussetzt.
Suva	VE DSG	15	1-3		**Antrag:** **Präzisierung** der Begriffe **Begründung:** Eine Informations- und Anhörungspflicht wird statuiert, wenn eine automatisierte Einzelentscheidung **rechtliche Wirkungen** oder **erhebliche Auswirkungen** auf die betreffende Person hat. In ihrer Tragweite sind dies Begriffe zu unbestimmt, was auch hinsichtlich der vorgesehenen Sanktionierung problematisch ist (nulla poena sine lege certa). Gemäss den Erläuterungen zum VE DSG (S. 59) beinhaltet der Begriff *rechtliche Wirkung*" alles, was die Rechtsstellung der betroffenen Person unmittelbar beeinflusst. Diese Umschreibung ist ausserordentlich weit gefasst und sollte auf Verordnungsstufe näher umschrieben werden. Dasselbe gilt für den noch unbestimmteren Begriff der *erheblichen* Auswirkungen auf die betroffene Person, worunter gemäss den

					Erläuterungen VE DSG (S. 59) tatsächliche Konsequenzen einer automatisierten Einzelentscheidung fallen, wobei diese einen gewissen Schweregrad erreichen müssen. Wann dies der Fall ist, ist unklar. Unklar ist auch, ob bei jeder einzelnen automatisierten Einzelentscheidung eine Anhörungs- und Informationspflicht besteht, oder ob bei gleichgearteten, mehrfach nacheinander folgenden Einzelentscheidungen die betroffene Person nur einmal anzuhören und zu informieren ist. Im Gegensatz zu Art. 22 Abs. 2 DSGVO lässt Art. 15 VE DSG (abgesehen von Abs. 3) keine Ausnahme von der Informations- und Anhörungspflicht vor. Die eben genannten Punkte könnten als Ausnahmetatbestände in der Verordnung konkretisiert werden. Damit Bundesorgane, insbesondere Sozialversicherungen wie Unfall-, Militär- und Krankenversicherungen, auch künftig im Massengeschäft eine automatisierte Rechnungsprüfung und Leistungsabwicklung vornehmen können, ist es zwingend, dass für sie in den Spezialgesetzen (UVG, MVG, KVG) die entsprechenden formell-gesetzlichen Grundlagen i.S. von Art. 27 Abs. 2 VE DSG geschaffen werden, um gestützt auf Art. 15 Abs. 3 von den Informations- und Anhörungspflichten befreit zu sein.
Suva	VE DSG	15	2		**Antrag:** „Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung ~~und zu den bearbeiteten Personendaten~~ zu äussern." **Begründung:** Die vorgesehene Regelung geht über Art. 22 DSGVO hinaus. Sie räumt der betroffenen Person kein Recht ein, sich auch zu den bearbeiteten Personendaten zu äussern. Dieser Satzteil ist deshalb zu streichen.
Suva	VE DSG	16	1		**Antrag:** „Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem ~~erhöhten~~ **hohen** Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen." **Begründung:** Art. 16 VE DSG geht über Art. 35 Abs. 1 DSGVO hinaus, welche eine Datenschutz-Folgenabschätzung nur

					bei einem hohen Risiko verlangt. Eine Datenschutz-Folgenabschätzung i.S. von Art. 16 sollte deshalb auch im revidierten DSG nur bei einem hohen Risiko nötig sein. In den Erläuterungen VE DSG, S. 61 werden als Indizien für das Vorliegen eines erhöhten Risikos zudem u.a. die Bearbeitung von besonders schützenswerten Personendaten genannt. Für die Suva hätte dies zur Konsequenz, dass für fast alle Datenbearbeitungen vorab eine formelle, dem EDÖB zu meldende Datenschutz-Folgenabschätzung durchgeführt werden müsste, was zu einem grossen innerbetrieblichen Aufwand führen würde. Aus Gründen der Rechtssicherheit begrüssenswert ist, wenn die Fälle, in welchen eine Datenschutz-Folgenabschätzung nötig ist, auf Verordnungsstufe bezeichnet werden, wie dies z.B. im Kanton Zürich in § 24 der Verordnung über die Information und den Datenschutz (IDV) umgesetzt wurde. Zu Streichen ist auch eine Pflicht des Auftragsbearbeiters zur Erstellung einer Datenschutz-Folgenabschätzung, zumal eine solche Pflicht nach der DSGVO ebenfalls nicht besteht und schwerlich vorstellbar ist, wie ein Auftragsbearbeiter dazu in der Lage sein soll.
Suva	VE DSG	16	3		**Antrag:** Keine Meldepflicht an den EDÖB für Unternehmen, die einen betrieblichen Datenschutzbeauftragten bezeichnet haben. **Begründung:** Art. 36 Abs. 1 DSGVO sieht eine Konsultation der Aufsichtsbehörde nicht in jedem Fall vor, sondern nur dann, wenn der Verantwortliche zum Schluss kommt, dass trotz der von ihm ergriffenen Schutzmassnahmen eine hohes Risiko der Verletzung der Persönlichkeit der betroffenen Person weiterhin besteht. Zumindest dies sollte auch im neuen DSG umgesetzt werden. Bei Unternehmen, welche über einen betrieblichen Datenschutzverantwortlichen verfügen, wäre begrüssenswert, wenn eine Meldepflicht generell nur an diesen, und nicht den EDÖB statuiert würde, vergleichbar mit der heutigen Lösung bei den Datensammlungen (Art. 11a Abs. 5 lit. e). Der betriebliche Datenschutzverantwortliche könnte die Datenschutz-Folgenabschätzung bei sich sammeln und dem EDÖB bei Bedarf Einsicht gewähren.
Suva	VE DSG	16	4		**Antrag:**

					„Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter ~~innerhalb von drei Monaten~~ **spätestens acht Wochen** nach Erhalt aller erforderlichen Informationen mit.“ **Begründung:** Die vom VE DSG vorgesehene Reaktionszeit des EDÖB von 3 Monaten ist aus unternehmerischer Sicht zu lange und blockiert geplante Datenbearbeitungen. Art. 36 Abs. 2 DSGVO sieht einen Zeitraum von bis zu acht Wochen nach Erhalt des Ersuchens vor; diese Lösung wäre als Mindeststandard zu übernehmen.
Suva	VE DSG	17	1		**Antrag:** „Der Verantwortliche meldet dem Beauftragten ~~unverzüglich~~ **ohne unnötigen Verzug** einen Verstoss gegen Sicherheitsmassnahmen ~~unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht~~, **der** zu einem **hohen** Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person **führt**.“ **Begründung**: Die vorgesehene Regelung geht über die Bestimmungen der DSGVO hinaus. Art. 33 Abs. 1 DSGVO schreibt dem Verantwortlichen eine unverzügliche Benachrichtigung der zuständigen Aufsichtsbehörde bei Datenpannen („Verletzungen des Schutzes personenbezogener Daten“) vor. Der Begriff der „Verletzung des Schutzes personenbezogener Daten“ wird in Art. 4 Nr. 12 DSGVO definiert als eine Verletzung der Sicherheit. Im Gegensatz dazu umfasst die in Art. 17 VE DSG vorgesehene Regelung jegliche unbefugte Datenbearbeitung, zumal keine unbefugte Datenbearbeitung vorstellbar ist, die nicht auch ein Risiko für die Persönlichkeit der betroffenen Person darstellt. Eine solch umfassende Meldepflicht geht zu weit. Die Meldepflicht ist deshalb in Angleichung an das europäische Recht auf die Verletzung von Sicherheitsmassnahmen zu beschränken. Zudem ist eine Meldung an den Beauftragten nur dann vorzusehen, wenn der Verstoss gegen Sicherheitsmassnahmen zu einem hohen Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt.
Suva	VE DSG	18	1+2		**Antrag:**

					Artikel 18 sollte **gestrichen** werden. **Begründung:** Die in Art. 18 VE DSG enthaltenen Massnahmen zur Sicherstellung des Datenschutzes (Abs. 1: privacy by design / Abs. 2: privacy by default) gehören thematisch zu Art. 11 (Datensicherheit). Art. 11 VE DSG entspricht dem geltenden Art. 7 DSG, welcher bereits heute angemessene technische und organisatorische Massnahmen fordert und mithin auch die Grundsätze von privacy by design und privacy by default bereits umfasst. Es erübrigt sich deshalb, in einem separaten Artikel spezielle Regelungen zum Datenschutz durch Technik und zu datenschutzfreundlichen Voreinstellungen aufzunehmen. Art. 18 VE DSG ist deshalb zu streichen und ist (allenfalls) in Art. 11 VE-DSG zu integriere, wobei nicht über die Anforderungen der DSGVO hinauszugehen ist.
Suva	VE DSG	19	1	a	**Antrag:** Die Dokumentationspflicht sollte nicht über die in Art. 30 DSGVO enthaltenen Pflichten hinausgehen. **Begründung:** Weitergehende Dokumentationspflichten führen zu keinem Mehrwert für den Datenschutz, sondern nur zu einem unverhältnismässigen Aufwand.
Suva	VE DSG	19	1	b	**Antrag:** Ersatzlose **Streichung** von lit. b **Begründung:** Gemäss lit. b müssen der Verantwortliche und der Auftragsbearbeiter im Falle einer Berichtigung, Löschung und Vernichtung von Daten Dritte, denen sie zuvor die entsprechenden Daten zugänglich gemacht haben, über die erfolgte Berichtigung, Löschung und Vernichtung der Daten informieren. Eine solch umfassende Pflicht löst eine Flut von Informationen aus, ohne dass aus datenschutzrechtlicher Sicht ein Mehrwert resultieren würde. Deshalb wird angeregt, eine solche Information an Dritte nur dann zu statuieren, wenn eine betroffene Person die Nachinformation tatsächlich verlangt und sie über ein entsprechendes schützenswertes Interesse verfügt. Dies kann durch eine Ergänzung von Art. 4 Abs. 5 VE

					DSG erreicht werden (vgl. die dortigen Ausführungen).
Suva	VE DSG	20	2	g	**Antrag:** **„**g. gegebenenfalls die Informationen **nach Artikel 13 Absatz 3“** **Begründung:** Art. 13 Abs. 4 VE DSG ist zu streichen (siehe Antrag und Begründung), weshalb Art. 20 Abs. 2 lit. g VE DESG anzupassen ist.
Suva	VE DSG	23	2	d	**Antrag:** **„**d**.** durch Profiling ohne ~~ausdrückliche Einwilligung~~ **Information** der betroffenen Person“ **Begründung:** Die Fiktion einer Persönlichkeitsverletzung ist aufgrund der sehr breiten Begriffsdefinition von Profiling (Art. 3 lit. f VE DSG) zu streichen. Stattdessen soll eine Persönlichkeitsverletzung nur fingiert werden, wenn die betroffene Person nicht über ein Profiling informiert wird.
Suva	VE DSG	24	2		**Antrag:** **„**Ein überwiegendes Interesse der bearbeitenden Person ist ~~möglicherweise~~ gegeben, wenn dieser insbesondere:…“ **Begründung:** Die bisherige Regelung in Art. 13 Abs. 2 DSG entspricht bewährter Rechtspraxis. Die damit gewonnene Rechtssicherheit sollte nicht mit der Aufnahme des Wortes „möglicherweise“ wieder gedämpft werden.
Suva	VE DSG	24	2	a	**Antrag:** „a. in ~~unmittelbarem~~ Zusammenhang mit dem Abschluss oder der Abwicklung eines im Interesse der betroffenen Person geschlossenen Vertrages Personendaten bearbeitet“ **Begründung:**

					Aus Kohärenzgründen ist es sinnvoll, den Wortlaut dieser Bestimmung an Art. 6 Abs. 1 lit. b VE DSG anzupassen.
Suva	VE DSG	27	2		**Antrag:** „Für die Bearbeitung besonders schützenswerter Personendaten, ~~das Profiling oder den Erlass einer automatisierten Einzelfallentscheidung nach Art. 15 Abs. 1~~ ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich“ **Begründung:** Beim Erlass einer automatisierten Einzelfallentscheidung wie auch beim Profiling ist das Vorhandensein einer Grundlage in einem Gesetz im formellen Sinn zu verzichten. Vielmehr haben sie immer dann als zulässig zu gelten, soweit sie vom Sinn und Zweck des Gesetzes als gedeckt betrachtet werden können. Das Fordern einer expliziten Grundlage in einem Gesetz im formellen Sinn für automatisierte Einzelfallentscheide/Profiling ist praxisfremd und gesetzgebungstechnisch kaum befriedigend umsetzbar. Vielmehr müssen alle automatisierten Einzelfallentscheidungen/Profiling automatisch als zulässig gelten, wenn sie der Durchführung/Abwicklung des Versicherungsverhältnisses dienen. Mithin darf einzig der datenschutzrechtliche Grundsatz der Zweckbindung die Zulässigkeit der Bearbeitungsarten bestimmen. **Beispiel:** Die Identifikation und Bearbeitung von Hoch- und Höchstkostenfällen bedingt, dass die Suva als Unfallversicherer ihren Datenbestand unter Anwendung eines einschlägigen Regelwerks bearbeiten darf. Die Zulässigkeit der Durchführung eines Case Managements dürfte ebenso unbestritten sein wie das Faktum, dass Case Management einen wichtigen Beitrag zur Reduktion der Unfallversicherungskosten leistet. Dennoch enthält das UVG bereits heute nicht eine einzige gesetzliche Bestimmung über Case Management. Die effiziente Abwicklung des Unfallversicherungsgeschäfts als Massengeschäft bedingt einen sehr hohen Automatisierungsgrad. Die Leistungsprüfung erfolgt damit zu einem sehr hohen Anteil vollautomatisch anhand vordefinierter Regelwerke. Das UVG enthält jedoch keine entsprechenden Grundlagen.
Suva	VE DSG	44	3		**Antrag:**

					„Beschwerden gegen vorsorgliche Massnahmen nach Art. 42 kommt ~~keine~~ aufschiebende Wirkung zu." **Begründung:** Eine vom EDÖB bspw. vorsorglich verfügte Einstellung oder Anpassung einer Datenbearbeitung kann innerhalb eines Unternehmens zu massivem Aufwand resp. Kosten führen. Deshalb muss Unternehmen die Möglichkeit gewährt werden, mittels einer Beschwerde mit aufschiebender Wirkung die Verfügung des EDÖB vorgängig auf deren Rechtmässigkeit zu überprüfen.
Suva	VE DSG	45			**Antrag:** „Art. 45 ~~Anzeigepflicht~~ **Anzeige von Verletzungen der Datenschutzbestimmungen** ~~Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit~~. **Der Beauftragte kann Verletzungen der Datenschutzbestimmungen den Strafverfolgungsbehörden mitteilen."** **Begründung:** Auf eine Anzeigepflicht des EDÖB bei Offizialdelikten ist zu verzichten; stattdessen ist gestützt auf das gemässigte Opportunitätsprinzip lediglich eine Anzeigebefugnis zu statuieren. Auch die europäischen Regelungen sehen keine Verpflichtung zur Meldung vor.
Suva	VE DSG	50 ff.			**Strafbestimmungen Art. 50-55 VE DSG** Als schärfstes Mittel des Staates zur Steuerung sollte das Strafrecht immer nur als letztes Mittel („ultima ratio") eingesetzt werden. Zuvor sind andere Steuerungsinstrumente wie z.B. das Verwaltungsverfahren auszuschöpfen. Der massiv erweiterte Katalog der Strafbestimmungen ist unverhältnismässig. Die Bestimmungen führen zu einer nicht sachgerechten Kriminalisierung der Mitarbeitenden und werden dazu führen, dass die gesetzlich gewollten Spielräume (vgl. erste Leitlinie der Revision: risikobasierter Ansatz, Ziff. 1.4.1, S. 18, erläuternder Bericht) bei der Datenbearbeitung aus Angst vor persönlicher Bestrafung nicht ausgeschöpft werden und sehr viel mehr Bürokratie betrieben wird als sinnvoll und vertretbar ist. Der Compliance Aufwand würde exponentiell zunehmen, insbesondere auch weil auch fahrlässiges Verhalten bestraft

					werden würde. Ausserdem richten sich die Strafbestimmungen nicht gegen eigentliche Datenschutzverletzungen, sondern viel eher steht die Einhaltung von flankierenden Massnahmen (Informations- und Meldepflichten) im Fokus. Wobei die Meldepflichten auch gegen den „nemo tenetur“ Grundsatz verstossen würden.
Suva	VE DSG	52			**Antrag:** Artikel 52 ist **zu streichen**. **Begründung:** Die Bestimmung ist viel zu offen und unbestimmt formuliert. Sie steht darüber hinaus im falschen Gesetz. Sie gehört ins StGB und nicht ins DSG. Für die Mitarbeitenden der Sozialversicherungen bringt sie grosse Rechtsunsicherheit mit sich. Gemäss erläuterndem Bericht zum Vorentwurf hat Art. 52 VE DSG zum Ziel, die Schweigepflicht auch auf Berufe auszudehnen, die nicht unter Art. 321 StGB fallen, „für deren Ausübung der Schutz der Vertraulichkeit aber ebenfalls unerlässlich ist“. Der Geheimnisschutz soll auf alle Arten von Personendaten ausgedehnt werden (vgl. S. 86, erläuternder Bericht). Im Bereich der Sozialversicherungen besteht mit Art. 33 ATSG ebenfalls eine Schweigepflicht. Es besteht damit die Gefahr, dass die viel zu offene Formulierung von Art. 52 VE DSG damit die Sozialversicherungen mitumfassen können.
Suva	VE DSG	59			**Antrag:** Aufnahme einer allgemeinen Übergangsfrist für die Umsetzung des revidierten DSG aufzunehmen, nicht nur Hinweise auf 16, 18 und 19 lit. a VE DSG. Es ist eine angemessene Übergangsfrist für Umsetzung des revidierten DSG von fünf Jahren vorzusehen. Keine Rückwirkung oder beschränkte Rückwirkung der neuen Bestimmungen. **Begründung:** Die Vernehmlassungsvorlage sieht keine umfassende Übergangsbestimmung vor. Die neuen und revidierten Bestimmungen des DSG stellen hohe Anforderungen und haben bedeutende Auswirkungen auf Geschäftsprozesse. Eine Übergangsbestimmung ist deshalb zwingend aufzunehmen.

Anhang (Art. 58)					
Suva	IPRG	139	3		**Antrag:** «[3] Absatz 1 ist auch anwendbar auf Ansprüche aus Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten sowie aus Beeinträchtigung des Rechts auf Auskunft über Personendaten. **Dabei kann ein ausländischer Erfolgsort im Sinne von Absatz 1 Buchstabe c nicht allein damit begründet werden, dass die Daten im betreffenden Land gespeichert sind.**» **Begründung:** Im Rahmen der DSG-Revision sollte auch Art. 139 Abs. 3 IPRG, der die Anwendbarkeit des DSG im internationalen Verhältnis regelt, angepasst werden. Wegen dem weit gehenden Recht des Geschädigten, das anwendbare Recht gemäss Art. 139 Abs. 1 IPRG zu wählen, sind Schweizer Verantwortliche andernfalls auch in Konstellationen potentiell der Datenschutz-Grundverordnung der EU (EU-DSGVO) unterworfen, in denen sich die EU-DSGVO trotz ihren extraterritorialen Bestimmungen (Art. 3) für nicht anwendbar erklärt. Ohne Änderungen würde das IPRG damit zu einer weitergehenden extra-territorialen Anwendbarkeit der EU-DSGVO auf ausländische Verantwortliche führen als dies gemäss den weitgehenden betreffenden Bestimmungen der EU-DSGVO selbst der Fall ist. Gleiches gilt für andere ausländische Datenschutzgesetze.
Suva	43. UVG	96			**Antrag:** Streichen von Art. 96 VE UVG Einleitungssatz. Ändern von Art. 96 Abs. 1 UVG, wie folgt: „[1] Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter ~~Daten~~ Personendaten ~~und Persönlichkeitsprofile~~, zu bearbeiten oder bearbeiten zu lassen, **das Profiling im Sinne von Artikel 3 Buchstabe f DSG durchzuführen und automatisierte Einzelentscheidungen im Sinne von Art. 15 Absatz 1 DSG zu erlassen, soweit dies notwendig ist**, ~~die sie benötigen,~~ um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:“

					„[2 (neu)] **Die mit der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Personendaten im Sinne von Artikel 3 Buchstaben a und b DSG zu bearbeiten oder bearbeiten zu lassen und das Profiling im Sinne von Artikel 3 Buchstabe f DSG durchzuführen, um mit Einwilligung der Versicherten Case-Management-Massnahmen zu ergreifen. Die Einwilligung der Versicherten hat in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu erfolgen**." **Begründung:** Es gilt, die als Folge der Revision des DSG notwendigen gesetzlichen Grundlagen im UVG zu verankern. **Absatz 1:** Gemäss VE DSG soll der Passus „und Persönlichkeitsprofile" in Art. 96 UVG gestrichen werden. Dem erläuterndem Bericht zum VE DSG vom 21. Dezember 2016 kann zwar entnommen werden, dass der Begriff „Persönlichkeitsprofil" im revidierten DSG durch den Begriff „Profiling" ersetzt werden soll (siehe Ziffer 8.1.1.3 erläuternder Bericht; Art. 3 Bst. F VE DSG). Es kann ihm jedoch keine Begründung dafür entnommen werden, weshalb der Begriff im UVG nicht ebenfalls ersetzt, sondern vielmehr ersatzlos gestrichen werden soll. Die ersatzlose Streichung bedeutet eine unnötige, massive Einschränkung im Rahmen der Durchführung des UVG. Denn der Begriff „Profiling" definiert auch die Auswertung von nicht-personenbezogenen Daten, um wesentliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Es ist nicht nachvollziehbar, weshalb dies inskünftig nicht mehr möglich sein soll. Im Interesse der Rechtssicherheit sollte auch im UVG von besonders schützenswerten Personendaten die Rede sein, damit die Begriffe im DSG und im UVG einheitlich verwendet werden. Ferner gilt es im Hinblick auf Art. 27 Abs. 2 VE-DSG im UVG eine Grundlage für den Erlass von automatisierten Einzel-entscheidungen zu schaffen. Eine Informations- und Anhörungspflicht bei automatisierten Einzelentscheidungen würde zu einem enormen administrativen Mehraufwand mit entsprechenden Kosten führen – und dies ohne den Versicherten einen erkennbaren Nutzen zu bringen. **Neuer Absatz 2:** Die neue Bestimmung ist notwendig, da Bundesorgane und damit auch UVG-Versicherer gemäss Art. 27 Abs. 3 VE-DSG nur noch im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten dürfen – und auch dies nur unter bestimmten Voraussetzungen. Von «ausnahmsweise» und «im Einzelfall» kann aber bei Case-Management-Massnahmen wohl kaum die Rede sein. Es besteht somit die Gefahr, dass die stetig an Bedeutung gewinnenden Case-Management-Massnahmen als Folge der Revision des DSG nicht mehr zulässig sind, weil sie nicht zu den Aufgaben

					gehören, die das UVG von Gesetzes wegen den Versicherern überträgt, sondern um freiwillige Wiedereingliederungsbemühungen des UVG-Versicherers. Mit der vorgeschlagenen Ergänzung wird ausdrücklich präzisiert, dass solche Massnahmen die Einwilligung der Versicherten in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht, erfordern.
Suva	43. UVG	97	6	b	**Antrag:** «b. Personendaten, sofern die betroffene Person im Einzelfall ~~schriftlich~~ **in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht**, eingewilligt hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse des Versicherten vorausgesetzt werden darf.» **Begründung:** Das Parlament hat im Rückweisungsbeschluss betreffend die VVG-Revision verlangt, dass bei der Erarbeitung einer neuen Vorlage dem elektronischen Geschäftsverkehr Rechnung getragen wird. Dies im Hinblick auf die Tatsache, dass die Digitalisierung im gesamten Versicherungswesen Einzug gehalten hat. Es gilt daher, nicht nur im VVG, sondern auch im UVG die Bestimmungen technologieneutral zu formulieren und Begriffe, die den elektronischen Geschäftsverkehr behindern, konsequent zu eliminieren. Der VE-DSG als solcher behindert den elektronischen Geschäftsverkehr zwar grundsätzlich nicht, da das Erfordernis der Schriftlichkeit nur in einer einzigen Bestimmung betreffend die Auftragsdatenbearbeitung vorgesehen ist. Die Änderung von Art. 97 Abs. 6 Bst. b UVG ist jedoch notwendig, da das UVG als Spezialgesetz dem DSG vorgeht.
Suva	44. MVG	94a			**Antrag:** Streichen von Art. 94a VE MVG Einleitungssatz. Ändern von Art. 94a MVG, wie folgt „[1] Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter ~~Daten~~ Personendaten ~~und Persönlichkeitsprofile~~, zu bearbeiten oder bearbeiten zu lassen, **das Profiling im Sinne von Artikel 3 Buchstabe f DSG durchzuführen und automatisierte Einzelentscheidungen im Sinne von Art. 15 Absatz 1 DSG zu erlassen, soweit dies notwendig ist**, ~~die sie benötigen,~~ um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:“

					„[2 (neu)] Die mit der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Personendaten im Sinne von Artikel 3 Buchstaben a und b DSG zu bearbeiten oder bearbeiten zu lassen und das Profiling im Sinne von Artikel 3 Buchstabe f DSG durchzuführen, um mit Einwilligung der Versicherten Case-Management-Massnahmen zu ergreifen. Die Einwilligung der Versicherten hat in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu erfolgen." **<u>Begründung:</u>** Siehe Begründung zu 43. UVG Art. 96

Creditreform
Wirtschaftsauskünfte Inkasso Marketing

Schweiz. Verband Creditreform
(Genossenschaft)
Präsident
Teufener Strasse 36
9000 St. Gallen
Tel. 071 221 11 01
Fax 071 221 11 85
e-mail info@creditreform.ch

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per eMail gesandt an:
jonas.amstutz@bj.admin.ch

St. Gallen, 04. April 2017

Vernehmlassung zum Vorentwurf Datenschutzgesetz und Änderung weiterer Erlasse und zur Revision der SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Sehr geehrter Herr Amstutz

Wir machen hiermit gerne von der Möglichkeit zur Einreichung einer Vernehmlassung zu den genannten Revisionsvorlagen Gebrauch.

Als Anhang zu dem vorliegenden Mail erhalten Sie die in die vorgegebene Tabelle eingearbeitete Vernehmlassung zu folgenden Revisionsentwürfen:

- Vorentwurf Bundesgesetz über den Datenschutz (Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutzgesetz)
- Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten

Ergänzend erlauben wir uns, Ihnen den im Jusletter vom 20. Februar 2017 erschienenen Aufsatz von David Rosenthal "Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet" zugehen zu lassen. Dieser zeigt sehr eindrücklich auf, wo die Gesetzgebung über die Anforderungen des EU-Rechts sowie des Europarates hinausgehen will ("Swiss Finish"). Was uns fehlt, ist eine fundierte Auseinandersetzung mit den Interessen der Wirtschaft; im Bestreben, Personendaten - koste es, was es wolle - vor den Unternehmen zu schützen, scheint die Tatsache völlig untergegangen zu sein, dass wirtschaftsfreundliche Rahmenbedingungen die Basis für den weiteren, ökonomischen Erfolg der Schweiz bilden.

Des Weiteren erachten wir die Vernehmlassungsunterlagen als irreführend. Gemäss dem Gesetzgebungsleitfaden des Bundesamts für Justiz dient die Erarbeitung eines "Vorentwurfs" als Grundlage für die Abschätzung der Auswirkungen eines künftigen Gesetzes. Im Anschluss daran wird ein Vernehmlassungsentwurf ausgearbeitet, welcher dann in die eigentliche Vernehmlassung geht. Gemäss den uns gegenüber gemachten Aussagen soll dieses Prozedere hier nicht eingehalten werden, bzw. soll der Oeffentlichkeit nach erfolgter, verwaltungsinterner Auseinandersetzung mit den jetzt eingereichten Vernehmlassungen keine Gelegenheit mehr geboten werden, sich zu äussern. Hier besteht dringender Klärungsbedarf!

Der Schweizerische Verband Creditreform ist 1888 als Selbsthilfeorganisation der kreditgebenden Wirtschaft gegründet worden. Mit rund 12'000 Mitgliedern und Kunden, 7 regionalen Kreisbüros und insgesamt rund 200 Mitarbeitenden bildet er die grösste schweizerische Gläubigervereinigung für Kreditschutz.

Creditreform
Wirtschaftsauskünfte Inkasso Marketing

Zu seinen Tätigkeiten gehören u.a. die Erteilung von Bonitätsauskünften und das Forderungsmanagement (Inkasso). Diese Dienstleistungen haben eine Verminderung des Risikos von Forderungsausfällen bei Lieferanten und Kreditgebern zum Ziel. Sie tragen zur Erhaltung der Zahlungsfähigkeit von Firmen, Selbständigerwerbenden und Privatpersonen bei.

Wir danken Ihnen für Ihre Aufmerksamkeit, und verbleiben

mit freundlichen Grüssen

Schweiz. Verband Creditreform
(Genossenschaft)

Raoul Egeli
Präsident

Claude Federer
Sekretär

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Schweizerischer Verband Creditreform

Abkürzung der Firma / Organisation : SVC

Adresse : Teufener Strasse 36, 9000 St. Gallen

Kontaktperson : Raoul Egeli, Präsident

Telefon : 071 221 11 02

E-Mail : raoul.egeli@creditreform.ch

Datum : 04. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Allgemeine Bemerkungen	
Name/Firma	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.	Der Vorentwurf zum DSG zeugt insgesamt von einem ausgeprägten patronalstaatlichen Uebereifer und ungenügender Reflexion. Er hebelt ohne Not diverse, ansonsten unbestrittene Rechtsgrundsätze aus (Vertragsfreiheit, Schutz von Geschäftsgeheimnissen, Abweichung vom Grundsatz, dass niemand sich selbst belasten muss, etc.). Die Vorlage wird von Seiten des SVC insgesamt als legislatorischer Overkill zurückgewiesen. Ein erheblicher Eingriff in die Vertragsfreiheit liegt v.a. in den völlig überschiessenden Begründungs-, Anhörungs- und Informationspflichten; zivilrechtlich muss der Nichtabschluss eines Vertrages grundsätzlich nicht begründet werden, nach DSG soll dies aber plötzlich erforderlich sein, wenn die Ablehnung auf einer automatisierten Datenbearbeitung basiert. Die stipulierte Pflicht zur Selbstanzeige widerspricht ebenfalls ansonsten unbestrittenen Rechtsgrundsätzen, schliesslich wurde dem Schutz von Geschäftsgeheimnissen offensichtlich nicht die notwendige Aufmerksamkeit geschenkt. In welchen Punkten eine Anpassung an die DSGVO 2016/679 und/oder an die Konvention 108 wirklich erforderlich ist, und wie weit diese im Einzelfall gehen muss, bleibt im Dunklen. Der Erläuterungsbericht verweist meist einfach generell auf das Europarecht, was als Begründung aber offensichtlich nicht ausreicht. Teilweise werden in ausländischen Erlassen enthaltene Einschränkungen der Datenbearbeitung sogar noch ausgeweitet (die sattsam bekannte Neigung zum "Swiss Finish" ist auch hier festzustellen). Der tatsächliche Anpassungsbedarf wird auch in der Regulierungsfolgenabschätzung der PWC nicht beleuchtet. Zur Uebungsanlage gehörte offenbar nicht, das Revisionsvorhaben kritisch zu diskutieren. Das Papier der PWC stellt vielmehr tel quel auf die Vorgaben der Politik ab. Entsprechend wohlwollend ist denn auch die Abschätzung der Folgen ausgefallen, die wir nicht teilen können. Die administrative Belastung für die KMU (Datenschutzverantwortlicher, Folgeabschätzungen, Informationspflichten unklaren Umfangs, Begründungspflichten für Entscheide, etc. etc.) wird offensichtlich unterschätzt. Selbst dort, wo die Botschaft im Interesse der Wirtschaft auf die Praktikabilität eingeht, spiegelt sich dies im Wortlaut der Vorlage häufig nicht (so etwa bei den Informationspflichten). Offenbar sind einige neue Regelungen wegen der Schengen-Richtlinie in den VE DSG aufgenommen worden, die jetzt auch auf Private ausgedehnt werden sollen (z.B. die weitgehenden Befugnisse des Beauftragten zum Erlass von Verfügungen). Dies wäre ggf. im Rahmen des Schengen-Acquis bzw. im öffentlich-rechtlichen Teil des DSG zu regeln. Ein ungelöstes Problem liegt in der fehlenden Regelung für eine Daten*sperre*. Eine Löschung reicht nicht unbedingt, um einen Eintrag dauernd aus einer Datenbank zu entfernen. Um zu gewährleisten, dass eine Person zu einem späteren Zeitpunkt nicht wieder in den Datenbestand gelangt, müssen deren Identifikationsmerkmale (idealerweise mit einem eindeutigen Personenidentifikator) gespeichert werden können. Der SVC hat stets die Auffassung vertreten, dass der Datenschutz für den öffentlichen und den Privatbereich in zwei separaten Gesetzen geregelt

	werden sollte. Die Vermischung von öffentlich- und privatrechtlichen Regelungen im gleichen Erlass führt zu einer Auflösung der - sinnvollen - Unterscheidung zwischen Privatrechtsverkehr einerseits, Regelungen zum Verhältnis zwischen Staat und rechtsunterworfenem Bürger anderseits. Ausserdem könnte dann auch die Umsetzung des Schengen-Acquis da erfolgen, wo sie hingehört, nämlich im öffentlichen Recht.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	1			**Antrag:** Nicht nur die juristischen Personen, sondern auch die im HR eingetragenen Einzelunternehmen und Mitglieder von Personengesellschaften sind vom Schutz auszunehmen, den das DSG für von einer Datenbearbeitung betroffene Personen vorsieht. Die Abgrenzung der geschützten von den nicht geschützten Personenkategorien ist in dieser Form nicht sachgerecht. Im HR eingetragene Einzelfirmen oder Mitglieder von Personengesellschaften wären datenschutzrechtlich vielmehr gleich zu behandeln wie juristische Personen. Die strafrechtlichen Bestimmungen über den Schutz der Ehre und das Verbot des wirtschaftlichen Nachrichtendienstes sowie der Persönlichkeitsschutz gemäss Art. 28ff. ZGB (die für diese Kategorien auch weiterhin gelten würden), wären aus unserer Sicht ausreichend. Art. 1 veranschaulicht die unerwünschten Auswirkungen der Ausgestaltung des DSG als Doppelerlass (Vermischung von öffentlichem und privatem Sektor) im übrigen sehr schön. In der jetzigen Fassung kann er so interpretiert werden, dass hier quasi durch die Hintertür eine direkte Drittwirkung von Grundrechten im Privatrechtsbereich eingeführt werden soll.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	2	2	c)	**Antrag:** Beibehaltung des geltenden Wortlauts. Der VE will nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung also nicht mehr gelten. Dies öffnet Missbräuchen Tür und Tor (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	3	1	c) 4.	**Antrag:** Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Bilder in Zeitungen wären damit ausgenommen (nach dem Wortlaut des VE würden sie unter den Begriff der "biometrischen Daten" fallen).
Fehler! Ver-	VEDSG	3	1	c) 5	**Bemerkung:** Die Bestimmung ist in dieser allgemeinen Form problematisch. etwa wenn Vermögensdelikte

weisquelle konnte nicht gefunden werden.					zur Diskussion stehen, von denen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	3	1	f)	**Antrag:** Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes "Daten". Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um "Personendaten". Die reflexartige Uebernahme von Begriffen des ausländischen Rechts beinhaltet die Gefahr, dass auch die Anwendung sich primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und weder notwendig noch sachgerecht. Dies umso weniger, als der Begriff des "Profiling" gegenüber dem EU-Recht sogar ausgeweitet worden ist; die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Kautelen und Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Was damit gewonnen wäre, ist unerfindlich. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich höchst kontraproduktiv, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als "Voraussage" eines späteren Verhaltens interpretiert werden können. Die Revision schiesst hier weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen. ohne all die Kautelen einzuhalten, die der VE mit dem "Profiling" verknüpft; selbst die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind, würde plötzlich problematisch, etc. Der Begriff des "Profiling" ist zu unbestimmt und gefährdet damit die Rechtssicherheit. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem "Persönlichkeitsprofil" des geltenden Rechts absolut abzulehnen.

Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	3	1	h), i)	**Antrag:** Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), eventualiter zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu unklaren - teilweise unsinnigen - Aufteilungen der Verantwortung und Doppelspurigkeiten. Offenbar wird zudem übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen kann. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für den "Verantwortlichen"?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den "Verantwortlichen?") geradezustehen und muss Betroffene über Aenderungen oder Löschungen (durch den "Verantwortlichen"?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht- Unklar ist auch, ob Arbeitnehmer unter den Begriff des "Auftragsbearbeiters" fallen können, was dem Wortlaut und der Systematik entspräche, aber offensichtlich zu einer völlig ausufernden Verantwortlichkeit führen würde.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	4	3		**Antrag:** Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft nur neue Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Die Botschaft argumentiert, es sei keine Aenderung beabsichtigt. Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. Die Einführung kompatibler Bearbeitungszwecke ist zu begrüssen.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	4	4		**Antrag:** Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.
Fehler! Verweisquelle konnte nicht gefunden	VEDSG	4	5		**Antrag:** Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Seite 47 des Erläuterungsberichts sind hier keine materiellen Aenderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten, sonst wird nur neue Unsicherheit geschaffen.

werden.					Eventualiter: Beschränkung von Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind", Streichung des Restes dieses Passus'. Bekanntlich fängt die "Bearbeitung" ja schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE). Eine fortdauernde Verpflichtung zur Nachführung wäre offensichtlich unerfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status' einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind!
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	4	6		**Antrag:** Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (s. auch die Bemerkungen zu Art. 3 lit. f VE)
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	5	3	d)	**Antrag:** Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	5	4 - 6		**Antrag:** Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt - wie aus dem Wort ersichtlich - nach den Weisungen des Verantwortlichen, dem - wiederum entsprechend seiner Bezeichnung - die Verantwortung für die Information des Beauftragten obliegt.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	6	2		**Antrag:** Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1, lit b, c und d ins Ausland bekanntgegeben wird; dies gilt erst recht, wenn - wie hier - neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Die Verantwortlichkeiten sind einmal mehr unklar geregelt. Die Bestimmung ist im übrigen auch insofern heikel, als solche Meldungen z.T. sensible Geschäftsinterna betreffen werden (etwa Gerichtsverfahren im Ausland), die dann kraft Oeffentlichkeitsgesetz auch für Dritte einsehbar werden. Dem Schutz von Geschäftsgeheimnissen ist im Rahmen des VE DSG generell nicht die

					nötige Aufmerksamkeit geschenkt worden.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	7	2		**Antrag:** Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Der Auftragsbearbeiter ist auch hier zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	7	3		**Antrag:** Schaffung der Möglichkeit einer generellen Einwilligung. In der DSGVO – auf welche diese Bestimmung offensichtlich Bezug nimmt – wird ausdrücklich klargestellt, dass auch eine generelle Einwilligung zur Begründung von Unteraufträgen möglich ist, die noch nicht auf einen bestimmten Unter-Auftragsbearbeiter Bezug nimmt. Zu denken ist etwa an eine entsprechende Klausel im Vertrag zwischen Verantwortlichem und Auftraggeber, in welchem die Zustimmung pauschal erteilt würde.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	8			**Antrag:** Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der "interessierten Kreise" - erfahrungsgemäss damit einseitig der politischen Linken - ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. U.a. ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen tel quel zugrunde legen werden. Der Beauftragte wird im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich Recht zu setzen. Dies wiegt umso schwerer, als der Beauftragte noch nicht einmal Jurist zu sein braucht.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	9			**Antrag:** Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zulasten des Datenbearbeiters führen.
Fehler! Verweisquelle konnte nicht gefunden	VEDSG	12	4		**Antrag:** Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Allfällige Aenderungen wären im ZGB vorzunehmen. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und

werden.					Löschungsrecht völlig ausreichen. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären, etc-. Art. 4 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	13			**Vorbemerkungen**: – Es fehlt an Uebergangsbestimmungen, die regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar. – die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention - und nicht die DSGVO - den Massstab für den "angemessenen" Datenschutz zu liefern haben.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	13	1 + 2		**Antrag:** Es ist - im Minimum - ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird festgehalten, es genüge eine "allgemeine Information" im beschriebenen Sinn (vgl. S. 55). Der Wortlaut von Art. 13 VE widerspricht dem allerdings. In der vorliegenden Form ist die Bestimmung dabei völlig unpraktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. In einem Wort: Ein kompletter Overkill (dies wurde sogar in der RFA der PWC richtig erkannt, wenn auch anscheinend nur von einer Minderheit; vgl. Ziff. 4.1.1.5 des genannten Dokuments). Dieser wäre umso gravierender, als dann je nach Tätigkeit des datenverarbeitenden Unternehmens jedermann auch noch sämtliche Empfänger und Empfängerinnen bekanntgegeben - und damit Geschäftsgeheimnisse of-

					fengelegt - werden müssten. Der Aufwand wäre schlicht jenseits von Gut und Böse. Es muss genügen, dass diese Informationen öffentlich zugänglich sind.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	13	3		**Antrag:** Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist unakzeptabel. "Kategorien" muss wie bis anhin genügen. Eine weitergehende Offenlegungspflicht wäre - wenn schon - auf solche Fälle zu beschränken, wo persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger auch noch der "unschuldigsten" Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen. Bemerkung: Die Weitergabe von Daten innerhalb eines Konzerns wird damit unnötig erschwert (Konzerngesellschaften gelten ja als Dritte)
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	13	4		**Antrag:** Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	13	5		**Antrag:** Ersatzlos streichen; eventualiter Beschränkung der aktiven Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten. Die vorliegend stipulierte, uferlose Informationspflicht ist impraktikabel und völlig unverhältnismässig. Sie geht auch weiter als die Con108 (vgl. etwa Art. 7bis Abs. 2). Die Bestimmung ist im übrigen strenger als die DSGVO, die immerhin noch einen Monat Frist gewährt (!). Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	14			Die Ausnahmen von der Informationspflicht sind unnötigerweise restriktiver geregelt als in der Con108.

Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	14	1		**Antrag:** Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung), in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	14	2		**Antrag:** 1. Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der Vorentwurf für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	14	4	a)	**Antrag:** Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Bemerkung: Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns unnötig erschwert.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	15	1		**Antrag:** Streichen, ev. um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a) DSGVO EU (2016/679) ergänzen. Art. 22 DSGVO EU nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor - eine Abweichung wäre demnach zweifellos auch für die Schweiz zulässig. Weiter wäre zumindest ausdrücklich vermerken, dass es sich um "erhebliche" und "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als überzogener und unreflektierter Versuch, Konsumenten vor jedweder Art von automatisierten Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche Auswirkung" ist, dürfte letztlich von der Sensibilität des Betroffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung frei und muss dies auch

					bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Die Formulierung der "Auswirkungen" ist so breit, dass jeder kommerzielle Entscheid - z.B. über eine Lieferung von Ware gegen Rechnung - darunter fallen kann. Auch die Lieferung von Ware gegen Rechnung ist in keiner Weise zwingend, und die Verweigerung darf nicht begründungspflichtig werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	15	2		**Antrag:** Streichen; wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand. Jedes Unternehmen, das über ein strukturiertes Kreditmanagementsystem verfügt, wird inskünftig mit jedem, den es nicht gegen Rechnung beliefern will, Korrespondenz führen müssen um ihm zu erklären, wie der Entscheid zustande gekommen ist. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens. Es scheint den Autoren des VE entgangen zu sein, dass in der Schweiz immer noch Vertragsfreiheit herrscht, und sich grundsätzlich niemand für seine Lieferkonditionen rechtfertigen muss. Der VE geht, wie erwähnt, in diesem Punkt sogar über die DSGVO hinaus.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	15	3		**Antrag:** Streichen. Diese Bestimmung entlastet einmal mehr einseitig den Staat.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	16			**Antrag:** Streichen. In den Wortlaut kann jeder hineindeuten, was er will. Im Ergebnis wird wohl jedes Unternehmen eine solche "Folgeabschätzung" vornehmen müssen, welches mehr tut, als die Daten seiner eigenen Kunden zu bearbeiten. Hier wird ein bürokratisches Monstrum in die Welt gesetzt, das in der Privatwirtschaft im Ergebnis nichts bringen wird (im öffentlichen Sektor mag es hingegen durchaus angebracht sein). Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier und Zeit dafür aufwenden müssen. Der Verweis auf die Grundrechte macht übrigens einmal mehr deutlich, dass ein Datenschutzgesetz, welches sowohl den privaten als auch den öffentlichen Sektor regeln will, zwangsläufig zu Regulierungen führt, die dem einen oder anderen Bereich unangemessen sind. Die übrigen datenschutzrechtlichen Verpflichtungen der Datenbearbeiter - wie z.B. die Zweckbindung oder die Verhältnismässigkeit - reichen zum Schutz der Betroffenen völlig aus. Eine - drakonisch strafbewehrte - Verpflichtung zur Erstellung und Unterbreitung einer solchen

					Folgeabschätzung beim Beauftragten ist als bürokratischer Leerlauf zurückzuweisen. Vor kurzem war der Tagespresse zu entnehmen, wie schwer der Bundesrat sich mit der Aufgabe der Regulierungsfolgeabschätzung tut. Dies sollte zur Vorsicht mahnen; im Gegensatz zu staatlichen Organen hätte ein Rechtsunterworfener immerhin gravierende Konsequenzen bis hin zu seiner wirtschaftlichen Vernichtung zu befürchten für den Fall, dass er die Aufgabe der "Folgenabschätzung" nicht zur Zufriedenheit der Amtsstellen oder Gerichte abwickelt, die sich mit ihm befassen wollen oder müssen.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	16	3, 4		**Antrag:** Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen, und das Vetorecht des Beauftragten sind in jedem Fall zu streichen. Die 3 Monatsfrist wäre im übrigen viel zu lang.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	17			**Antrag:** Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien. Wieso dieser im Bereich des Datenschutzes plötzlich nicht mehr gelten soll, ist völlig unerfindlich; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja verpflichtet wäre, allfällige strafbare Handlungen zur Anzeige zu bringen. Der Verantwortliche müsste sich m.a.W. nicht nur an das datenschutzrechtliche, sondern auch noch an das strafrechtliche Messer liefern. Im übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der nachgerade terroristischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer regelrechten Flut an Selbstanzeigen zu rechnen, die nur den Apparat des Beauftragten übermässig aufblähen würde.
Fehler! Verweisquelle konnte nicht gefunden	VEDSG	17	2		**Antrag:** In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen. Kompetenzzuweisungen, die nicht schon im heutigen Recht vorgesehen sind, sind generell zu streichen.

werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	17	4		**Bemerkung:** Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	18			**Antrag:** Ersatzlos streichen. Die Bestimmung ist redundant, der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	19			**Antrag:** Ersatzlos streichen. Die Bestimmung ist nicht nur überflüssig, sondern teilweise gar nicht umsetzbar. Die vom VE stipulierte Dokumentationspflicht würde für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b. ist sodann von vornherein nicht umsetzbar bzw. nachgerade absurd. Was gewonnen sein soll, wenn alle früheren Empfänger von Daten über jede spätere Aenderung, Löschung oder Vernichtung informiert werden, ist völlig unerfindlich. Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine - allfällige - Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gem. Art. 25 machen zu müssen (bei der obendrein nicht klar ist, was man sich darunter vorzustellen hätte). Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Zudem ist zu bedenken, dass die Umsetzung der Bestimmung häufig ihrerseits zu Datenschutzverletzungen führen würde. Beispiel: Bezüger von Wirtschaftsauskünften besitzen in der Regel kein schützenswertes Interesse daran, von nach der Abfrage erfolgten Änderungen einer Auskunft Kenntnis zu erhalten; dies gilt z.B. immer dann wo die vertraglichen Beziehungen zum Betroffenen fertig abgewickelt sind. Sie über

					spätere Berichtigungen zu informieren, würde zweifellos einen Verstoss gegen das DSG bedeuten.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	20	2	e)	**Antrag:** Streichen - in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich, z.B. im Online-Handel, etc. Vgl. auch den Antrag zu Art. 15 hievor.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	20	2	f)	**Antrag:** Streichen: Die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntzugeben, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	20	3		**Antrag:** Streichen, ev. Beschränkung auf die Pflicht, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt - ein Vertrag wird geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, Geschäftsgeheimnisse offenlegen zu müssen, die ansonsten ausdrücklich strafrechtlich geschützt sind. Wieso es erforderlich sein soll, dem Betroffenen die Auswirkungen zu erläutern, ist sodann völlig unerfindlich. In aller Regel wird er absolut in der Lage sein, diese selber einzuschätzen.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	23	2	d)	**Antrag:** Streichen. Zum Profiling vgl. auch die Bemerkungen zu Art. 3 lit f) VE.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	23	3		**Bemerkung:** Abs. 3 gaukelt eine scheinbare Sicherheit vor. Was über Facebook verbreitet worden ist, kann auch dann nicht wieder aus der Welt geschafft werden, wenn der Betroffene Facebook die (weitere) Verbreitung untersagt
Fehler! Verweisquelle	VEDSG	24	2		**Antrag:** Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit. Das neue DSG wimmelt nachgerade von

konnte nicht gefunden werden.					Vorschriften, die einseitig auf die Einschränkung der Datenbearbeitung und auf eine Kriminalisierung datenbearbeitender Unternehmen ausgerichtet sind.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	24	2	a)	**Antrag:** Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft einmal mehr nicht gelöste Abgrenzungsfragen auf.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	24	2	c) 3.	**Antrag:** Streichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar, die Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft. Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit 100 %-iger Sicherheit bestimmbar, geschweige denn sein Alter. Im übrigen würde es klar zum Schutz Minderjähriger beitragen, wenn zumindest ihr Alter gespeichert und die Information aufbewahrt werden dürfte!
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	25	1	a) bis c)	**Antrag:** Hier muss spezifiziert werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. ansonsten kann die Bestimmung nicht umgesetzt werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	25	2		**Antrag:** Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", ev. Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis krause Ergebnisse erwarten. Zudem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hätte.
Fehler! Verweisquelle konnte nicht gefunden	VEDSG	25	3		**Antrag:** Streichen. Abs. 1 lit. a. bis c. reichen völlig, um dem Betroffenen Genüge zu tun. Auch die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor

werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	28	1, 2		**Antrag:** Entweder streichen, oder die entsprechenden Möglichkeiten auch Privaten eröffnen. Hier kommt einmal mehr das einseitig etatistische Denken zum Ausdruck, das dem ganzen Erlass zugrunde liegt.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	37	1		**Antrag:** Dem Bundesrat soll nur ein Vorschlagsrecht zukommen, die Wahl muss durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Dauer von 4 Jahren gewählt". Ein blosses Recht des Parlaments, den Gewählten abzunicken, ist als Augenwischerei zurückzuweisen. Wir sind uns bewusst, dass der VE in diesem Punkt dem geltenden Recht entspricht, sind jedoch der Auffassung, dass eine politisch derart sensible Stelle zwingend vom Parlament zu besetzen ist.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	37	4		**Antrag:** Das Budget muss durch das Parlament genehmigt werden. Wird das Konzept des vorliegenden VE DSG auch nur annähernd übernommen, werden sich die Kosten der Administration gewaltig erhöhen. Ein Mitspracherecht des Parlamentes erscheint schon insoweit zwingend.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	38	2		**Antrag:** Die automatische Wiederwahl ist zu streichen. Ein solches Institut existiert bei keiner einzigen anderen, magistralen Position.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	39	2		**Antrag:** Jede Nebenbeschäftigung muss offengelegt werden. Hier ist absolute Transparenz unabdingbar.
Fehler! Verweisquelle	VEDSG	41	4		**Antrag:** Streichen. Ein Tätigwerden des Beauftragten gegenüber Privaten ohne konkrete Hinweise auf eine Datenschutzverletzung ist strikte abzulehnen. Die Kosten solcher amtlicher Initiativen werden in der

konnte nicht gefunden werden.					Praxis regelmässig den Privaten überbunden. Daher muss gelten: Keine "Ueberprüfung ohne konkreten Anlass!"
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	42			**Antrag:** Streichen. Vorsorgliche Massnahmen sind - auch im Persönlichkeitsschutz - Sache der Gerichte. Hier soll einer Einzelperson, die nicht einmal Jurist sein muss, ohne Not eine völlige "carte blanche" erteilt werden! Dies ist rechtsstaatlich unhaltbar.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	43	1		**Antrag:** Streichen. Der Beauftragte erhält hier Befugnisse zum Erlass hoheitlicher Verfügungen, die teilweise nicht wieder gutzumachende Folgen zeitigen (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Der Persönlichkeitsschutz von Art. 28ff. ZGB reicht zum Schutz Betroffener völlig aus.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	44	3		**Antrag:** Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Wenn schon, wäre vorzusehen, dass die aufschiebende Wirkung auf **Antrag** durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt unsinnige Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	45			**Antrag:** Streichen. Ein *Recht* zur Anzeige wäre bei Weitem sachgerechter. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE); besonders untragbar wären diese in dem Fall, dass die überzogenen Offenlegungs- und Informationspflichten gegenüber dem Beauftragten beibehalten werden sollten.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	49		b)	**Antrag:** Streichen. Es besteht die Gefahr, dass der Beauftragte zum verlängerten Arm ausländischer Behörden wird.
Fehler! Verweisquelle	VEDSG	50			**Antrag:** Die Straftatbestände sind ins Strafgesetzbuch zu verlagern und die entsprechenden Bestimmungen nochmals grundlegend zu überarbeiten. Der vorgesehene Strafrahmen ist völlig überrissen und nach-

konnte nicht gefunden werden.					gerade als terroristisch zu bezeichnen. Dies gilt sowohl für vorsätzliche als auch - erst recht - für fahrlässige Verstösse. Es wird beantragt, bei Fahrlässigkeit von einer strafrechtlichen Sanktionierung abzusehen, eventuell den Bussenrahmen auf eine maximale Höhe von CHF 5'000.00 bzw. - im Wiederholungsfall - CHF 10'000.00 zu begrenzen. Die Straftatbestände sind teilweise derart unbestimmt gefasst, dass sie auch hinsichtlich des Bestimmtheitsgebots nochmals umformuliert werden müssen. Ein gutes Beispiel bietet Abs. 3 lit. b) der vorliegenden Bestimmung der obendrein auch den Grundsatz „nemo tenetur“ bzw. das Verbot, sich selber belasten zu müssen, verletzt. Bei den Unternehmensbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen hergestellt werden, wie dies in der DSVGO EU ausdrücklich vorgesehen ist (Art. 83 Abs. 2 lit. geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen; die Umsatzrendite beträgt bei hiesigen KMU häufig weniger als 5 %). Die Strafbestimmungen stellen ein weiteres Beispiel dar, wie sehr der Politik das Augenmass abhandengekommen ist. Offenbar hat sich inzwischen der Glaube durchgesetzt, dass ein Gesetz nur dann von Gutem sein kann, wenn es Strafdrohungen im Phantasiebereich enthält und möglichst viele Akteure kriminalisiert. Theoretisch genügt EIN Betroffener, der sich falsch behandelt fühlt, um einen Datenbearbeiter als Kriminellen abzustempeln und wirtschaftlich in den Ruin zu treiben. Im "gewöhnlichen" Strafrecht beträgt die maximale Busse für eine Uebertretung CHF 10'000.00 (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Rahmen. Die Erhöhung des Strafrahmens auf CHF 500‘000.00 ist absolut überrissen. Beispielsweise sieht das kantonalbernische Verwaltungsrecht im Baurecht bei schweren (!) Verstössen Höchstbussen von CHF 100'000.00 vor (Art. 50 Abs. 3). Gemäss Art. 14ff. VStrR können bei Leistungs- und Abgabebetrug, Urkundenfälschung und Erschleichung einer Falschbeurkundung sowie Begünstigung Höchstbussen von CHF 30'000.00 festgelegt werden. Gemäss DBStG können bei Verstössen wie Mithilfe bei der Steuerhinterziehung Bussen von 10‘000.00 bis max. CHF 50‘000.00 (in schweren Fällen oder bei Wiederholungsfall) gesprochen werden. Bei Steuerbetrug beträgt die Busse max. 30‘000.00. Bei Verstössen gegen das DSG handelt es sich mi Ausnahme von Art. 52 VE - der eine Freiheitsstrafe als

					Höchststrafe vorsieht - nicht um Vergehen oder Verbrechen, sondern um Uebertretungen. Es existiert kein nachvollziehbarer Grund, für vergleichbare Verstösse übliche Bussenrahmen im DSG um das Zehnfache oder mehr zu überschreiten. Eine Persönlichkeitsverletzung, die dies rechtfertigen würde, ist nicht vorstellbar. Eine solche Pönalisierung von DSG-Verstössen kommt einer schweren Kriminalisierung der Fehlbaren gleich und ist komplett unverhältnismässig. U.a. übersteigt der im VE DSG gesteckte Rahmen auch die Schmerzensgelder bei weitem, die nach hiesiger Rechtsprechung bei Körperschäden zugesprochen werden. Als Vergleich noch einige Beispiele aus der deutschen Rechtsprechung für die Bemessung von Schmerzensgeld wegen Persönlichkeitsverletzung (Mobbing und ähnliches): - Mobbing durch nicht gerechtfertigte Aufgabenentziehung durch den Arbeitgeber, Schikanierung und Degradierung des Arbeitnehmers: 53.000 Euro (ArbG Leipzig, 2012) - vielfältige persönliche Herabsetzung des Arbeitnehmers, rund € 26.500, ArbG Ludwigshafen am Rhein, 2000 - Beleidigungen, Auftragsentziehung, Verbot des Kundenkontakts, Gehaltskürzung durch den Arbeitgeber, € 24.000 , LAG Hannover, 2005 - systematische Persönlichkeitsverletzungen des Arbeitnehmers in 34 Fällen über 1 Jahr, € 17.500, ArbG Eisenach, 2005 - schikanöse und entwürdigende Handlungen, € 7.000, ArbG Siegburg, 2012 - Demütigung wegen der ethnischen Herkunft durch ein Rap-Video bei YouTube, € 5.000, LG Bonn, 2013 - Cybermobbing via Facebook mit Unterstellung der Homosexualität und Pädophilie, € 1.500, LG Memmingen, 2015 Quelle: http://www.schmerzensgeldtabelle.net/mobbing/#tabelle http://www.schmerzensgeldtabelle.net/mobbing/#tabelle
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	51	2		**Antrag:** Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen. Vorsatzstrafen: S. Bemerkungen zu Art. 50
Fehler! Verweisquelle	VEDSG	52			**Antrag:** Streichen. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Unklar, wer hier neu zum Träger eines Berufsgeheimnisses gemacht werden soll, ebenso unklar,

konnte nicht gefunden werden.					was "geheime Personendaten" im vorliegenden Zusammenhang genau bedeuten würde. Wenn schon die blosse kommerzielle Bearbeitung von Daten als Aufhänger für die Strafdrohung genügen soll, würde wohl nahezu jeder Datenbearbeiter zum Träger einer strafbewehrten Schweigepflicht gemacht.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	55			**Antrag:** Reduktion der Verjährungsfrist auf 3 Jahre. Dies entspricht Art. 109 StGB und wäre völlig ausreichend und sachgerecht
	VEDSG	56			**Antrag:** Es fehlt der Titel zu diesem Artikel.
Fehler! Verweisquelle konnte nicht gefunden werden.	VEDSG	56			**Antrag:** Die Genehmigung des Parlamentes ist zwingend einzuholen.
Fehler! Verweisquelle konnte nicht gefunden werden.	ZPO	20, 99, 113, 114, 243			**Antrag zu den zivilprozessualen Bestimmungen in der ZPO {bezieht sich auf alle Artikel wie vorgeschlagen}**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Wo das Gesetz in Abweichung von den normalen Regeln von der Erhebung von Gerichtskosten absieht, geht es üblicherweise um Vertragsstreitigkeiten (Miete, Arbeitsvertrag, auch Gleichstellungsfragen pflegen sich jeweils im Zusammenhang mit einem Arbeitsverhältnis zu stellen). Wegleitend ist dabei die Annahme des Gesetzgebers, dass eine Partei besonders geschützt werden muss, weil sie in einem Abhängigkeitsverhältnis zur anderen steht. Im Datenschutzbereich werden oft keinerlei vertragliche oder persönliche Beziehungen zwischen Datenbearbeiter und Betroffenem bestehen. In dieser Konstellation ist nachgerade mit einer Flut von - durchaus auch mutwilligen - Klagen zu rechnen, wenn das Prozessieren gratis ist. Es besteht kein Anlass, die üblichen, zivilprozessualen Regeln hier zu ändern. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll - wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist - seine Kostenrisiken abwägen müssen. Der SVC spricht sich auch dagegen aus, alle Streitigkeiten ins vereinfachte Verfahren zu weisen. Dies ver-

					kürzt die beklagte Partei wesentlich in ihren Verfahrensrechten.
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	Der SVC kritisiert die Ausdehnung des Anwendungsbereichs der Konvention 108, die hier quasi durch die Hintertür vorgenommen wird. Bisher beschränkte sich die Konvention 108 auf die *automatisierte* Bearbeitung von Personendaten, während der Entwurf jede Art der Bearbeitung von Personendaten avisiert. Nachdem der VE DSG bereits stark auf das europäische Datenschutzrecht ausgerichtet ist, scheint der Abschluss eines zusätzlichen Uebereinkommens - das zwangsläufig zu Ueberschneidungen, Redundanzen und vermeidbaren Rechtsunsicherheiten führt - von vornherein überflüssig. Nachstehend erfolgt keine umfassende Stellungnahme zum Konventionsentwurf. Es wird lediglich auf einige Bestimmungen hingewiesen, bei denen der VE DSG weiter geht, als er dies aufgrund des Entwurfstextes tun müsste.
Fehler! Verweisquelle konnte nicht gefunden werden.	Bemerkungen zu den einzelnen Artikeln:
Fehler! Verweisquelle konnte nicht gefunden werden.	Art. 5 Abs. 4 lit. d): Die schrankenlose Nachführungspflicht, die der VE DSG einführen will, ist im Text des Konventionsentwurfs explizit relativiert ("wenn nötig").
Fehler! Verweisquelle konnte nicht gefunden werden.	Art. 8 Abs. 21 lit a) und Abs. 2: Der Entwurf würde explizit die Möglichkeit offenlassen, auf die impraktikablen Bestimmungen über die Informations- und Anhörungspflichten bei automatisierten Entscheidungen gemäss Art. 15 VE DSG zu verzichten. Insofern ist nicht einzusehen, wieso diese Bestimmung trotzdem in den VE aufgenommen werden musste. Der Schutz, den schon das geltende DSG für die von einer Datenbearbeitung Betroffenen vorsieht, würde auch für diese Fälle ausreichen.

Fehler! Verweisquelle konnte nicht gefunden werden.	Art. 9 lit. Abs. 1 lit. b): Die Rechte und Freiheiten Dritter werden ausdrücklich als mögliche Gründe für eine Abweichung von bestimmten Kautelen der Konvention aufgeführt. Der VE DSG widerspiegelt dies nicht; die auf der Hand liegende Erkenntnis, dass - nicht nur, aber insbesondere - die umfassenden Informations- und Auskunftspflichten des VE DSG zu einem übermässigen Eingriff in die Rechte Dritter führen können, scheint nicht bis zu den Redigierenden des VE DSG vorgedrungen zu sein.
Fehler! Verweisquelle konnte nicht gefunden werden.	Art. 12 Abs. 5 und 6: Es ist also nicht zwingend, den Beauftragten über vertragliche Garantien zu informieren, die im grenzüberschreitenden Verkehr auszuhandeln sind, wenn das Bestimmungsland kein "angemessenes Datenschutzniveau" aufweist. Gemäss Art. 12bis Abs. 2 lit. b i.V. mit Art. 9 Abs. 3 ist auch die Einholung entsprechender Genehmigungen nicht zwingend.
Fehler! Verweisquelle konnte nicht gefunden werden.	Art. 12bis Abs. 2 lit. a - d, insb. lit. c): Art. 9 Abs. 3 des Konventionsentwurfs ermöglicht den einzelnen Staaten ausdrücklich, die Befugnisse des Beauftragten eigenständig zu regeln. Insbesondere ist keine Verfügungskompetenz erforderlich. Die Kompetenzzuweisungen des geltenden Rechts hätten auch insofern problemlos beibehalten werden können.
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")		
Name/Firma	**Kapitel-Nr.**	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

www.jusletter.ch

David Rosenthal

Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet

Mit mehr als drei Monaten Verspätung präsentierte der Bundesrat am 21. Dezember 2016 den Vorentwurf für ein totalrevidiertes Datenschutzgesetz. Vieles, was er bietet, war erwartet worden. Dennoch stösst das «Weihnachtsgeschenk» auf enorme Resonanz. Insbesondere die strafrechtlichen Sanktionen sorgen für heftige Kritik. Doch der Vorentwurf birgt noch ganz anderen Zündstoff, der allerdings erst auf den zweiten und dritten Blick sichtbar wird. Der Beitrag legt diesen offen und beleuchtet, welche Folgen die Regelungen des Vorentwurfs für die Schweizer Wirtschaft hätten. Denn eines wird klar: Es besteht noch erheblicher Nachbesserungsbedarf.

Beitragsarten: Beiträge
Rechtsgebiete: Datenschutz

Zitiervorschlag: David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017

Inhaltsübersicht

[Rz 1] Viele Experten – so auch der Autor dieses Beitrags – sind der Ansicht, dass das bestehende Datenschutzgesetz (DSG) in der Sache vollauf genügt, selbst in Anbetracht der schnellen technischen Entwicklungen im Bereich der Informationstechnologie. In seiner Durchsetzung ist es wesentlich effizienter und kostengünstiger als es das neue DSG sein wird. Die Frage nach dem Sinn einer Revision des DSG ist jedoch aus zwei Gründen müssig: Erstens wird die revidierte Konvention 108 des Europarats[1], auf welchem schon das bisherige DSG aufbaut, diverse Anpassungen erforderlich machen.[2] Zweitens dominiert nicht nur in Bundesbern die Angst, die Schweiz könnte ihre Anerkennung als Land mit angemessenem Datenschutz durch die EU verlieren, sollte die Schweiz ihr DSG nicht massiv verschärfen. Ein solches Risiko besteht freilich nach der vorliegend vertretenen Auffassung nicht wirklich, und zwar schon gar nicht, wenn die Schweiz die revidierte Konvention 108 umsetzt, welche den freien Datenfluss mit der EU explizit vorsieht. Die Schweiz gibt sich in diesen Dingen viel zu wenig selbstbewusst. Wenn schon die Einhaltung des «Privacy Shield» für Exporte in die USA als ein datenschutzrechtlich angemessener Standard gilt[3], so wäre bereits das heutige Schweizer Recht hinreichend. Die Angst vor der EU ist somit ein schlechter Berater in dieser Sache. Schon gar nicht ist es angezeigt, in einem revidierten DSG über die Anforderungen der EU hinauszugehen.

[Rz 2] Noch bis zum 4. April 2017 ist es möglich, zum Vorentwurf für das revidierte DSG (VE DSG)[4] Stellung zu nehmen. Es ist davon auszugehen, dass die Vernehmlassung ein grosses Echo auslösen wird, was zu begrüssen ist. Das Bundesamt für Justiz dürfte versuchen, eine entspre-

1 Abrufbar unter http://www.coe.int/en/web/data-protection/modernisation-convention108 (bisher nur im Entwurf), Alle Websites zuletzt besucht am 13. Februar 2017.

2 Über deren Sinnhaftigkeit kann zwar gestritten werden, aber als die breitere politische Öffentlichkeit in Bundesbern von der Revision der Konvention Wind bekam, war es bereits zu spät. Zudem wird auch der Europarat von der EU dominiert, welche im Rahmen der Revision ihre Bedürfnisse, wie sie in der DSGVO ihren Niederschlag fanden, zu grossen Teilen durchgedrückt hat.

3 Vgl. etwa http://europa.eu/rapid/press-release_IP-16-2461_de.htm.

4 https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-21.html; eine englische Fassung ist erhältlich unter http://datenrecht.ch/vorentwurf-des-dsg-englische-fassung/.

chende Botschaft auszuarbeiten, die der Bundesrat möglichst noch vor der Sommerpause dieses Jahres dem Parlament unterbreiten müsste. In der Herbstsession würde dann das Geschäft in der Kommission des Erstrates, in der Wintersession im Plenum beraten werden können. Genügt dies, wird der Zweitrat sich in der Frühjahres- und Sommersession damit befassen können und das revidierte DSG im Sommer oder Herbst 2018 verabschiedet werden können. Damit ist ein Inkrafttreten frühestens auf Januar 2019 möglich, also etwas mehr als ein halbes Jahr nach dem Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018, die bekanntlich für eine ganze Reihe von Schweizer Firmen ebenfalls Anwendung findet. Ein solcher Zeitplan würde es erforderlich machen, dass das Bundesamt für Justiz noch während der parlamentarischen Beratung an den Ausführungsverordnungen arbeitet. Inzwischen halten einige einen solchen Fahrplan für viel zu optimistisch.

[Rz 3] Im Folgenden werden die neuen Regelungen des VE DSG erörtert, welche die Privatwirtschaft betreffen. Auf den behördlichen Datenschutz wird hier nicht eingegangen, auch nicht auf die Anpassungen im Zusammenhang mit Schengen. Wie gezeigt werden wird, haben es einige der Bestimmungen in sich, und sie gehen durchaus über das hinaus, was nach der DSGVO erforderlich ist. Ob ein solcher «Swiss Finish» wirklich sinnvoll ist, wird im Rahmen der Vernehmlassung zu klären sein. Vorliegend wird die Ansicht vertreten, dass strengere oder inkompatible Schweizer Alleingänge zweifellos nicht sinnvoll sind. Dies dürfte auch dem gegenwärtigen politischen Trend entsprechen. Es ist somit noch mit einigen Änderungen zu rechnen.

[Rz 4] Dies gilt im Übrigen auch für die sprachliche Ausgestaltung insbesondere der deutschen Fassung des Gesetzes, die gegenüber der französischen deutlich abfällt, die vermutlich Ausgangspunkt der Arbeiten war. Auf diese Punkte wird in diesem Beitrag nicht näher eingegangen. Es wäre aber sinnvoll, auf die Einheitlichkeit der Begrifflichkeiten zu achten. So ist zum Beispiel nicht ersichtlich, warum in Art. 14 VE DSG das eine Mal von einer «Bekanntgabe» von Personendaten die Rede ist und im nächsten Absatz von deren «Übermittlung».

1. Geltungsbereich wird eingeschränkt und ausgeweitet

[Rz 5] Die wichtigste Änderung im Geltungsbereich des revidierten DSG war schon vor dem VE DSG klar: Der Schutz juristischer Personen fällt weg. Erfasst sein soll neu nur noch die Bearbeitung von Daten, die sich auf eine bestimmte oder bestimmbare *natürliche* Person beziehen. Das entspricht der Regelung in fast allen Ländern. Die Anpassung wird kaum zu Diskussionen Anlass geben, auch wenn sie weder systemtreu noch wirklich konsequent ist: Nach Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB), welcher durch das DSG konkretisiert wird, geniessen auch juristische Personen Persönlichkeitsschutz, und sie tun es weiterhin; Art. 13 der Bundesverfassung (BV) gewährleistet den Schutz der Persönlichkeit auch von juristischen Personen. Eine Verletzung durch die Bearbeitung von Personendaten von juristischen Personen ist also über diesen Umweg nach wie vor möglich, wenngleich die Fälle eher selten sein werden.[5] Der Vorteil der Streichung wird sein, dass die formalen Vorschriften betreffend Daten über Firmen wegfallen. Dies wird etwa dem Schindluder mit dem Auskunftsrecht nach dem heutigen Art. 8 DSG (Art.

[5] Das DSG wird hierbei vermutlich analog beigezogen werden. Werden also Daten einer Firma zweckwidrig verwendet, kann argumentiert werden, dass dies Art. 28 ZGB verletzt, weil ein solches Verhalten gemäss DSG eine Persönlichkeitsverletzung darstellt.

20 VE DSG) bei Unterlagen betreffend juristische Personen Einhalt bieten; das Auskunftsrecht dient heute primär der Beschaffung von Beweismitteln für Prozesse und anderen, datenschutzfremden Zwecken, was aber durch die bisherige Gerichtspraxis leider ohne Not geschützt wird.[6] Allerdings darf die Wirkung der Streichung des Schutzes juristischer Personen nicht überbewertet werden: Unternehmen handeln regelmässig durch ihre Organe und Hilfspersonen, und deren Personendaten sind weiterhin durch das DSG erfasst und zwar auch im professionellen Kontext.[7]

[Rz 6] Geht es um Daten natürlicher Personen, wird dem Auskunftsrecht mit dem VE DSG allerdings eine noch grössere Bühne bereitet als bisher: Das DSG soll künftig – ausser für die Gerichte selbst[8] – selbst im Rahmen bereits hängiger Zivilprozesse und laufender Strafverfahren gelten. Somit kann neu selbst während solchen Verfahren weiterhin das Auskunftsrecht zur Beweisbeschaffung benutzt werden, was für eine betroffene Person zweifellos attraktiv ist, da für diese Form der Beweisbeschaffung weder etwas bezahlt werden muss, noch sonst die hohen Hürden der Zivilprozessordnung für Editionsbegehren gelten. Der Missbrauch ist damit leider vorprogrammiert und dürfte mangels sinnvoller Anpassung des Auskunftsrechts in Art. 20 f. VE DSG (vgl. Rz 54 ff., hinten) von den Gerichten weiterhin geschützt werden.

[Rz 7] Der Vorentwurf ändert nicht nur den Geltungsbereich, sondern auch die Begrifflichkeiten in einigen Bereichen. Die gewichtigste Anpassung dürfte die Abschaffung der «Persönlichkeitsprofile» und deren Ersatz durch den Begriff des «Profiling» sein. Dieser umfasst nach Art. 3 Bst. f VE DSG «jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität». Diese Definition ist extrem breit, und die Schweiz geht damit deutlich über die entsprechende Regelung der EU hinaus. Anders als in der DSGVO ist auch das Profiling von Hand erfasst, also beispielsweise das Ausfüllen einer Mitarbeiterbeurteilung oder die Einschätzung eines Arztes, wie sich die Krankheit einer Person entwickeln wird. Aber auch die Versicherung, die im Rahmen einer Police ein Alterskapital berechnet, nimmt nach dem Wortlaut der VE DSG ein Profiling vor, da sie eine Entwicklung bezüglich wirtschaftlicher Lage des Versicherten prognostiziert. Dies alles gilt neu nach Art. 23 Abs. 2 Bst. d VE DSG *per se* als Persönlichkeitsverletzung, was wiederum einen Rechtfertigungsgrund erfordert, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden ist. Eine solche Regelung erscheint doch etwas übertrieben.

[Rz 8] Ob für das Profiling Personendaten benutzt werden oder nicht, spielt zudem keine Rolle («Daten oder Personendaten»). Die Befürchtung, dass damit auch das Bearbeiten von nicht personenbezogenen Daten plötzlich erfasst wäre, dürfte zwar unberechtigt sein: Hier greift Art. 2 Abs. 1 VE DSG, wonach das DSG nur dann gilt, wenn Personendaten bearbeitet werden. Ein Profiling ist somit dann erfasst, wenn sich mindestens das Ergebnis auf eine bestimmte oder bestimmbare Person bezieht. Die Formulierung «Daten oder Personendaten» ist trotzdem unnötig

---

6 Vgl. statt vieler BGE 138 III 425 und Urteil des Bundesgerichts 4A_506/2014 vom 3. Juli 2015; vgl. auch David Rosenthal, Aktuelle Anwaltspraxis 2013, S. 731 ff.; ders., Aktuelle Anwaltspraxis 2015, S. 586 ff.

7 Hierbei ist auf Erwägung 14 der DSGVO hinzuweisen, die erklärt, dass die DSGVO keine Anwendung finden soll auf die Kontaktdaten juristischer Personen, was häufig natürliche Personen sind. Die Tragweite dieser Erklärung ist allerdings nicht klar. Es gibt etliche Daten natürlicher Personen in ihrer Eigenschaft als Arbeitnehmer einer juristischen Person, die ohne Weiteres schutzwürdig sind.

8 Der VE DSG regelt nur noch die eidgenössischen Gerichte; die Datenbearbeitung der kantonalen Gerichte wird von den kantonalen Datenschutzgesetzen geregelt werden müssen. Allerdings ist die diesbezügliche Regelung in Art. 57 VE DSG mit Bezug auf Art. 2 Abs. 3 VE DSG nicht korrekt formuliert. Es fehlt der Hinweis, dass die Regelungen für eidgenössische Gerichte im kantonalen Recht sinngemäss für kantonale Gerichte umzusetzen ist.

und irreführend: Handelt es sich beim Output eines Profilings um Personendaten, muss es sich naturgemäss auch beim Input um solche handeln, weil ein Personenbezug offenkundig möglich ist, wie das Profiling selbst beweist. Der Hinweis auf «Daten» ist daher zu streichen.

[Rz 9] Der Katalog der besonders schützenswerten Personendaten wurde wie von der revidierten Konvention 108 vorgegeben um genetische und biometrische Daten erweitert, letztere mit der Einschränkung, dass nur Daten gemeint sind, die eine natürliche Person eindeutig identifizieren. Diese Beschränkung ist allerdings wenig hilfreich: Jedes Gesichtsfoto soll nach dem Vorentwurf künftig als besonders schützenswertes Personendatum gelten. Gedacht war die Regelung an sich etwas enger: Gemäss dem Erläuterungsbericht sollen nur jene Fotos erfasst sein, die mit spezifischen technischen Mittel so bearbeitet wurden, dass eine eindeutige Identifizierung oder Authentisierung eines Individuums möglich ist. Gemeint sind also Fälle der Gesichtserkennung, wobei die meisten Fälle wiederum aufgrund fehlender Zuverlässigkeit in der Erkennung wegfallen dürften. Hier besteht somit noch Nachbesserungsbedarf in der Legaldefinition. Erfasst sein sollten nach Art. 3 Bst. c Ziff. 4 VE DSG nicht jene biometrische Daten, die eine natürliche Person eindeutig identifizieren, sondern nur solche, die zum Zweck bearbeitet werden, dies zu tun. Mehr verlangt auch die Konvention 108 nicht. Bilder in der Zeitung, auf welchen Personen zu erkennen sind, wären nach dieser Definition somit nicht mehr besonders schützenswerte Personendaten, während dies gemäss Vorentwurf noch so wäre.

[Rz 10] Weggefallen ist auch das Konzept der Inhaberschaft einer Datensammlung. Es wurde ersetzt durch den in der EU schon seit langem gebräuchlichen Begriff des «Verantwortlichen» (*Controller*) und des «Auftragsbearbeiters» (*Processor*). Die Definition des Verantwortlichen gibt aber nicht ganz das in Europa herrschende Begriffsverständnis wieder: Der Verantwortliche zeichnet sich nicht dadurch aus, dass er über Zweck, Mittel und Umfang der Bearbeitung der Daten entscheidet, sondern dass er dies *final* tut oder tun kann, also der «Herr der Daten» ist. In der Praxis wird der Entscheid über die Mittel und den Umfang der Datenbearbeitung häufig dem Auftragsbearbeiter delegiert, wie z.B. auch die Bestimmung der angemessenen Schutzmassnahmen. In den Erläuterungen wird ohne Begründung vertreten, dass die Arbeitnehmer eines Verantwortlichen nicht als Auftragsbearbeiter gelten, was systematisch und dogmatisch falsch ist. Die Regeln der Auftragsbearbeitung müssen auch im Verhältnis zu den eigenen Arbeitnehmern gelten, denen ein Unternehmen die Bearbeitung von Daten anvertraut, auch wenn die Genehmigung nach Art. 7 Abs. 3 VE DSG regelmässig implizit als erteilt gelten wird und die Information nach Art. 13 Abs. 4 VE DSG für diese Fälle keinen Sinn macht. Diese beiden Neuerungen sollten daher relativiert werden.

[Rz 11] Anpassungsbedarf besteht ferner bezüglich der Verantwortlichkeiten des Auftragsbearbeiters: Zahlreiche der neuen Bestimmungen nehmen nicht nur den Verantwortlichen in die Pflicht, sondern parallel auch den Auftragsbearbeiter. Dieser wird jedoch oftmals gar nicht in der Lage sein, aus eigenem Antrieb oder in eigener Verantwortlichkeit diesen Pflichten nachzukommen; in der DSGVO werden die Auftragsbearbeiter nicht derart in die Pflicht genommen. Beispiele hierfür sind die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 16 VE DSG), *Privacy by Design* und *Privacy by Default* (Art. 18 VE DSG) oder die Information von Datenempfängern über etwaige Berichtungen oder Löschungen von Daten (Art. 19 VE DSG). Für all diese Aufgaben kann sinnvollerweise nur der Verantwortliche verantwortlich sein, auch wenn er zu deren Umsetzung allenfalls die Hilfe eines Auftragsbearbeiters beanspruchen wird.

[Rz 12] Der Begriff der Datensammlung selbst soll im revidierten DSG ebenfalls weggefallen. Dogmatisch und systematisch war das Konzept der Inhaberschaft sauberer und differenzierter

als die neue Lösung, aber sie war seit je her selbst für Spezialisten schwer zu verstehen. Die Anpassung erscheint als Massnahme zur Harmonisierung mit den internationalen Gepflogenheiten im Datenschutzrecht daher sinnvoll. Sie hat immerhin die Folge, dass diverse Pflichten ausgeweitet werden: Das Auskunftsrecht nach Art. 8 DSG galt bisher nur für Daten in Datensammlungen; neu soll es jedenfalls nach dem Wortlaut für alle Daten, die ein Verantwortlicher bearbeitet, gelten (Art. 20 Abs. 1 VE DSG). Sinngemäss wird es freilich weiterhin nur für jene Daten zur Anwendung kommen können, die nach der betroffenen Person erschlossen werden können, denn wenn ein Verantwortlicher selbst nicht ohne Weiteres nach einer bestimmten Person in seinem Datenbestand suchen kann, weil es für seine Datenbearbeitung keine Rolle spielt, wird dies von ihm auch im Rahmen des Auskunftsrechts nicht verlangt werden können. Anwendungsfälle, wo sich der Unterschied zeigt, könnten zum Beispiel Aufnahmen von Sicherheitskameras sein: Sie sind regelmässig keine Datensammlung, da sie nicht nach betroffenen Personen erschlossen werden können. Gibt eine Person unter neuem Recht an, wann sie von einer Kamera erfasst wurde und will sie die Aufnahme sehen, wird ihr dieser Zugang unter neuem Recht gewährt werden müssen. Die praktische Relevanz ist in diesem Falle allerdings beschränkt: Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) stellt sich aufgrund des gefühlten Datenschutzes und ohne Rechtsgrundlage auf den Standpunkt, dass schon unter heutigem Recht eine Auskunftspflicht besteht, und kaum jemand wagte es bisher, ihm zu widersprechen.

2. Kein Methodenwechsel bei «Personendaten»

[Rz 13] Vom Wegfall des Schutzes juristischer Personen abgesehen, soll der Begriff der Personendaten auch im neuen Recht so bleiben, wie er ist[9]. Dies war ein mit Spannung erwarteter Punkt und der Entscheid ist richtig und wichtig. Es bleibt somit bei durch die bundesgerichtliche Rechtsprechung bestätigten «relativen» Methode, wenn es darum geht zu ermitteln, ob die betroffene Person bestimmbar ist. Danach genügt es nicht, dass der Aufwand zur Identifizierung objektiv gering genug ist, dass ein Interessent ihn nach allgemeiner Lebenserfahrung auf sich nimmt (objektive Komponente). Wesentlich ist ebenso, welches Interesse der Datenbearbeiter oder ein Dritter mit Zugang zu den Daten an der Identifizierung hat (subjektive Komponente), was vom konkreten Fall abhängig ist.[10] Es genügt daher nicht wie bei der «absoluten» Methode, dass irgendjemandem die Identifizierung möglich ist. Obwohl in der EU immer wieder die «absolute» Methode vertreten wird, hat der EuGH kürzlich auch für das geltende EU-Recht die relative Methode bestätigt.[11]

[Rz 14] Daran dürfte sich auch unter der DSGVO bei richtiger Auslegung nichts ändern. Zwar wird im Falle der DSGVO teilweise vertreten, dass bereits dann Personendaten vorliegen, wenn sie eine «Singularisierung» erlauben, also so spezifisch sind, dass sie sich nur noch auf eine bestimmte Person beziehen können, selbst wenn sich diese nicht identifizieren lässt. Dies übersieht

9 Erläuterungen VE DSG, S. 43.

10 BGE 136 II 508, E. 3.2.

11 Urteil des EuGH vom 19. Oktober 2016 C-582/14 *Breyer*, welches die Frage der Identifikation des Inhabers einer IP-Adresse zum Inhalt hatte. Während die Bestimmbarkeit der betroffenen Person für den Internet-Service-Provider klar war (RN 33 f., mit Hinweis auf den Urteil des EuGH vom 24. November 2011 C-70/10 *Scarlet Extended*), war sie gemäss EuGH für den Betreiber einer Website, der die IP-Adresse für den Fall von Cyberangriffen aufzeichnete, separat zu prüfen (RN 44–49). Damit folgte der EuGH wie schon zuvor BGE 136 II 508 auch für das EU-Recht der «relativen» Methode.

jedoch, dass die DSGVO die Singularisierung nur als Indiz für eine Identifizierbarkeit vorsieht[12] und sie als Konzept über massive Mängel verfügt, die sie untauglich werden lassen.[13] Wesentlich zuverlässiger ist hierbei der sog. Referenzdaten-Test, wie ihn auch der EuGH angewandt hat.[14]

[Rz 15] Das Festhalten am bisherigen Begriff des Personendatums im Vorentwurf bedeutet insbesondere, dass die Bekanntgabe von pseudonymisierten Daten an Personenkreise, die nicht über den Schlüssel zur Zuordnung der Daten zu betroffenen Personen verfügen, weiterhin *keine* Bekanntgabe von Personendaten darstellen wird und daher auch die diesbezüglichen datenschutzrechtlichen Kautelen nicht beachtet werden müssen. Dies gilt jedenfalls solange die Nichtidentifizierbarkeit der Daten durch die Dritten sichergestellt ist. Das macht auch Sinn. Wäre dem nämlich nicht so, wäre beispielsweise die Bekanntgabe von geschwärzten Unterlagen durch Behörden oder Unternehmen an vielen Orten nicht mehr zulässig, ebenso nicht die Speicherung von vollverschlüsselten Daten auf einem Speichersystem im Internet. Beides sind letztlich Formen der Pseudonymisierung.

3. Bisheriges Regelungskonzept mit Bearbeitungsgrundsätzen bleibt

[Rz 16] Das bisherige Regelungskonzept des DSG, welches von einer generellen Erlaubnis zur Bearbeitung von Personendaten ausgeht und einzelne Fälle definiert, in welchen sie verboten ist, soll bestehen blieben. Es gilt im privaten Bereich somit weiterhin das Prinzip des «opt-out», nicht des «opt-in». Eine Zustimmung zur Bearbeitung von Personendaten ist weiterhin nicht zwingend; anders als in der DSGVO soll es in der Schweiz nicht erforderlich sein, für eine Datenbearbeitung einen Rechtfertigungsgrund vorweisen zu können.[15] Ein Rechtfertigungsgrund wird nur und erst dann benötigt, wenn eine Datenbearbeitung die Persönlichkeit einer betroffenen Person verletzt, was sich neu aus Art. 24 VE DSG ergibt. In welchen Fällen eine Persönlichkeitsverletzung vorliegt, umschreibt Art. 23 VE DSG, welcher gegenüber dem heutigen Art. 12 DSG erweitert wurde.

[Rz 17] Aber auch hier bleibt das Grundkonzept dasselbe: In Art. 23 Abs. 2 VE DSG wird aufgezählt, in welchen Fällen eine Persönlichkeitsverletzung *per se* vorliegt, nämlich bei Verletzung der Bearbeitungsgrundsätze, bei einer Datenbearbeitung gegen den erklärten Willen einer betroffenen Person (wie bisher), bei der Bekanntgabe von besonders schützenswerten Personendaten an Dritte (wie bisher) und beim Profiling ohne ausdrückliche Einwilligung der betroffenen Person.

---

12 Erwägung 26 der DSGVO («To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, . . . »).

13 Beispielsweise wäre ein automatisches Foto einer Person in einer misslichen Lage aufgrund der Einmaligkeit der Aufnahme selbst dann ein Personendatum, wenn ausser dieser Person selbst kein Mensch auf der Welt herausfinden kann, um wen es sich handelt.

14 Hierbei wird geprüft, ob die bearbeiteten Daten bereits verfügbaren oder nach allgemeinem Ermessen wahrscheinlich verfügbaren Daten real existierender Personen eindeutig zugeordnet werden können. Können aus biologischem Material beispielsweise genetische Daten gewonnen werden, so werden diese erst dann zu Personendaten, wenn diese mit Referenzdaten realer, bekannter Personen abgeglichen werden können, wobei solche Referenzdaten oder Vergleichsproben normalerweise nicht verfügbar sein werden (vgl. Botschaft Humanforschungsgesetz, BB 2009 8045, 8096). Denselben Test wendete auch das Urteil des EuGH vom 19. Oktober 2016 C-582/14 *Breyer* an, um festzustellen, ob eine IP-Adressen für einen Website-Provider Personendaten darstellen, was es im konkreten Fall bejahte, da er davon ausging, dass er Zugang zu den Referenzdaten des Internet-Service-Providers erlangen würde. Die Frage der Zugänglichkeit zu Referenzdaten ist jeweils aus der Perspektive derjenigen zu beurteilen, die Zugang zu den bearbeiteten Personendaten haben («relative Methode»).

15 Vgl. Art. 6 DSGVO.

Letztere Regelung ist neu und insofern nicht ganz nachvollziehbar, als dass der Begriff des Profiling extrem breit definiert ist. Dies wird zweifellos noch für Diskussionen sorgen.

[Rz 18] Art. 23 Abs. 2 Bst. a VE DSG führt neu auch Art. 5 und 6 VE DSG auf, welche sich auf die Bekanntgabe ins Ausland beziehen. Dies ist lediglich eine redaktionelle Klarstellung, denn schon bisher war eine unerlaubte Bekanntgabe ins Ausland als Persönlichkeitsverletzung zu werten. Die Aufzählung von Art. 5 und 6 VE DSG in Art. 23 VE DSG ändert allerdings nichts daran, dass die Rechtfertigungsgründe in Art. 24 VE DSG, insbesondere der Rechtfertigungsgrund des überwiegenden privaten Interesses, in den Fällen von Art. 5 und 6 VE DSG keine Anwendung finden.

[Rz 19] Hinzuweisen ist in diesem Zusammenhang allerdings auf einen Fehler in den Erläuterungen: Diesen zufolge kommt Art. 23 Abs. 3 VE DSG (er handelt von veröffentlichten Daten) angeblich nur zum Tragen, wenn die Bearbeitung von Daten rechtmässig erfolge, d.h. die Grundsätze von Art. 4, 5, 6 und 11 eingehalten würde.[16] Das ist falsch. Abs. 3 führt dazu, dass die Bearbeitung von Daten, die mit Wissen und Willen einer Person publiziert wurden, in der Regel selbst dann rechtmässig ist, wenn sie unter Verletzung der Bearbeitungsgrundsätze erfolgt. Das war schon im bisherigen Recht so.

[Rz 20] Die exemplarische Aufzählung der Fälle, in welchen von einem überwiegenden Interesse auszugehen ist, wurde überarbeitet. Sie entsprechend im Kern der heutigen Regelung von Art. 13 Abs. 2 DSG, mit gewissen geringfügigen Anpassungen:

- Der Rechtfertigungsgrund der Kreditüberprüfung soll nur noch gelten, wenn die betroffene Person volljährig ist, was zwar auf den ersten Blick zum Schutz von Kindern einleuchten mag, aber bei näherer Betrachtung nicht sinnvoll erscheinen: Online-Shops, die auch von nicht volljährigen Kunden genutzt werden, stellen zum Beispiel häufig auf automatisierte Kreditprüfungen ab, in deren Rahmen sie auch erfahren, ob eine Person bereits volljährig ist oder nicht. Auf diese Datenquelle würde verzichtet werden müssen. Nicht volljährige Personen werden notabene mindestens bei gewissen Kreditauskunfteien zwar als solche ausgewiesen, erhalten aber automatisch ein positives Kreditrating. Diese Daten dürfen neu möglicherweise nicht mehr bereitgehalten werden. Weiterhin nicht bearbeitet werden dürfen auch besonders schützenswerte Personendaten, was in jenen Fällen als problematisch erscheint, als dass es sich um Daten zu Verurteilungen im Zusammenhang mit bestimmten Vermögensdelikten handelt, die durchaus von erheblicher Relevanz für die Kreditwürdigkeit einer Person sind.
- Der Rechtfertigungsgrund der nicht-personenbezogenen Bearbeitung erfordert nun nicht mehr nur, dass die Ergebnisse so veröffentlicht werden, dass keine Rückschlüsse auf die betroffenen Personen mehr möglich sind. Auch vorgängig darf Dritten nichts bekanntgegeben werden, was aus deren Sicht Personendaten sind. Sie müssen somit pseudonymisiert oder anonymisiert werden. Zudem wird in Erinnerung gerufen, dass Personendaten anonymisiert werden müssen, sobald es der Zweck der Bearbeitung erlaubt. Das ergab sich allerdings schon bisher aus dem Grundsatz der Verhältnismässigkeit.

[Rz 21] Die Formulierung von Art. 24 Abs. 2 VE DSG ist insofern zurückhaltender geworden, als dass nun davon die Rede ist, dass in den aufgeführten Fällen das überwiegende private Interesse nur noch «möglicherweise» gegeben ist. Gemäss den Erläuterungen soll dies darauf hinwirken,

16 Erläuterungen VE DSG, S. 69.

dass die spezifischen Umstände des Einzelfalls stärker berücksichtigt werden.[17] Für diese Einschränkung gibt es jedoch keinen Grund; die bisherige Regelung und Formulierung hat sich bestens bewährt. Durch die Einführung des Worts «möglicherweise» wird nunmehr die Rechtssicherheit, welche mit Art. 23 Abs. 2 VE DSG geschaffen werden soll, gleich wieder zunichtegemacht. Schon die bisherige Regelung galt nicht absolut, aber sie stellte klar: Gibt es keine gewichtigen Gründe von der Bewertung in Art. 13 Abs. 2 DSG abzuweichen, wird das überwiegende Interesse nach Ansicht des Gesetzgebers gegeben sein. Zu Problemen führte dieses System bisher nicht; dazu sind die aufgezählten Fälle zu klar.

[Rz 22] Die Bearbeitungsgrundsätze wurden im VE DSG sinnvollerweise in Art. 4 zusammengefasst. Es sind jedenfalls auf den ersten Blick keine grundlegenden Änderungen ersichtlich. Der Grundsatz der Zweckbindung und Erkennbarkeit wurde in Art. 4 Abs. 3 VE DSG zusammengefasst. Bisher genügte es für die Zweckbindung, dass eine bestimmte Bearbeitung vom Schweizer Recht vorgeschrieben war. Nach dem neuen Wortlaut und System scheint das nicht mehr der Fall zu sein. Dies würde bedeuten, dass Unternehmen auch auf gesetzlich vorgeschriebene Datenbearbeitungen hinweisen müssen, was wenig sinnvoll erscheint. Dieser Punkt bedarf der Klärung mindestens in den Erläuterungen, wonach die Tatsache, dass eine Bearbeitung gesetzlich vorgesehen ist, diese zugleich auch erkennbar macht.

[Rz 23] Das in Abs. 3 neu eingefügte Erfordernis der «klaren» Erkennbarkeit ist hingegen ersatzlos zu streichen: Es ist nicht ersichtlich, welchen Mehrwert dieser Zusatz hat; eine materielle Änderung gegenüber der heutigen Rechtslage ist erklärtermassen nicht beabsichtigt.[18] Die Deutlichkeit, mit welcher auf einen bestimmten Bearbeitungszweck hinzuweisen ist, ergibt sich schon unter dem heutigen Recht aus dem Risiko, dass mit ihm für die betroffene Person verbunden ist. Es gibt keinen Grund, daran etwas zu ändern. Das Wort «klar» im Zusammenhang mit der Erkennbarkeit des Bearbeitungszwecks sorgt lediglich für Verwirrung.

[Rz 24] Zu begrüssen ist hingegen die Einführung «kompatibler» Bearbeitungszwecke. Nach Art. 4 Abs. 3 Satz 2 VE DSG ist neu die Bearbeitung von Daten auch zu Zwecken erlaubt, die zwar nicht erkennbar, mit den erkennbaren Zwecken aber «vereinbar» sind. Damit greift die Formulierung ein Konzept auf, welches das EU-Recht bereits kennt und in der Praxis gewisse Erleichterungen mit sich bringt.[19] Ein typisches Beispiel ist die Anonymisierung von zu einem Zweck A beschafften Personendaten, um sie für den Zweck B zu verwenden. Der Vorgang der Anonymisierung ist eine Datenbearbeitung, die ihrerseits dem Zweckbindungsgrundsatz unterliegt. Ist dieser Zweck B nicht von Anfang an erkennbar gewesen, verlangt seine Verfolgung an sich einen Rechtfertigungsgrund. Das ist neu nicht mehr der Fall.

[Rz 25] Ein weiteres Praxisbeispiel ist die Beschaffung von Kundendaten zwecks Abwicklung von Verträgen. Will das Unternehmen diese Daten auch für eigene Targeting-, Analyse- oder Marketingzwecke verwenden und hat es dies im Rahmen der Datenbeschaffung nicht angekündigt, so stellt sich unter heutigem Recht die Frage, ob diese Nutzungen mindestens aus den Umständen ersichtlich waren. Ist dem (ausnahmsweise) nicht so, wäre ein Rechtfertigungsgrund erforderlich. Neu entfällt dieses Erfordernis: Beide Nutzungen dürften zwar vom ursprünglichen Be-

17 Erläuterungen VE DSG, S. 69.

18 Erläuterungen VE DSG, S. 46.

19 Art. 6 Abs. 4 DSGVO.

schaffungszweck nicht abgedeckt, mindestens aber mit diesem «vereinbar» sein.[20] Nicht richtig ist allerdings die Aussage in den Erläuterungen, dass eine Weiterbearbeitung dann als vereinbar gilt, wenn sie durch einen Rechtfertigungsgrund wie etwa eine Einwilligung des Betroffenen legitimiert ist;[21] hierbei werden zwei verschiedene Konzepte unzulässigerweise miteinander vermischt. Ob ein neuer Datenbearbeitungzweck mit dem ursprünglichen Zweck vereinbar ist, ergibt sich aus einer inhaltlichen Verwandtschaft, den möglichen Auswirkungen der Datenbearbeitung zum neuen Zweck, vorhandenen Massnahmen zum Schutz der betroffenen Person oder ihrem Verhältnis zum Verantwortlichen.

[Rz 26] Nur scheinbar neu ist der Grundsatz in Art. 4 Abs. 4 VE DSG, welcher eine Anonymisierung von Daten verlangt, sobald der Zweck der Bearbeitung dies erlaubt. In Tat und Wahrheit ergab sich dies schon bisher aus dem Grundsatz der Verhältnismässigkeit, der weiterhin gilt[22]. Neu formuliert wurde auch der Grundsatz der Datenrichtigkeit in Art. 4 Abs. 5 VE DSG, dessen neuer Wortlaut etwas absoluter abgefasst ist, als bisher. Da eine Änderung des bisherigen Rechts nicht beabsichtigt ist,[23] stellt sich allerdings die Frage, warum der Wortlaut angepasst wird; die bisherige Formulierung erscheint sachgerechter.

[Rz 27] Die Verletzung der Bearbeitungsgrundsätze in Art. 4 VE DSG wird notabene weiterhin nicht sanktioniert.

4. Einwilligung: Alles bleibt beim Alten

[Rz 28] Die Einwilligung schien bisher das Allerheilmittel im Datenschutz zu sein, geht es doch letztlich um informationelle Selbstbestimmung. Die Anpassungen der DSGVO in diesem Bereich liessen allerdings Böses erahnen. Auch hier haben sich die Befürchtungen nicht bewahrheitet: Der Wortlaut der Definition der Einwilligung in Art. 4 Abs. 6 VE DSG wurde zwar um den Hinweis erweitert, dass eine Einwilligung eindeutig sein muss, um gültig zu sein. Damit wird jedoch lediglich wiederholt, was heute schon gilt.[24] Es gilt auch im Bereich der Einwilligung weiterhin ein risikobasierter Ansatz: Je einschneidender die Folgen einer Einwilligung, desto klarer muss sie sein. Je ungewöhnlicher die beabsichtigte Datenbearbeitung, desto deutlicher muss darauf hingewiesen werden. Die Erläuterungen sind insofern nicht korrekt, als dass eine Einwilligung nicht den gesamten Zweck einer Bearbeitung abdecken muss[25]; es genügt, dass sie jenen Teil einer Bearbeitung abdeckt, für den sie eingeholt wird.

[Rz 29] Nach Schweizer Recht wird es aber weiterhin möglich sein, dass etwa ein Kästchen auf einem Online-Formular, das eine bestimmte Datenbearbeitung für erlaubt erklärt, standardmässig bereits angekreuzt ist. Dies wird unter der DSGVO mit der Begründung abgelehnt, dass die Einwilligung in Bezug auf diese Bearbeitung nicht mehr eine unmissverständliche sei, was dort be-

20 Erläuterungen VE DSG, S. 46, welche das Versenden von unverlangten Werbe-E-Mails als Beispiel für eine nicht vereinbare Nutzung nennt.

21 Erläuterungen VE DSG, S. 46.

22 Art. 4 Abs. 2 VE DSG.

23 Erläuterungen VE DSG, S. 47.

24 Erläuterungen VE DSG, S. 47.

25 Ebd.

grifflich ebenfalls verlangt wird.[26] Die Begründung verkennt jedoch den Gesamtzusammenhang und stimmt jedenfalls für die Schweiz nicht: Ist das Kästchen in seinem Zustand (angekreuzt oder nicht) Gegenstand einer Erklärung, die ihrerseits einer eindeutigen Willensbekundung der betroffenen Person unterliegt, so gilt dies auch für den Inhalt des Kästchens, und zwar gleichgültig, ob es zunächst angekreuzt war oder nicht. Entscheidend ist der Zustand zum Zeitpunkt der Willenserklärung. Sonst wäre auch jeder Satz, der ganz ohne Wahlmöglichkeit angezeigt wird («Es gelten die AGB und die Preisliste.») nicht von der Willenserklärung erfasst, was wohl niemand behaupten wird und auch den Grundkonzepten des Schweizer Rechts zuwiderlaufen würde. Wenn überhaupt müsste die Frage der Voreinstellung des Kästchens im Rahmen der Regelung zum «*Privacy by Default*» in Art. 18 Abs. 2 VE DSG beantwortet werden (dazu Rz 79 hinten).

[Rz 30] Verwirrend sind die Ausführungen der Erläuterung in Bezug auf die Frage, wann eine Einwilligung eines «ausdrückliche» ist, wie sie für besonders schützenswerte Personendaten und das Profiling erforderlich ist.[27] Hierzu gibt es verschiedene Ansichten, wobei nicht klar ist, worin sich diese wirklich unterscheiden.[28] Zur vermeintlichen Klärung wurden im VE DSG die französischen und italienischen Begriffe «explicite» und «explicito» durch «exprès» und «espresso» ersetzt. Es wird ausgeführt, dass dies auch durch ein Zeichen geschehen kann, wie etwa das Anklicken einer Schaltfläche.[29] Die Frage, wann eine Einwilligung eine ausdrückliche ist, wird damit freilich nicht geklärt.

[Rz 31] Hierzu ist es nötig, das Wesen der Einwilligung in seine Einzelteile zu zerlegen. Leider herrscht auch in der Grundlagenliteratur zum Obligationenrecht bezüglich den verschiedenen Arten der Willenserklärung, wie sie auch jeder Einwilligung zugrunde liegt, ein Wildwuchs.[30] Die meisten Definitions- und Erklärungsversuche erweisen sich bei näherer Betrachtung als nicht zu Ende gedacht oder sogar in sich widersprüchlich. Dabei werden Begriffe wie «ausdrücklich», «konkludent» und «Stillschweigen» beliebig gemischt und gegenübergestellt.[31] So wird teilweise behauptet, die Frage der Ausdrücklichkeit beziehe sich nur auf die Form einer Willenserklärung, was schon begrifflich falsch ist, weil das Gegenstück zur ausdrücklichen Willenserklärung – die konkludente – sich sachlogisch überhaupt nur aus einer inhaltlichen Komponente ergeben kann. Wird nur von der Form einer Willenserklärung gesprochen, so ist zwischen aktivem und passivem Verhalten und den dazu benutzten Elementen wie Sprache, Gestik, Schrift oder sonstigen Bewegungen zu unterscheiden. Ein solches Verhalten muss jedoch immer in einen inhaltlichen Kontext gesetzt werden, um zur Willenserklärung zu werden; auch ein simples «Ja» oder der

---

26 Art. 4 Ziff. 11 DSGVO, Erwägung 32 DSGVO (wonach ein bereits angekreuztes Kästchen dem Stillschweigen gleichgestellt wird).

27 Es stellt sich die Frage, ob es überhaupt in allen vorgesehenen Fällen sinnvoll ist, eine ausdrückliche Einwilligung zu verlangen; gerade der Begriff des Profiling ist so breit angelegt, dass er auch viele nicht sensible Konstellationen erfasst. Dass trotzdem Ausdrücklichkeit verlangt wird, wird rein historische Gründe haben, da sie bisher auch für Persönlichkeitsprofile verlangt wurde.

28 Erläuterungen VE DSG, S. 47, m.w.H.

29 Erläuterungen VE DSG, S. 47 f.

30 Vgl. Alfred Koller, Schweizerisches Obligationenrecht Allgemeiner Teil, § 3, Rn. 127, der von einem «eigentlichen Wirrwarr» spricht.

31 Claire Huguenin, Obligationenrecht Allgemeiner und Besonderer Teil, Rn. 175, stellt der ausdrücklichen Willenserklärung die konkludente gegenüber, wobei die stillschweigende Erklärung als Unterfall der konkludenten und ausnahmsweise auch der ausdrücklichen Willenserklärung erachtet wird. Gl.M. Ernst Kramer/Bruno Schmidlin, in: Berner Kommentar, Arthur Meier-Hayoz (Hrsg.), Art. 1, Rn. 9; Andreas Furrer/Markus Müller-Chen, Obligationenrecht Allgemeiner Teil, Kapitel 2, Rn. 52. Andreas von Tuhr, Allgemeiner Teil des Schweizerischen Obligationenrechts, S. 163, bezeichnet die konkludente Willenserklärung hingegen als Unterfall der stillschweigenden; so auch Max Keller/Christian Schöbi, das Schweizerische Schuldrecht, Band I, S. 32.

Klick auf den «Ich stimme zu»-Knopf auf einer Website sagt für sich nichts aus.[32] Erst aus diesem Zusammenspiel von Form und Inhalt ergibt sich, ob eine Willenserklärung eine ausdrückliche oder – dem Gegenstück – eine konkludente ist.

[Rz 32] Ausdrücklich ist eine Einwilligung in eine Datenbearbeitung korrekterweise dann, wenn ein (i) aktives Verhalten oder ein solches vorliegt, das als affirmativ vereinbart wurde[33], und (ii) die Bedeutung dieses affirmativen Verhaltens sich direkt auf die betreffende Datenbearbeitung bezieht. Nicht ausdrücklich und somit konkludent ist eine Einwilligung in eine Datenbearbeitung dann, wenn das affirmative Verhalten sich lediglich auf eine Handlung bezieht, welche die fragliche Datenbearbeitung zur Folge hat und nicht auf die Datenbearbeitung selbst.

[Rz 33] Ein Beispiel illustriert dies: Wer ein Produkt auf die Ladentheke legt, gibt kund, dass er dieses Produkt kaufen möchte. Dies ergibt sich aus den Umständen. Nimmt die Person die gleiche Handlung zu Hause am Küchentisch vor, würde dies hingegen nicht bedeuten, dass sie das Produkt kaufen möchte; der Wille das Produkt kaufen zu wollen, wird nicht ausdrücklich kundgetan, sondern geht lediglich aus den Umständen hervor. Ausdrücklich ist hierbei höchstens die Tatsache, dass die Sache auf die Theke gelegt worden ist. Wer für den Kauf eines Produkts ein Formular mit seinen Personendaten ausfüllt und dieses einem Vertragspartner übergibt, nimmt ein affirmatives Verhalten vor. Eine lediglich konkludente Einwilligung in Bezug auf die mit dem Kauf zusammenhängende Datenbearbeitung liegt vor, wenn auf dem Formular nur auf den Kauf Bezug genommen wird, auch wenn aus den Umständen (d.h. implizit) hervorgeht, dass der Vertragspartner zur Abwicklung die übergebenen Personendaten bearbeiten wird. Dies ist dementsprechend auch nicht als ausdrückliche, sondern konkludente Einwilligung in eine Datenbearbeitung zu werten.[34] Steht auf dem Formular hingegen (auch), dass die Daten für Marketingzwecke bearbeitet werden, so resultiert aus der Übergabe des Formulars – also der exakt derselben Handlung bzw. Form – eine ausdrückliche Einwilligung bezüglich der Marketingzwecke.[35] Entscheidend ist somit vereinfacht formuliert, ob die Datenbearbeitung, in welche eingewilligt werden soll, beim Namen genannt wird. Dieses Begriffsverständnis wird auch dem Schutzzweck, den das Erfordernis der Ausdrücklichkeit hat, optimal gerecht.

[Rz 34] Eine in der Praxis wichtige Detailfrage ist die Möglichkeit der Einwilligung durch Stillschweigen oder rein passives Verhalten. Hierzu halten die Erläuterungen fest, dass ein passives Verhalten nie eine ausdrückliche Einwilligung sein kann. Das ist nicht richtig. Es ist auch hier zu differenzieren: Stillschweigen ist normalerweise keine Zustimmung, sondern nur unter den Voraussetzungen von Art. 6 des Obligationenrechts (OR). Wenn jedoch zwei Parteien miteinander vereinbart haben, dass Stillschweigen als Zustimmung gilt, dann stellt ein Stillschweigen in der definierten Situation ein affirmatives Verhalten, mithin ein vereinbartes Zeichen der Zustimmung

---

32 So auch Alfred Koller, Schweizerisches Obligationenrecht Allgemeiner Teil, §3, Rn. 116. Vgl. auch Ernst Kramer/Bruno Schmidlin, in: Berner Kommentar, Arthur Meier-Hayoz (Hrsg.), Art. 1, Rn. 7.

33 Es wurde z.B. vereinbart, dass Stillschweigen Zustimmung bedeuten soll.

34 Aus diesem Grund trägt die Anpassung der Begrifflichkeiten von «explicite» zu «exprès» im Vorentwurf nicht zur Klärung bei; die Verwendung des Begriffspaars «explizit» und «implizit» wäre weiterhin richtig, sofern der Bezug stimmt. Die EU übersetzt den Begriff der «ausdrücklichen Einwilligung» in der DSGVO im Übrigen mit «explicit consent» (vgl. z.B. Art. 9 abs. 2 Bst. a DSGVO).

35 Nicht entscheidend ist, ob auf dem Formular nur steht, dass die Daten für Marketingzwecke verwendet werden oder ob eine Einwilligungserklärung umfassender formuliert wird («Durch Abgeben des Formulars stimme ich zu, dass meine Daten für Marketingzwecke bearbeitet werden») oder das Formular gar unterschrieben wird. Letzteres wäre nur dann erforderlich, wenn die Einwilligung auch eine schriftliche sein müsste, was das DSG und der Vorentwurf jedoch nicht verlangt.

dar und wird auch in der Literatur zum Obligationenrecht als ausdrückliche Willenserklärung anerkannt.[36] Dies ist vor allem in einem Anwendungsfall der Praxis von zentraler Bedeutung: Der Anpassung von AGB. Diese wird normalerweise mit einer Klausel bewerkstelligt, wonach dem Kunden zugestellte Anpassungen von AGB als genehmigt gelten, wenn er ihnen nicht innert Frist widerspricht. Es handelt sich um eine klassische stillschweigende Zustimmung (*deemed consent*), die durchaus wirksam ist. Beschreiben die AGB, wie die Daten des Kunden bearbeitet werden, und widerspricht der Kunde nicht, so liegt diesbezüglich eine ausdrückliche Zustimmung im Sinne von Art. 4 Abs. 6 VE DSG vor. Das Schweigen als Zeichen der Zustimmung ist vereinbart und damit hinreichend, und die Zustimmung bezieht sich direkt auf den Inhalt der AGB und damit auch auf die darin explizit erwähnte Datenbearbeitung. Ob diese Datenbearbeitung so ungewöhnlich ist, dass darauf besonders hingewiesen werden muss, ist eine weitere Frage, die aber nichts mit jener der Ausdrücklichkeit zu tun hat. Die Frage der Ausdrücklichkeit hat auch nichts direkt mit der Frage der Information zu tun, die für eine informierte Einwilligung erforderlich ist, da diese Information sich auch auf die Konsequenzen der Einwilligung bezieht und daher ohne Weiteres breiter sein kann als der Bedeutungsgehalt des zustimmenden Verhaltens. Diese einzelnen Aspekte sind sauber zu trennen, und es bleibt zu hoffen, dass die Botschaft zum revidierten DSG diesbezüglich klarer ausfällt.

[Rz 35] Sinnvollerweise verzichtet wurde im VE DSG auf eine besondere Regelung zum Rückzug von Einwilligungen und zum *Bundling* von solchen, wie es in Art. 7 Abs. 4 DSGVO diskutiert wird; vor allem letztere Regelung ist auch im EU-Recht unklar und umstritten, da ein Bundling von Einwilligungen nach Art. 7 Abs. 4 DSGVO zwar verpönt, aber nicht *per se* unzulässig sein soll. Im Schweizer Recht können schon heute Einwilligungen in die Datenbearbeitung in der Regel zurückgezogen werden, wobei dies nur für die Zukunft gilt und entsprechende vertragliche Konsequenzen nach sich ziehen kann, wie etwa ein ausserordentliches Kündigungsrecht des betroffenen Unternehmens. Auch eine Regelung, wonach Datenschutzeinwilligungen in AGB oder sonst in Verträgen von anderen Einwilligungen getrennt erfolgen müssen, findet sich im VE DSG sinnvollerweise nicht. Es wäre auch nicht einzusehen, warum für den Datenschutz andere Standards gelten sollen als für andere Regelungsbereiche wie die Haftung, Gewährleistung oder Geheimhaltungspflichten.

5. Auslandtransfer: Komplizierter und langwieriger, aber nicht schwerer

[Rz 36] Die Regeln zur Bekanntgabe ins Ausland verändern sich grundsätzlich nicht. Es soll im revidierten DSG in materieller Hinsicht nicht schwieriger werden Daten ins Ausland zu übermitteln. Aber es wird aufgrund neuer Notifikations- und Genehmigungspflichten komplizierter, mitunter viel langwieriger und vor allem drohen neu empfindliche Sanktionen bei Verstössen.

[Rz 37] Die Eigenverantwortung im Rahmen der Bekanntgabe ins Ausland wird ein gutes Stück abgeschafft: War es bisher so, dass jeder Datenexporteur selbst beurteilen musste, ob seine Daten im Ausland noch angemessen geschützt sind, kann er sich neu auf den Entscheid des Bundesrates verlassen. Hat dieser festgestellt, dass das Recht im Zielstaat einen angemessenen Datenschutz

36 Ingeborg Schwenzer, Schweizerisches Obligationenrecht Allgemeiner Teil, Rn. 27.11; Ernst Kramer/Bruno Schmidlin, in: Berner Kommentar, Arthur Meier-Hayoz (Hrsg.), Art. 1, Rn. 8; Claire Huguenin, Obligationenrecht Allgemeiner und Besonderer Teil, Rn. 173; Wilhelm Schönenberger/Peter Jäggi, Zürcher Kommentar, Art. 1–17 OR, Art. 1, Rn. 145.

gewährleistet, so steht dem Art. 5 Abs. 1 VE DSG offenbar nichts mehr entgegen. Der Vorentwurf muss so zu verstehen sein, dass der Export selbst dann zulässig ist, wenn der Datenexporteur zum Schluss kommen sollte, dass er die Persönlichkeit der betroffenen Person schwerwiegend gefährdet, weil die Bekanntgabe die betroffene Person zum Beispiel einer Strafverfolgung im Ausland aussetzt.[37] Ist dies nicht die Absicht, dann wäre dieser Punkt zu klären. Ist diese Folge beabsichtigt, so kann und sollte Abs. 1 als überflüssig und verwirrend gestrichen und (etwa in Abs. 2) festgehalten werden, dass Personendaten *nur* dann exportiert werden dürfen, wenn einer der Fälle von Art. 5 und 6 VE DSG erfüllt ist (Angemessenheitsentscheid, Garantien, Ausnahmen). Wer einwendet, dass selbst bei Einhaltung der Fälle von Art. 5 und 6 VE DSG Situationen entstehen können, in welchen ein Export die Persönlichkeit einer betroffenen Person verletzt, so sei darauf hingewiesen, dass solche Konstellationen entweder über die Bearbeitungsgrundsätze in Art. 4 VE DSG oder aber über Art. 23 Abs. 1 VE DSG «gelöst» werden können, wenn auch ohne entsprechendes Sanktionsrisiko.

[Rz 38] Liegt kein Angemessenheitsbeschluss vor, kann weiterhin auf Basis von Standardklauseln, wie sie heute die Regel sind, exportiert werden. Eine Genehmigung ist nach wie vor nicht erforderlich; es gilt weiterhin nur eine Pflicht zur Information des EDÖB betr. den Einsatz solcher Verträge oder vergleichbaren Vorkehren (Art. 5 Abs. 6 VE DSG). In der Verordnung wird sich zeigen, ob hierzu neu weitere Angaben zu den konkreten Datentransfers nötig sind (wie sie der EDÖB heute ohne Rechtsgrundlage verlangt und einen unverhältnismässigen Aufwand mit sich bringen kann) oder weiterhin eine pauschale Information mit einem allgemeinen Hinweis auf die Verwendung der Standardklauseln ausreicht, was vollauf genügt. Welchen Sinn eine solche Informationspflicht hat und was sie zum Datenschutz beiträgt, ist allerdings schon unter dem heutigen Recht unklar; die Schweiz sollte die Informationspflicht streichen, wie schon die EU im Rahmen der DSGVO.

[Rz 39] Vom Standard abweichende Verträge («spezifische Garantien») können bei entsprechender Notifikation weiterhin benutzt werden (Art. 5 Abs. 3 Bst. b VE DSG). Binding Corporate Rules («BCRs») oder zu Deutsch «verbindliche unternehmensinterne Datenschutzvorschriften» benötigen hingegen neu eine Genehmigung durch den EDÖB (Art. 5 Abs. 3 Bst. d VE DSG). Dies ist inkonsequent, weil BCRs letztlich eine Untergruppe der «spezifischen Garantien» von Bst. b sind,[38] für welche lediglich eine Informationspflicht vorgesehen ist. Worin der Unterschied zwischen Garantien nach Bst. b und d besteht, bedarf daher einer Klärung, sollte an der Unterscheidung festgehalten werden; sie erscheint jedoch wenig sinnvoll. Offenbar gingen die Verfasser des Vorentwurfs davon aus, dass es Datenexportverträge für den «Einzelfall» gibt[39] und solche, die von Unternehmen (und Behörden) für mehrere verschiedene Datenübermittelungen eingesetzt werden, während nur letztere der Genehmigung bedürfen (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d VE DSG). Die meisten nicht standardisierten Verträge werden in letztere Kategorie fallen.

[Rz 40] Die Frist zur Genehmigung ist mit einem halben Jahr allerdings enorm lange angesetzt; bisher musste die Prüfung selbst von BCR innert 30 Tagen durchgeführt sein. Das wird dazu

37 Die Erläuterungen VE DSG betonen jedenfalls für den Fall eines Angemessenheitsbeschlusses die Zulässigkeit des freien Datenverkehrs (S. 48).

38 Auch BCR werden regelmässig über (multilaterale) Verträge der einzelnen Gruppengesellschaften vereinbart. Sie kommen in der Regel dann zum Tragen, wenn nicht mit den Standardklauseln operiert werden soll (da in vielen EU-Ländern individuelle Verträge nur in Form von BCR möglich sind).

39 Erläuterungen VE DSG, S. 49, welche auf die Verwendung des Begriffs «im Einzelfall» Bezug nehmen, der sich jedoch nicht (mehr?) im VE DSG befindet.

führen, dass gerade nicht standardisierte Datenexportverträge in der Praxis völlig uninteressant werden, da kaum jemand ein halbes Jahr warten will, bevor er seinen Datentransfer durchführen kann. Hinzu kommt, dass die tatsächliche Frist sehr viel länger sein kann, da der EDÖB sich jederzeit auf den Standpunkt stellen kann, er habe noch nicht alle erforderlichen Informationen und die Frist von sechs Monaten somit von neuem zu laufen beginnt. Für BCRs ist immerhin vorgesehen, dass die Anerkennung durch eine andere Datenschutzbehörde auch für die Schweiz genügt, was insofern nicht sinnvoll ist, da BCR nur dann für die Schweiz genügen, wenn auch die Datentransfers *aus der Schweiz* erfasst sind. Dies wird bei der Prüfung durch eine ausländische Behörde nicht sichergestellt und muss in der Praxis erfahrungsgemäss immer wieder nachträglich angepasst werden, weil es vergessen ging.

[Rz 41] Als weitere Neuerung ist auch der Auftragsbearbeiter der Informations- bzw. Genehmigungspflicht unterworfen, nicht nur der Verantwortliche. Bisher hatte nur der Inhaber der Datensammlung eine Pflicht zur Notifikation. Die neue Regelung ist insbesondere in Konstellationen, in welchen der Verantwortliche in einem Land ohne angemessenen Datenschutz befindet, problematisch, so zum Beispiel Schweizer Cloud-Provider mit Kunden von ausserhalb Europas: Anerkannte Musterklauseln gibt es für diese Fälle nicht[40], und eigene Klauseln erfordern ein langwieriges Genehmigungsverfahren. Der Provider könnte sich zwar auf den Standpunkt stellen, dass vertragliche Garantien gar nicht erforderlich sind, weil mutmasslich die Einwilligung der betroffenen Personen für den Re-Export der Daten aus der Schweizer Cloud in das Land des Verantwortlichen vorliegt. Ob sich ein Provider angesichts der Strafsanktionen jedoch auf das Restrisiko einlassen wollen wird, ist eher fraglich. Diese Regelung sollte daher überdacht werden.[41]

[Rz 42] Die weiteren Rechtfertigungsgründe zur Übermittlung von Personendaten in Länder ohne angemessenen Datenschutz finden sich neu in einem separaten Artikel (Art. 6 VE DSG). Als wichtige Anpassung ist hier der Fall zu nennen, dass Unterlagen zwecks Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen ins Ausland übermittelt werden. Solche Transfers waren in ein Land ohne angemessenen Datenschutz wie etwa die USA bisher nur möglich im Zusammenhang mit Gerichtsverfahren, nicht jedoch Untersuchungen durch andere Behörden. Letztere sind neu ebenfalls abgedeckt; gestützt auf dem Sinn und Zweck der Erweiterung sollte der verwendete Begriff der «Verwaltungsbehörde» nicht nur Aufsichtsbehörden erfassen, sondern alle Behörden, vor welchen Verfahren zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen stattfinden können, also etwa eine Kartellbehörde, eine Steuerbehörde oder auch eine Behörde, die strafrechtliche Tatbestände untersucht und allenfalls sogar vergleichsweise regelt, wie dies etwa die *Criminal Division des US Departement of Justice* regelmässig tut. Unter heutigem Recht fallen diese Fälle zwischen Stuhl und Bank, was in weit über hundert Datenschutzprozessen vor Schweizer Gerichten im Zusammenhang mit dem US-Steuerstreit zur Blockierung von Datenlieferungen in die USA führte.[42] Diese Fälle waren denn auch der Anlass für die Erweiterung. Um Verwirrungen über die Frage zu vermeiden, was genau mit «Verwaltungsbehörden» gemeint ist,

40 Die *Controller-Processor-Clauses* der EU funktionieren nur in die umgekehrte Richtung.

41 Immerhin ist zu erwähnen, dass es im Falle von «*Processor-BCRs*» durchaus Konstellationen gibt, in welchen der Auftragsbearbeiter in die Pflicht genommen werden muss. Im heutigen Recht wird so verfahren, dass solche Regelungen durch Auftragsbearbeiter dem EDÖB zur Vorprüfung vorgelegt werden, dieser dann aber im konkreten Einzelfall jeweils nochmals prüft, ob sie hinreichend sind.

42 Vgl. etwa David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 594 ff.

empfiehlt es sich wie in der DSGVO[43] den Zusatz «vor einem Gericht oder einer Verwaltungsbehörde» zu streichen. Hierbei kann ferner die Wendung, dass die Bekanntgabe «unerlässlich» sein muss, an den Wortlaut der DSGVO angeglichen werden, die von «erforderlich» spricht. Zwar verwendet schon das bisherige Recht das Wort «unerlässlich». Es wird jedoch nicht wortwörtlich verstanden: Alles, was in einem entsprechenden Verfahren an Unterlagen Eingang finden soll oder von der Gegenpartei verlangt werden kann, ist damit erfasst.[44] Ebenso ist nicht nur die aktive Durchsetzung von Ansprüchen erfasst, sondern ebenso die Abwehr und Verteidigung gegen Rechtsansprüche. Damit der neue Wortlaut der Bestimmung überhaupt Sinn macht, ist der Begriff der «Rechtsansprüche» so zu verstehen, dass er auch straf- oder verwaltungsrechtliche Massnahmen umfasst. Dies wäre mindestens in der Botschaft klarzustellen.

[Rz 43] Gegenüber heutigem Recht nicht geändert, wurde die Ausnahmeregelung für Bekanntgaben im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags mit der betroffenen Person. Damit ist die Schweiz allerdings strenger als die DSGVO. Letztere erlaubt die Bekanntgabe auch dann, wenn ein Vertrag lediglich im Interesse der betroffenen Person abgeschlossen worden ist.[45] Diese Ergänzung wäre auch für das Schweizer Recht sinnvoll. Sie sollte aus Gründen der Konsistenz auch im Rahmen von Art. 24 Abs. 2 Bst. a VE DSG vorgenommen werden.

[Rz 44] Eine besonders heikle neue Bestimmung findet sich schliesslich in Art. 6 Abs. 2 VE DSG: Sie verlangt, dass Datenexporte in etlichen Konstellationen dem EDÖB gemeldet werden müssen, so auch in allen Fällen, in welchen der Export durch Vertragsabschluss oder -erfüllung oder ein ausländisches Rechtsverfahren gerechtfertigt wird. Dies wird nicht nur zu zahlreichen Meldungen führen, die der EDÖB gar nicht vernünftig oder innert nützlicher Frist bearbeiten können wird. Sie zwingt Unternehmen faktisch auch, dem EDÖB sensible Geschäftsgeheimnisse wie etwa laufende ausländische Untersuchungen und Gerichtsverfahren offenzulegen, wofür es keinen guten Grund gibt. Hierbei ist zu beachten, dass alle dem EDÖB gelieferten Unterlagen gemäss Öffentlichkeitsgesetz öffentlich einsehbar sind, einschliesslich Meldungen nach Art. 6 VE DSG. Geschäftsgeheimnisse sind zwar nach dem Buchstaben des Gesetzes vom EDÖB zu schützen, doch hat er diesen Schutz bisher sehr eng ausgelegt. Geschwärzt wird in der Praxis nur sehr wenig. Zur Meldung ist zudem nicht nur der Verantwortliche verpflichtet, sondern auch der Auftragsbearbeiter, obwohl er regelmässig nicht über die erforderlichen Angaben verfügen wird und nicht Herr der Daten ist. Es ist zu hoffen, dass diese Meldepflicht ersatzlos gestrichen wird.

6. Deutlich erweiterte Informations- und Auskunftspflichten

[Rz 45] Die Informationspflicht in Art. 13 VE DSG wird in der Praxis eine der materiell wichtigsten Neuerungen des revidierten DSG für private Datenbearbeiter sein. Sie sieht eine Informationspflicht im Rahmen jeder Datenbeschaffung vor, die deutlich weitergeht als das, was bisher erforderlich war. Sie ist wie der bisherige Art. 14 DSG kein Bearbeitungsgrundsatz, sondern eine öffentlich-rechtliche Norm, deren Verletzung nicht zwingend eine Persönlichkeitsverletzung zur Folge hat, dafür strafrechtlich sanktioniert wird. Anders als bisher erfasst die neue Infor-

43 Vgl. Art. 49 Abs. 1 Bst. e DSGVO.

44 David Rosenthal, Handkommentar DSG, Art. 6, N 66.

45 Art. 49 Abs. 1 Bst. c DSGVO.

mationspflicht jede Datenbeschaffung, d.h. es muss immer informiert werden. Der Katalog der Ausnahmen ist wesentlich enger als bei der generellen Transparenzpflicht nach Art. 4 VE DSG.

[Rz 46] Die Bestimmung ist in verschiedener Hinsicht problematisch. Zunächst ist unklar, über welche Dinge informiert werden muss. Art. 13 Abs. 2–4 VE DSG zählen zwar einige konkrete Angaben auf, doch muss die Information alles umfassen, was für eine betroffene Person erforderlich ist, um ihre Rechte nach DSG geltend zu machen. Gemäss den Erläuterungen soll die Beschränkung auf Mindestangaben eine flexible Handhabung der Informationspflicht erlauben und so zu viele Informationen verhindern. Da die Informationspflicht aber strafrechtlich massiv sanktioniert ist und sogar die fahrlässige Verletzung strafbar sein soll, werden Verantwortliche und Auftragsbearbeiter zur Risikominimierung wesentlich mehr Informationen liefern, als sie müssen, da sie sich auf ihre eigene Beurteilung, was an Informationen wirklich sinnvoll ist, nicht verlassen werden wollen.

[Rz 47] Es ist daher davon auszugehen, dass viele Schweizer Unternehmen sich an die umfassenderen Vorgaben der DSGVO halten werden.[46] In einem Punkt geht der VE DSG allerdings über die DSGVO hinaus: Nach Art. 13 Abs. 4 VE DSG muss auch über die Identität und Kontaktdaten der Auftragsbearbeiter informiert werden. Dies geht nach der hier vertretenen Auffassung viel zu weit und bringt betroffenen Personen in der Regel keinen Mehrwert. Hier sollte die Regelung darauf beschränkt werden, dass diese Information wenn überhaupt nur im Rahmen des Auskunftsrechts auf spezifische Nachfrage geliefert werden muss.[47] Über die DSGVO hinaus geht auch Art. 13 Abs. 5 VE DSG, der eine Information der betroffenen Person bei indirekter Datenbeschaffung spätestens bei Speicherung vorsieht; die DSGVO gewährt hier eine Frist von bis zu einem Monat.[48]

[Rz 48] Unklar im Rahmen der Bestimmung bleibt ferner, ob dann, wenn nachträglich neue Bearbeitungszwecke hinzukommen, «nachinformiert» werden muss; das dürfte (weiterhin) wohl nicht der Fall sein. Das gilt auch für die anderen Punkte, über die informiert werden muss. Es wird daher nur darüber informiert werden müssen, was schon zum Zeitpunkt der Beschaffung feststand; liegt eine laufende Beschaffung vor, genügt es, die Information für die künftig erfolgenden Beschaffungen anzupassen. Sollen bestehende Daten zu einem neuen Zweck bearbeitet werden, wird hierfür eine Einwilligung oder ein anderer Rechtfertigungsgrund erforderlich werden, soweit es kein mit dem ursprünglichen Zweck vereinbarer Zweck darstellt (dazu Rz 24 oben). Der Schutz der betroffenen Person wird so z.B. auch bei der Erweiterung der Kategorien der Empfänger sichergestellt. Etwas anderes wäre in letzter Konsequenz auch absurd, wenn pauschal nachinformiert werden müsste, wenn sich die Umstände, über die informiert wurde, geändert haben: Man stelle sich vor, ein Unternehmen ändert seine Kontaktadresse und müsste deswegen alle Personen, von denen es je Daten beschafft hat, darüber in Kenntnis setzen. Natürlich könnte argumentiert werden, dass dies nötig sei, damit diese Personen weiterhin wissen, wo sie ihre Rechte geltend machen können, aber eine solche Regelung würde jedes vernünftige Mass missen.

[Rz 49] Ohnehin ist absehbar, dass die Informationspflicht zu einer unnötigen, ja sogar kontraproduktiven Überinformation der betroffenen Personen führen wird, die kaum einen wirksamen Beitrag zur Verbesserung des Datenschutzes leisten wird. Die DSGVO geht punkto Informations-

46 Vgl. Art. 13 und 14 DSGVO.

47 Art. 20 VE DSG sieht die Information ebenfalls vor.

48 Art. 14 Abs. 3 Bst. a DSGVO.

pflicht zwar bezüglich der Elemente, über die informiert werden muss, noch weiter, doch wird dort inzwischen ebenfalls deutliche Kritik laut. Eine risikobasierte Transparenzpflicht, wie sie in Art. 4 DSG und VE DSG enthalten ist, genügt völlig.

[Rz 50] Eine im Vorfeld vorgeschlagene Lösung, wonach es genügen soll, dass ein Unternehmen statt einer Detailinformation bei jeder Datenbeschaffung mit einer Information auf seiner Website arbeiten kann, fehlt leider im Vorentwurf. Sie ermöglicht einen einigermassen sinnvollen Umgang mit der Informationsflut für jene, die diese Informationen tatsächlich erhalten möchten. Diese wenigen betroffenen Personen könnten sich dann auf den Webseiten der betreffenden Unternehmen im Detail darüber ins Bild setzen, wofür diese ihre Daten verwenden. Die Information am Beschaffungspunkt könnte auf die Identität und Information für weitergehende Informationen beschränkt werden; da der Zugang zu dieser Information gesichert wäre, wären auch die Vorgaben der Konvention 108 erfüllt. Die Lösung entspricht auch der heutigen Praxis des EDÖB. Es soll jedoch gemäss den Erläuterungen zum Vorentwurf gerade nicht genügen, wenn die betroffene Person nach der Information suchen oder fragen muss.[49] Dies dürfte bedeuten, das inskünftig überall, wo im Alltag Personendaten beschafft werden mit entsprechend langen (und entsprechend kleingedruckten) Informationstexten gerechnet werden muss, damit die Vorgaben von Art. 13 VE DSG der guten Form halber erfüllt sind. Wird die Norm ernst genommen, wird beispielsweise neben Sicherheitskameras in einem Gebäude jeweils ein Schild mit einem entsprechenden Informationstext befestigt werden müssen. Bisher genügte es, dass die Kameras sichtbar waren; alles andere ergab sich aus dem Zusammenhang, und wer mehr wissen wollte, konnte nachfragen und Auskunft erhalten.

[Rz 51] Der Katalog der Ausnahmen in Art. 14 VE DSG entspricht in Teilen der bisherigen Ausnahmeregelung von Art. 9 DSG, ist jedoch nach der hier vertretenen Auffassung zu eng und enger, als sie es gemäss der revidierten Konvention 108 sein müsste. So ist die Berufung auf überwiegende private Interessen nur dann möglich, wenn die Personendaten nicht an Dritte weitergegeben werden (Art. 14 Abs. 4 Bst. a VE DSG). Es ist dies eine schon im bisherigen Recht vorgesehene Einschränkung, für die es keine Berechtigung gibt. Entscheidend kann letztlich nur sein, ob das Interesse des Datenbearbeiters dem Interesse an der Information der betroffenen Person überwiegt. Tut es das im konkreten Fall, ist damit bereits gesagt, dass eine Information nicht mehr sinnvoll und auch nicht legitim ist. So werden sich Konzerne, die ihre Daten konzernintern nicht nur für die Zwecke der Auftragsbearbeitung teilen, bei der heutigen Regel nie auf überwiegendes eigenes Interesse berufen können, während es Unternehmen, die aus nur einer einzigen juristischen Person bestehen, können. Auch die Weitergabe an Behörden – zum Beispiel eine Aufsichtsbehörde – führt dazu, dass ein Unternehmen sich nicht mehr auf die Ausnahmebestimmung berufen kann, selbst wenn es ansonsten gute Gründe dafür gäbe. Es ist zu hoffen, dass der betreffende Zusatz gestrichen wird.[50]

[Rz 52] Es sollte zudem erwogen werden, die typischen Ausnahmefälle im Gesetz analog dem heutigen Art. 13 Abs. 2 DSG (bzw. Art. 24 VE DSG) klarzustellen, wobei dies für das Auskunftsrecht nach Art. 20 VE DSG (dazu sogleich) wichtiger ist als für die Pflicht zur Information nach Art. 13 VE DSG. So besteht zum Beispiel heute und unter dem Vorentwurf kein pauschales Recht, die Herausgabe der Kommunikation zwischen Unternehmen und Anwalt zu verweigern. Wäh-

49 Erläuterungen VE DSG, S. 56.

50 Gemeint ist: «und er die Personendaten nicht Dritten bekannt gibt».

rend ein Unternehmen dies in einem zivilrechtlich, strafrechtlichen und verwaltungsrechtlichen Verfahren ohne Weiteres kann, ist dies beim Auskunftsrecht nicht der Fall. Hier muss, soweit überhaupt zulässig, mit überwiegenden eigenen Interessen im Einzelfall argumentiert werden. Das erscheint stossend. Als weitere überwiegende private Interessen fallen gemäss heute herrschender Lehre und Praxis insbesondere in Betracht Daten zur internen Meinungsbildung[51], Sicherheitsinteressen (z.B. keine Mitteilung der Aufbewahrungsdauer von Daten zur Bekämpfung von Missbräuchen), die Lieferung von Unterlagen, die der Auskunftspflichtige schon hat (z.B. nutzen Bankkunden das Auskunftsrecht heute, um kostenlos Kontoauszüge nachzubestellen, die sie verloren haben, da Datenschutzgründe immer vorgeschoben werden können), zum Schutz von eigenen Geheimhaltungsinteressen (heute führt das Auskunftsrecht mitunter zur absurden Situation, dass einem Mitarbeiter zwar verboten werden kann, Geschäftsunterlagen mit nach Hause zu nehmen oder privat zu nutzen, sie ihm aber kostenlos in Kopie zur privaten Nutzung übergeben werden müssen, wenn er darin erwähnt wird und er sie unter Vorwand des Datenschutzes nach Art. 8 DSG herausverlangt, selbst wenn er das Unternehmen längst verlassen hat).

[Rz 53] Dass die Informationspflicht nach Art. 14 Abs. 2 Bst. b VE DSG auch entfällt, wenn die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist, ist bezüglich der Berufung auf überwiegende eigene Interessen keine Lösung: Die Ausnahme gilt nur, wenn die Informationen nicht bei der betroffenen Person direkt beschafft werden, und sie soll gemäss den Erläuterungen eng ausgelegt werden.[52] Werden beispielsweise für ein Gerichtsverfahren Beweismittel zusammengetragen, so wird künftig bei wortgetreuer Auslegung der Norm versucht werden müssen, alle darin erwähnten Personen[53] zu kontaktieren, um sie darüber zu informieren, dass die Unterlagen möglicherweise im Prozess eingereicht werden, auch wenn das Verfahren sie aller Voraussicht nach nicht tangiert. Eine Berufung auf überwiegende private Interessen ist aufgrund der Weitergabe an Dritte nicht möglich. Findige Köpfe werden argumentieren, es liege ein Fall von Art. 14 Abs. 2 Bst. a VE DSG vor, nämlich dass die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist, doch das gilt, wenn überhaupt, nur für Verfahren vor Schweizer Gerichten und zweitens nur für Dokumente, die als Beweismittel auch eingereicht werden. Auch Art. 14 Abs. 3 Bst. a VE DSG greift nicht, da diese Bestimmung nur dann den Verzicht auf die Information erlaubt, wenn ein Gesetz die Preisgabe der Information verbietet, wie z.B. der Bank mit Bezug auf vom Bankgeheimnis geschützte Daten. Schreibt das Gesetz die Bearbeitung von Daten lediglich vor, muss informiert werden; die Ausnahme von Art. 14 Abs. 2 Bst. a VE DSG greift nur, wenn die Daten über Dritte beschafft werden. Eine Bank müsste also genau genommen im Börsenhandel inskünftig jeden Händler, mit welchem sie zu tun hat, darüber informieren, dass die Telefonate aufgezeichnet und Daten über ihn aufbewahrt werden (mit allen Angaben gemäss Art. 13 VE DSG), weil die FINMA dies so verlangt, wobei sie dies nicht einmal in Form einer gesetzlichen Regelung, sondern im Rahmen ihrer «Rundschreiben» tut. Der Ausnahmekatalog von Art. 14 VE DSG sollte somit auch diesbezüglich erweitert werden, etwa indem in Abs. 1 auch jene Fälle erfasst werden, in denen sich die Datenbearbeitung aus Gesetz ergibt, in den betroffenen Verkehrskreisen als bekannt gilt oder sich aus den Umständen ergibt.

---

51 Vgl. Entscheid Bezirksgericht Zürich vom 2. Februar 2015, zitiert in: David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 600.

52 Erläuterung VE DSG, S. 58.

53 Z.B. Mitarbeiter anderer Unternehmen, die E-Mails gesandt, Verträge unterzeichnet haben oder sonst erwähnt sind.

Dies kann allenfalls durch eine Pflicht abgefedert werden, die Detailinformationen online oder auf Nachfrage bereitzustellen.

[Rz 54] Die Ausnahmen von Art. 14 VE DSG werden auch für das Auskunftsrecht von Relevanz sein, welches neu in Art. 20 VE DSG geregelt ist und bezüglich seiner Ausnahmen ebenfalls auf Art. 14 VE DSG verweist. Hier war erwartet – oder erhofft – worden, dass der Vorentwurf Massnahmen vorsieht, um dem grassierenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke Einhalt zu gebieten, was jedoch nicht geschah.[54]

[Rz 55] Stattdessen soll das Auskunftsrecht ausgebaut werden. Insbesondere sind weitere Informationen hinzugekommen, über die informiert werden muss, wie zum Beispiel die Aufbewahrungsdauer oder Kriterien zu ihrer Festlegung und die Identität und Kontaktdaten aller Auftragsbearbeiter. Weggefallen sind Angaben zu den Rechtsgrundlagen der Bearbeitung. Unter diesen Titel hatte das Zürcher Obergericht sogar die Herausgabe von Unterlagen angeordnet, welche keinerlei Personendaten der betroffenen Person enthielt – ein Fehlurteil.[55]

[Rz 56] In Art. 14 VE DSG fehlt auch ein Vorbehalt zugunsten von Datenbearbeitungen, welche gesetzlich vorgesehen sind.

[Rz 57] Gestrichen wurde immerhin die bisherige Regelung, wonach die Auskunft in der Regel schriftlich ist, in Form eines Ausdrucks oder einer Fotokopie zu erteilen ist. Sie muss aber kostenlos sein. Interessanterweise fehlt eine Norm, welche den Bundesrat ermächtigt, diese Punkte auf Verordnungsebene zu regeln, so namentlich Ausnahmen von der Kostenlosigkeit vorzusehen, wie dies die DSGVO tut.[56] Auch diese Aspekte des Auskunftsrechts hat in der Vergangenheit immer wieder zu Rechtsstreitigkeiten geführt, da das Auskunftsrecht von ehemaligen Mitarbeitern benutzt wurde, um für ihre Zwecke an Kopien ihrer eigenen Geschäftskorrespondenz und weiterer Geschäftsunterlagen, an denen sie beteiligt waren, zu gelangen. Da dem Bundesrat keine Kompetenz zur Definition von Ausnahmen von der Kostenlosigkeit eingeräumt werden soll, wird es nicht möglich sein, solche Fälle auf dem Verordnungsweg vorzusehen. Die Auskunft muss selbst bei querulatorischen, wiederholten und extrem aufwändigen Anfragen gratis sein, was stossend erscheint. Ein Auskunftsersuchen kann, wenn es eine etwas speziellere Materie betrifft, ohne Weiteres viele Tausend Franken kosten. Selbst beim Öffentlichkeitsgesetz (BGÖ) darf der Staat für seine Umtriebe Kostenersatz verlangen.

---

54 Lösungsansätze gibt es diverse. Sie reichen von der Beschränkung auf Fälle, in denen nachgewiesen werden kann, dass ein Auskunftsersuchen primär aus Datenschutzgründen erfolgt und nicht zum Zwecke der Beweisausforschung (Frage des Institutsmissbrauchs) über Kostenschranken bis hin zu einer Klarstellung, dass die Hürden zur Annahme eines Missbrauchs deutlich zu senken sind. Einer der erfolgversprechendsten Ansätze erscheint jedoch, das Auskunftsrecht inhaltlich nicht einzuschränken, es aber formal so auszugestalten, dass es für die Beweisausforschung nicht mehr interessant ist. Dies könnte zum Beispiel dadurch geschehen, dass der Auskunftspflichtige wählen kann, dass er die Daten nicht mehr in Kopie dem Auskunftsersuchenden übergibt, sondern stattdessen einer dritten Stelle, die entweder die Verletzung des Datenschutzes stellvertretend prüft (denn nur dazu dient das Auskunftsrecht), wie es der EDÖB heute in gewissen Fällen tut, oder bei welcher der Auskunftsersuchende die Daten einsehen kann, aber sie eben nicht mehr zweckentfremdet verwenden kann, z.B. als Beweismittel in einem nicht datenschutzrechtlich motivierten Forderungsprozess, was heute den Regelfall darstellt.

55 OGer vom 5. Dezember 2014 (LB140073-O3-1), E. 7; dazu David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 591 ff.

56 Art. 12 Abs. 5 Bst. a DSGVO.

7. Profiling und Einzelfallentscheide

[Rz 58] Auf den neuen Begriff des Profiling wurde bereits eingegangen. Demnach soll ein Profiling ohne ausdrückliche Einwilligung der betroffenen Person neu *per se* eine Persönlichkeitsverletzung darstellen. Dies ist gegenüber dem heutigen Recht eine deutliche Verschärfung, da bisher nur die *Weitergabe* von Persönlichkeitsprofilen eine Rechtfertigung erforderte. Die DSGVO kennt keine solche Regelung. Da dort jedoch jede Datenbearbeitung eine Rechtfertigung erfordert und im Falle besonders schützenswerter Personendaten eine ausdrückliche und eine solche auch im Falle eines automatisierten Profiling erforderlich ist, welches rechtliche oder in ähnlich erheblicher Weise auf eine Person wirkt, fällt die Regelung der DSGVO im Ergebnis nur etwas milder aus als die Schweizer Regelung.

[Rz 59] Neu findet sich im Vorentwurf auch eine Regelung zu automatisierten Einzelfallentscheiden. Eine solche Regelung war schon im Rahmen der letzten Revision des DSG diskutiert, dann aber wieder verworfen worden. In der EU sind solche schon heute eingeschränkt. Nun verlangt sie die revidierte Konvention 108. Im Kern geht es darum, dass bei automatisierten Einzelentscheiden, welche rechtliche oder erhebliche Auswirkungen auf eine Person haben, dieser Person ein Recht auf Anhörung durch einen Menschen gewährt wird. Dieser Anspruch auf «menschliches Gehör» findet sich neu in Art. 15 VE DSG. Die Anhörung kann vor oder nach dem Einzelentscheid stattfinden, und in dessen Rahmen verlangt das Schweizer Recht auch, dass die Person sich zu den über sie bearbeiteten Personendaten äussern können muss. Dies wiederum setzt sachlogisch eine Information über solche Entscheide voraus, die ebenfalls in Art. 15 VE DSG statuiert wird; unklar bleibt, wie allgemein die Information sein kann, was aber einen erheblichen Unterschied ausmachen kann.[57] Weiter stellt sich die Frage, ob nicht nur über die Tatsache eines automatisierten Entscheids informiert werden muss, sondern auch über die dazu bearbeiteten Personendaten, da sich die Person dazu ebenfalls äussern können muss; hier sollte darauf hingewiesen werden, dass diese Angaben nur auf Rückfrage zu liefern sind. Alles andere wäre uferlos. Da eine Person aber unabhängig von Art. 15 VE DSG die Möglichkeit hat, sich zu den über sie bearbeiteten Personendaten zu äussern, namentlich auch im Rahmen von Art. 4 Abs. 5 VE DSG, kann dieses Recht aus Art. 15 Abs. 2 VE DSG ohne Verlust gestrichen werden; die DSGVO sieht ein Recht zur Äusserung zu den bearbeiteten Daten in der Regelung zu automatisierten Einzelentscheiden auch nicht vor.[58]

[Rz 60] Aus dem Zusammenhang ergibt sich auch, dass der Entscheid zum Zeitpunkt der Anhörung nicht definitiv sein darf, auch wenn er von der «Maschine» schon gefällt worden ist. Es genügt also im Prinzip, bei automatisierten Einzelentscheiden eine Telefonnummer oder sonstige Kontaktmöglichkeit anzugeben, wo sich eine betroffene Person hinwenden kann, wenn sie sich zum Entscheid äussern möchte. Die Äusserung muss von einer Person zur Kenntnis genommen werden, welche bewirken kann, dass das Unternehmen auf seinen Entscheid zurückkommt; einfach nur entgegennehmen und ablegen wird nicht genügen (ähnliche Regelungen gibt es heute schon in anderen Bereichen, so z.B. Art. 333a Abs. 2 OR).

---

57 Eine allgemeine Klausel, wonach das Unternehmen auch automatisierte Einzelentscheide durchführt, wird allerdings nicht genügen. Es wird mindestens verlangt werden können, dass genügend Angaben geliefert werden, um automatisierte Entscheide als solche erkennen zu können. Die Schwierigkeit besteht allerdings nicht in den ohnehin der betroffenen Person kommunizierten Entscheiden, sondern jenen, die sowieso nicht kommuniziert werden (vgl. das nachfolgend erwähnte Schulbeispiel eines Viren- und E-Mail-Scanners, der jede Mail automatisiert daraufhin prüft, ob sie zugestellt wird; eine Mitteilung an den Absender erfolgt bestenfalls bei Nichtzustellung).

58 Art. 22 DSGVO.

[Rz 61] Anwendungsfälle sind gemäss Erläuterungen Situationen, in welchen ein Computer alleine darüber entscheidet, ob und zu welchen Konditionen ein Vertrag abgeschlossen wird oder Verkehrsbussen, die aufgrund einer Bildaufnahme automatisch verschickt werden.[59] Aber der Anwendungsbereich ist sehr viel breiter und umfasst etwa auch automatisierte Sicherheitskontrollen in Computernetzwerken wie z.B. im Falle von Spam- und Virenscannern, die E-Mails blockieren oder von den anderen separieren, Systeme zur Betrugsbekämpfung, welche z.B. Kreditkarten bei verdächtigen Transaktionen automatisch sperren und letztlich jeden etwas professionelleren Online-Shop, der automatisch Verträge abschliesst. In all diesen Fällen wird neu nicht nur über die Einzelentscheide informiert, sondern auch eine Möglichkeit zum Dialog mit einem Menschen vorgesehen werden müssen. Ausnahmen sieht Art. 15 VE DSG keine vor, die DSGVO hingegen lässt solche zu.[60] Weitere Beispiele sind Glücksspielsysteme, in welchem der Computer (sprich: Der Zufallsgenerator) über den Gewinn des Spielers entscheidet, selbstfahrende Autos oder automatische Börsenhandelssysteme. Sie sind zwar nur dann erfasst, wenn sie Personendaten bearbeiten, doch dies ist in allen drei Fällen ohne Weiteres denkbar.[61] Unklar wiederum ist, inwiefern auch automatisierte Abwicklungssysteme, wie etwa im Internet-Banking, erfasst sind. Ziel der Regelung sind sie sicher nicht, aber aufgrund der weitgefassten Definition und der Tatsache, dass heutzutage schon aus Gründen der Effizienz sehr viele Routineentscheide dem Computer übertragen werden, besteht das Risiko, dass sehr viele Fälle erfasst sind. Besonders hart wird dies die Bundesorgane treffen, da sie hierfür neu eine formelle Gesetzesgrundlage haben müssen (Art. 27 Abs. 2 VE DSG): Ohne eine Gesetzesanpassung wird ein Bundesorgan unter dem neuen DSG somit Computer selbst im Massengeschäft nicht mehr ohne Weiteres zur Effizienzsteigerung einsetzen können[62], was sicherlich nicht im Sinne des Erfinders wäre. Der Vorentwurf sieht solche Anpassungen nicht vor; viele der Anpassungen in anderen Gesetzen beschränken sich auf die Streichung der Erwähnung der Persönlichkeitsprofile.

[Rz 62] Die Erläuterungen zum Vorentwurf sprechen zwar davon, dass die Auswirkungen einer automatisierten Einzelentscheidung einen gewissen Schweregrad erreichen müssen, um erfasst zu sein.[63] Eine beliebige rechtliche Wirkung soll jedoch genügen. Wird in einer Online-Auktion automatisch darüber entschieden, wer den Zuschlag erhält, liegt eine rechtliche Wirkung vor und der Plattformbetreiber wird allen Mitbietern in diesem Fall die Möglichkeit geben müssen, sich zu äussern, auch wenn dies in der Sache völlig unsinnig ist. Noch absurder ist das Beispiel mit den Glückspielen: Sie müssten künftig konsequenterweise datenschutzrechtlich verboten werden, da sie immer rechtliche Wirkungen haben (der Computer entscheidet über die Pflicht zur Auszahlung von Gewinn), ausser der Spieler bleibt anonym oder es wird ihm die Möglichkeit gegeben, mit dem Betreiber darüber zu sprechen, warum er nicht gewonnen hat und warum das falsch ist.

---

59 Erläuterungen VE DSG, S. 59.

60 Art. 22 Abs. 2 Bst. b DSGVO.

61 Man denke an Online-Glückspiele oder Glückspiele, für welche sich eine Person anmelden muss, an selbstfahrende Autos, die über ihre Kameras Bilder von anderen Verkehrsteilnehmern machen, oder Handelssysteme, die es mit einem menschlichen Börsenteilnehmer als Gegenseite zu tun haben.

62 Ein Beispiel sind z.B. die heute bei Krankenkassen im obligatorischen Bereich eingeführten Systeme zur automatisierten Abrechnung.

63 Automatisierte Einzelfallentscheide gibt es überall im Alltag. Auch eine automatische, Badge-basierte Liftsteuerung kann z.B. eine solche sein. So entscheidet im Bürogebäude des Autors dieses Beitrags ein Computer alleine darüber, ob einem Mitarbeiter eine Liftkabine mit einer eingebauten Videokamera oder eine Liftkabine ohne zugeteilt wird, d.h. ob mehr oder weniger gewichtig in die Privatsphäre des Mitarbeiters eingegriffen wird.

[Rz 63] Fristen hierfür für die Anhörung der betroffenen Person sieht Art. 15 VE DSG allerdings keine vor, auch keine spezifische Form. Immerhin muss die Anhörung kostenlos sein.[64] Zu erwähnen ist, dass die Konvention 108 eine derart strenge Regelung nicht verlangt; auch hier geht die Schweiz weiter als nötig.

[Rz 64] Anders als in der DSGVO schaltet der Vorentwurf das Profiling den automatisierten Einzelentscheiden nicht gleich. In der DSGVO ist jedes automatisierte Profiling ein automatisierter Einzelentscheid und als solcher bei hinreichender Auswirkung geregelt; sonst gelten für das Profiling keine besonderen Bestimmungen. In der Schweiz schlägt der Vorentwurf eine breitere Regelung vor, indem auch «menschliches» bzw. manuelles und nicht nur ein maschinelles Profiling erfasst werden soll und daher eine Regelung unabhängig von automatisierten Einzelentscheiden erforderlich wurde. Ob das wirklich sinnvoll ist, ist eine andere Frage.

[Rz 65] Der Vorentwurf geht allerdings auch im Falle der automatisierten Einzelentscheide noch viel weiter als die DSGVO, indem in den Auskunftspflichten ein Verantwortlicher verpflichtet wird, bei *jedem* Entscheid, den er trifft und welchem die Bearbeitung von Personendaten zugrunde liegt, einer betroffenen Person Rechenschaft darüber abzulegen, wie und warum er so entschieden hat und welche Konsequenzen dies für die betroffene Person zusätzlich zu den Daten hat, die er hierzu verwendet hat. Diese Regel in Art. 20 Abs. 3 VE DSG gilt zwar insbesondere für automatisierte Einzelentscheide, aber ausdrücklich nicht nur. Eine solch breite Auskunftspflicht ist völlig überzogen und greift massiv in die Freiheiten der Unternehmen und betroffenen Privatpersonen ein. Stellt eine Person einer Firma eine Werbung für ein Angebot zu und entscheidet sich die Firma, diese Werbung in den Abfall zu werfen, so soll sie der Person für diesen Entscheid auf Nachfrage gemäss Vorentwurf rechenschaftspflichtig bleiben. Doch selbst wenn die Regel auf automatisierte Einzelentscheide beschränkt würde, wäre sie unsinnig: Diesfalls bliebe die Firma für ihren Viren- und Spamfilter rechenschaftspflichtig, um ein Beispiel zu nennen. Sinn macht eine Auskunftspflicht höchstens im Zusammenhang mit automatisierten Einzelentscheiden, die auch Anspruch auf «menschliches Gehör» gewähren, also gewisse Auswirkungen haben. So sieht es auch die DSGVO vor.[65]

[Rz 66] Es sollte zudem klargestellt werden, dass selbst in diesen Fällen nur dann Auskunft zu erteilen ist, wenn spezifisch nach den Zusatzdaten zu einem bestimmten Entscheid gefragt wird. Was nicht zugelassen werden sollte, wäre ein Ersuchen im Sinne von «gebt mir eine Liste aller automatisierten Einzelentscheide, die Ihr in Eurem Unternehmen trefft». Dies würde massiv in die Privatsphäre der Unternehmen eingreifen und dient primär der Ausforschung oder Schikane. Da die betroffene Person im Falle eines automatisierten Einzelentscheids ohnehin konkret auf diesen hingewiesen werden muss, genügt es, die Auskünfte nach Art. 20 Abs. 3 VE DSG auch nur in den Fällen zu gestatten, wo die betroffene Person diesem automatisierten Einzelentscheid unterworfen ist. Da sie ein Anhörungsrecht hat, genügt es, wenn sie die Auskunft vor ihrer konkreten Stellungnahme zum Entscheid erhält; eine Anfrage «auf Vorrat» ist somit nicht nötig.

64 Erläuterungen VE DSG, S. 60.

65 Art. 15 Abs. 1 Bst. h DSGVO.

8. Recht auf Vergessen, Widerspruchsrecht, Weitermeldepflicht

[Rz 67] Trotz erheblicher öffentlicher Diskussionen im Vorfeld der Vorlage[66] soll sich gemäss Vorentwurf am «Recht auf Vergessen» nichts ändern. Das ist völlig richtig so, denn das Schweizer Recht kennt schon heute eine umfassende und ausgewogene Regelung, die einer betroffenen Person erlaubt, sich gegen eine Datenbearbeitung in welcher Weise auch immer auszusprechen. Sie war bisher in Art. 12 DSG enthalten und findet sich nun unverändert in Art. 23 Abs. 2 Bst. b VE DSG.

[Rz 68] Der zivilrechtliche Rechtsschutz ist neu in Art. 25 VE DSG geregelt und entspricht ebenfalls dem heutigen Konzept; wer gegen eine Datenbearbeitung vorgehen will, kann dies vom Zivilgericht verlangen. Das gilt auch für das Recht, eine Berichtigung von Personendaten zu verlangen (bisher Art. 5 DSG, neu Art. 4 Abs. 5 DSG und Art. 25 DSG). Den «Bestreitungsvermerk» gibt es weiterhin. Es wird jetzt aber auch festgehalten, dass die bestrittenen Daten nur noch eingeschränkt bearbeitet werden, was schon bisher möglich war, auch wenn dies nicht ausdrücklich im Gesetz vorgesehen war. Es wird in diesen Fällen eine Interessenabwägung stattfinden müssen; rechtlich handelt es sich um einen Anwendungsfall des Widerspruchs gegen eine Datenbearbeitung, der nur mit einer entsprechenden Rechtfertigung (nach Art. 13 DSG bzw. Art. 24 VE DSG) wie etwa einem überwiegenden privaten Interesse «übergangen» werden kann.

[Rz 69] Neu ist hingegen die Regelung, wonach im Falle einer Berichtigung, Löschung oder Vernichtung von Daten und in weiteren Fällen der Verantwortliche und Auftragsbearbeiter die Dritten, denen sie zuvor die betroffenen Daten zugänglich gemacht haben, diese Berichtungen etc. mitteilen müssen, soweit dies nicht oder nur mit «unverhältnismässigem» Aufwand möglich ist (Art. 19 Bst. b VE DSG). Eine Begrenzung auf Fälle, in denen die betroffene Person ein schützenswertes Interesse hat, fehlt hingegen leider. Es ist nicht einmal erforderlich, dass die Berichtigung, Löschung oder Vernichtung auf einen Vorstoss der betroffenen Person zurückzuführen ist. Das kann zu absurden Verhältnissen führen, denn es gibt viele Gründe, warum Daten berichtigt, gelöscht oder vernichtet werden, ohne dass sich eine Nachinformation bisheriger Empfänger der Daten aufdrängt. Letztere benutzen die Daten möglicherweise gar nicht mehr. Oder eine Löschung erfolgt nicht, weil die Daten datenschutzwidrig bearbeitet wurden oder die betroffene Person dies verlangt hat, sondern weil sie der Inhaber selbst schlicht nicht mehr braucht. Das darf nicht eine Pflicht nach Art. 19 Bst. b VE DSG auslösen, sonst müsste jedes Unternehmen, das seine Archive und dergleichen bereinigt laufend prüfen, wem es die Daten schon einmal mitgeteilt hat und diese darüber informieren. Weil das schon ist im Ansatz unsinnig ist, kann es nicht sein, dass die Nachinformation lediglich wegen dem damit allenfalls verbundenen unverhältnismässigen Aufwand wegfällt. Art. 19 Bst. b VE DSG könnte zum Beispiel so eingeschränkt werden, dass sie nur zum Tragen kommen, wenn eine Person die Nachinformation aus berechtigten Gründen verlangt.

[Rz 70] Die DSGVO kennt eine ähnliche Regelung wie Art. 19 Bst. b VE DSG, doch geht der Vorentwurf auch bezüglich der mitzuteilenden Daten darüber hinaus,[67] als dass auch Verletzungen des Datenschutzes den Empfängern der davon betroffenen Daten mitgeteilt und somit offengelegt werden müssen. Das gilt paradoxerweise selbst dann, wenn die betroffenen Personen selbst darüber nicht informiert werden müssen. Aus der Regel geht auch nicht hervor, ob nur die melde-

66 Vgl. auch Postulat Schwaab 12.3152 und Erläuterungen VE DSG, S. 37.

67 Art. 19 DSGVO.

pflichtigen Datenschutzverletzungen gemeint sind, oder alle, wie es der Wortlaut suggeriert. So oder so ist nicht klar, welchen Sinn diese Pflicht haben soll. Sie ist überdies unverhältnismässig und greift ohne zwingenden Grund in die Privatsphäre der betroffenen Unternehmen ein.

[Rz 71] Man stelle sich zum Beispiel vor, dass in einem Unternehmen ein Mitarbeiter unbefugten Zugriff auf Daten nimmt, die das Unternehmen auch mit seinen Kunden teilt. Der Zugriff wird diesen als Datenschutzverletzung nach Art. 19 Bst. b VE DSG mitgeteilt werden müssen, obwohl er für diese Kunden ohne jede Relevanz ist, den Ruf der Firma aber schädigen wird. Ein anderes Beispiel wäre eine Zeitung, die im Zusammenhang mit der Berichterstattung über eine Person eine sie betreffende Datenschutzverletzung begeht. Nach der Regel von Art. 19 Bst. b VE DSG müsste die Zeitung diese Tatsache, sobald sie sie feststellt, allen Lesern des betroffenen Beitrags mitteilen, was technisch gesehen natürlich ohne Weiteres möglich ist. Tut sie dies nicht, können die betroffenen Mitarbeiter der Zeitung strafrechtlich verfolgt werden. Die Pflicht zur Mitteilung gilt zudem ungeachtet dessen, ob dies die betroffene Person oder andere Dritte in ihren Rechten verletzt.

9. Auch Daten verstorbener Personen geregelt

[Rz 72] Der Vorentwurf enthält mit Art. 12 VE DSG auch Bestimmungen zu Daten verstorbener Personen. Eine Regelung dieser Daten gibt es schon heute, allerdings ist sie erstens in Abs. 1 Abs. 7 VDSG versteckt und zweitens existiert für sie keine Rechtsgrundlage. Ohnehin gilt in der Schweiz der Grundsatz, dass die Persönlichkeit mit dem Tod endet[68], weshalb eine verstorbene Person auch keinen Datenschutz geniesst. Den Datenschutz geniessen allenfalls Personen im Umfeld der verstorbenen Person, die durch die Bearbeitung deren Daten ebenfalls betroffen sind. Die neue Regelung von Art. 12 VE DSG ist daher aus Sicht des Datenschutzes überflüssig. Dass es sie trotzdem gibt und ihr Regelungsgehalt über das bisherige Auskunftsrecht hinaus ausgebaut wird, ist die Folge einer politischen Intervention, welche Regelungen zum «digitalen Tod» in sozialen Medien verlangte.[69]

[Rz 73] Aus der Sicht der Praxis sind solche Zeitgeist-Regelungen unnötig und schädlich, da sie nur aufgrund eines sehr eng begrenzten, zum betreffenden Zeitpunkt gerade öffentlich diskutierten, aber meist nicht wirklich nachhaltig relevanten Anwendungsfalls hinaus verfasst werden. Problematisch sind solche Regelungen, weil sie aufgrund ihrer generell abstrakten Natur unzählige andere, nicht bedachte weitere Anwendungsfälle mitbetreffen und damit unkontrollierte und unüberlegte Nebenwirkungen haben. Das wird auch in diesem Fall so sein, da die Regelung keineswegs nur auf soziale Medien Anwendungen findet, sondern auf alle Unternehmen die Daten von natürlichen Personen bearbeiten.

[Rz 74] Verlangt ein einzelner Erbe, gleich in welcher Beziehung er zur verstorbenen Person steht, dass deren Daten gelöscht werden, soll sich das betroffene Unternehmen zum Beispiel nur auf überwiegende Interessen von Dritten oder der verstorbenen Person selbst berufen können, nicht aber etwa auf eigene überwiegende Interessen oder gesetzliche Pflichten, wie z.B. Aufbewahrungspflichten (Art. 12 Abs. 4 VE DSG). Damit hat der Erbe wesentlich mehr Rechte gegen einen Datenbearbeiter in der Hand als der Erblasser zu Lebzeiten, was keinen Sinn macht. Zudem bleibt

68 Art. 31 Abs. 1 ZGB.

69 Postulat Schwaab 14.3782 und Erläuterungen VE DSG, S. 38.

völlig im Dunkeln, ob und welche Interessen eine tote Person sachlogisch überhaupt haben kann. Konflikte unter den Erben regelt die Bestimmung ebenfalls in keiner Weise – sie sind naturgemäss vorprogrammiert. Interessant wird auch die Frage sein, wie der auskunftspflichtige Verantwortliche prüfen soll, ob eine Person eine faktische Lebensgemeinschaft mit der verstorbenen Person geführt hat.

[Rz 75] Durch die Universalsukzession der Vertragsverhältnisse mit den betreffenden sozialen Medien auf die Erbengemeinschaft und die weiteren Bestimmungen des anwendbaren Vertrags- und Erbrechts sowie der eigenen Persönlichkeitsrechte der Nachfahren wären die wesentlichen Rechtsfragen, die Sache des Gesetzgebers sind, hinreichend geklärt, oder dort zu klären und nicht im DSG. Erforderlich ist daher falls überhaupt nur eine moderate Bestimmung zum Auskunftsrecht; systematisch wäre es sinnvoller, sie mit der Revision des DSG ins ZGB aufzunehmen, wo sie hingehört, so zum Beispiel als neuen Art. 38^{bis} ZGB mit den Nachwirkungen der Ende der Persönlichkeit.

10. Massnahmen zur Sicherstellung des Datenschutzes

[Rz 76] Etliche der Bestimmungen des Vorentwurfs konkretisieren technische und organisatorische Massnahmen, die heute unter Art. 7 Abs. 1 DSG subsumiert werden könnten. Sie dienen der Gewährleistung des Datenschutzes, indem sie direkt oder indirekt auf die Einhaltung der Regelungen hinwirken.

[Rz 77] Die meisten dieser Bestimmungen wurden ins Gesetz genommen, um ein Zeichen zu setzen. Sie sind rechtlich an sich überflüssig, ergeben sie sich doch bereits aus einer korrekten Anwendung des Bearbeitungsgrundsatzes, wonach im Rahmen einer Datenbearbeitung jeweils angemessene (sprich: dem Risiko entsprechende) technische und organisatorische Massnahmen zu treffen sind, um eine unbefugte (sprich: DSG-widrige) Datenbearbeitung zu verhindern.

[Rz 78] Dieser Grundsatz findet sich in Art. 11 VE DSG. Neu wird hierbei der (ungewollte) «Verlust» von Daten als Unterform der unbefugten Bearbeitung im Einklang mit der Praxis der EU gesondert aufgezählt; erfasst war er schon bisher. Es wird allerdings nicht nur dem Bundesrat überlassen, diesen Grundsatz zu konkretisieren. Art. 18 Abs. 1 VE DSG tut dies unter dem Titel «Datenschutz durch Technik» (neudeutsch: «*Privacy by Design*»), wobei im Grunde dasselbe gesagt wird wie in Art. 11 Abs. 1 VE DSG, mit dem einzigen Hinweis, dass die Massnahmen bereits ab dem Zeitpunkt der Planung der Datenbearbeitung zu treffen sind, was aber so oder so gilt, wenn solche Massnahmen im Rahmen einer Datenbearbeitung von Anfang an bestehen müssen.

[Rz 79] Art. 18 Abs. 2 VE DSG schreibt den Grundsatz «datenschutzfreundlicher Voreinstellungen» («*Privacy by Default*») vor, welcher vor allem Anbieter von Online-Diensten und -Apps zwingen soll, die Grundeinstellungen ihrer Dienste so zu programmieren, dass von den im Rahmen eines Dienstes angebotene Datenbearbeitungen standardmässig die am wenigsten weitgehende vorgesehen ist. Die Formulierung im Vorentwurf bringt dies nicht wirklich zum Ausdruck und ist sachlogisch unkorrekt, da es nicht um die Frage geht, ob mehr Daten als für einen bestimmten Verwendungszweck erforderlich bearbeitet werden sollen, sondern zu welchem Verwendungszweck die Daten standardmässig vorgesehen werden soll. Hier ist somit eine Überarbeitung der Formulierung nötig. Ohnehin wäre es aufgrund der Nähe zu Art. 11 VE DSG sinnvoll, die beiden Grundsätze in den Wortlaut von Art. 11 Abs. 1 VE DSG zu integrieren, was mit wenigen Worten möglich wäre.

[Rz 80] Dies gilt im Übrigen auch für die in Art. 19 Bst. a VE DSG aufgeführte Pflicht zur Dokumentation der Datenbearbeitungen, die einerseits eine organisatorische Massnahme im Sinne von Art. 11 VE DSG darstellt und andererseits der Datenschutzaufsicht dient. Unternehmen werden hier gespannt auf die Konkretisierung im Rahmen der Verordnung sein, da je nach Ausgestaltung der Dokumentationspflicht ein erheblicher Aufwand auf sie zukommt. Sinnvoll wäre eine Regelung, die jedenfalls nicht über das von Art. 30 DSGVO vorgeschriebene Verzeichnis der Datenbearbeitungen hinausgeht, und eine Klarstellung, dass nur *regelmässige* Datenbearbeitungen in ein solches Inventar aufgenommen werden müssen, analog der heutigen Regelung von Art. 11a Abs. 3 DSG. Hinzu kommt, dass die meisten Unternehmen auch für die DSGVO nur *strukturierte* Datenbestände bzw. Datenbearbeitungen erfassen werden; eine solche Einschränkung erscheint aus Sicht der Praktikabilität und Möglichkeiten der Governance ebenfalls sinnvoll. Wird die Dokumentationspflicht zu breit oder absolut verstanden, muss jedes Schreiben einer E-Mail oder eines Briefs dokumentiert sein, weil sie jeweils eine Datenbearbeitung darstellen. Das wäre unsinnig. Es stellt sich vor diesem Hintergrund zudem die Frage, ob der gestrichene Begriff der Datensammlung nicht doch weiterhin benutzt werden sollte, um bezüglich gewisser Pflichten unter dem neuen DSG eine sinnvolle Beschränkung zu ermöglichen. Schliesslich wäre zu klären, dass mit Bezug auf die Dokumentation das Rad nicht neu erfunden werden muss und die Bestimmung keine eigenständige Dokumentation für Datenschutzzwecke erfordert, sondern es genügt, dass zum Beispiel auf bestehende Dokumentationen zurückgegriffen werden kann (z.B. ein Betriebshandbuch eines Systems) oder sich die Dokumentation sogar aus dem System selbst ergibt.

[Rz 81] Die in Art. 19 Bst. a VE DSG erwähnte Pflicht soll gemäss den Erläuterungen die Datenbearbeiter auch verpflichten, die Datenschutzverstösse im Sinne von Art. 17 VE DSG zu dokumentieren[70]. Hier kann auf die nachfolgenden Ausführungen zu diesem Thema verwiesen werden (vgl. Rz 93 ff. unten). Angesichts dem breiten Begriffsverständnis von Art. 17 VE DSG erscheint auch diese Dokumentation uferlos und ohne sichtbaren Mehrwert für den Datenschutz; hierbei ist zu beachten, dass diese Pflicht für jedes Unternehmen gilt, sei es noch so klein. Die DSGVO sieht eine solche Dokumentationspflicht zwar auch vor, geht aber von einem sehr viel engeren Verständnis der zu erfassenden Verstösse aus.

[Rz 82] Erstaunlicherweise keinen Eingang in die Vorlage gefunden haben Bestimmungen zum betrieblichen Datenschutzbeauftragten. Richtigerweise wird ein solcher nicht vorgeschrieben. Das war schon bisher nicht der Fall, und auch die DSGVO schreibt ihn für die meisten Betriebe nicht vor. Die Funktion des betrieblichen Datenschutzbeauftragten wäre aber ideal, um den EDÖB in gewissen Bereichen zu entlasten, wenn sichergestellt ist, dass eine solche Stelle über die nötigen Kompetenzen und das nötige Know-how verfügt. Es könnte zum Beispiel analog der bisherigen Regelung in Art. 11a DSG vorgesehen sein, dass die diversen Informations- und Meldepflichten wegfallen, soweit sie überhaupt beibehalten werden sollen, wenn ein Unternehmen selbst über eine solche Stelle verfügt; dies wäre ein erheblicher Anreiz zur Schaffung einer solchen Stelle, was wiederum der Datenschutz-Governance zugutekäme.

70 Erläuterungen VE DSG, S. 65.

11. Datenschutz-Folgenabschätzungen

[Rz 83] Ein neues Instrument zur Sicherstellung des Datenschutzes sind die «Datenschutz-Folgenabschätzungen» (*Privacy Impact Assessments*), welche Art. 16 VE DSG neu in allen Fällen vorschreibt, in welchen eine vorgesehene Datenbearbeitung «voraussichtlich zu einem erhöhten Risiko» für die Persönlichkeit der betroffenen Personen vorsieht. Eine solche Abklärung muss nicht zwingend umfangreich sein, wie die Erfahrung zeigt. Es geht im Wesentlichen darum, zunächst zu dokumentieren, wie die Datenbearbeitung vor sich gehen soll, was dabei schiefgehen bzw. negative Auswirkungen auf die betroffene Person haben kann, und welche Massnahmen zu ihrem Schutz vorgesehen sind, um diese Risiken und Auswirkungen auszugleichen (Abs. 2). Das mag auf einer Seite Platz finden. Das Ergebnis ist dem EDÖB mitzuteilen (Abs. 3), der dann etwaige Einwände innert einer Frist von drei Monaten nach Erhalt aller erforderlichen Informationen anmelden muss (Abs. 4).

[Rz 84] Auch die DSGVO schreibt solche Datenschutz-Folgenabschätzungen vor, und selbst im heutigen Schweizer Recht gibt es sie in den Kantonen teilweise schon[71]. Allerdings ist die im Vorentwurf vorgeschlagene Regelung in verschiedener Hinsicht problematisch. Erstens erscheint die Hürde für die Durchführung einer Abklärung sehr tief angesetzt. «Erhöhte» Risiken werden in der Praxis rasch gegeben sein, womit für fast alle Datenbearbeitungen vorab entsprechende Abklärungen durchgeführt werden müssen, mit den damit verbundenen Aufwänden und massiven Verzögerungen (dazu sogleich). Diesbezüglich beruhigen auch die Erläuterungen nicht, soll es doch schon genügen, dass die Verfügungsfreiheit der betroffenen Person über ihre Daten erheblich eingeschränkt wird oder werden kann[72], was in sehr vielen Fällen der Fall sein wird. Die Bearbeitung von besonders schützenswerten Personendaten oder ein Profiling soll bereits Indiz für ein «erhöhtes» Risiko sein, ebenso die Übermittlung in Drittstaaten ohne angemessenen Datenschutz. Die Strafbewehrung der Bestimmung wird ein ihres dazu beitragen, dass selbst in Fällen, in denen an sich kein erhöhtes Risiko besteht, aus Angst vor Strafbarkeit ein entsprechendes Verfahren durchgeführt wird, inklusive Meldung an den EDÖB. So wäre es bei der jetzigen Ausgangslage nicht erstaunlich, wenn inskünftig jede Übermittlung in die USA, jedes Profiling und jede Bearbeitung von besonders schützenswerten Personendaten zu einer Datenschutz-Folgenabschätzung führt, was völlig übertrieben wäre. Der dafür erforderliche Aufwand für die Wirtschaft (und den EDÖB) wäre enorm, ohne dass für den Datenschutz wirklich etwas gewonnen wäre.

[Rz 85] Die EU verlangt im Gegensatz dazu entsprechende Abklärungen nur bei «hohen» Risiken. Hierbei ist zu berücksichtigen, dass ohnehin jedes Bearbeitungsprojekt geprüft werden muss, denn nur dadurch kann überhaupt ermittelt werden, ob es voraussichtlich zu erhöhten oder hohen Risiken führt. Wesentlich ist, dass die gesetzliche Pflicht zur Erstellung einer formalen, dokumentierten Abklärung auf das beschränkt wird, was wirklich zwingend nötig ist. Die Fälle, in welchen Unternehmen solche formalisierten Abklärungen tatsächlich vornehmen sollen, sollten zudem im Rahmen der Verordnung konkretisiert werden. Eine Ausnahme bietet sich zudem für Fälle an, in welchen das Gesetz ein Unternehmen die Datenbearbeitung vorgibt, auch wenn die konkrete Ausgestaltung natürlich Risiken mit sich bringen kann, die adressiert werden müssen. Solche Fälle sind jedoch nicht im Fokus von Art. 16 VE DSG; die damit verbundenen

71 Vgl. etwa die Vorabkontrolle gemäss § 10 des ZH-IDG, die erforderlich ist, wenn eine Datenbearbeitung «besondere Risiken» mit sich bringt.

72 Erläuterungen VE DSG, S. 61.

fallspezifischen Risiken müssen im Rahmen der jeweiligen Gesetzesvorgaben abgewogen werden und, soweit ein Unternehmen nur die gesetzlichen Vorgaben umsetzt, wird die Datenbearbeitung in der Regel in materieller Hinsicht datenschutzkonform nach Art. 24 Abs. 1 VE DSG gerechtfertigt sein.

[Rz 86] Unpassend erscheint weiter, dass der Vorentwurf die Pflicht zur Abklärung nicht nur dem Verantwortlichen auferlegt, wie dies die DSGVO tut, sondern auch dem Auftragsbearbeiter, obwohl dieser dazu regelmässig nicht in der Lage sein wird und es auch nicht seine Aufgabe ist. Natürlich kann der Verantwortliche eine solche Abklärung an seinen Auftragsbearbeiter delegieren, aber es bleibt schon von der Natur der Sache her eine Pflicht des Verantwortlichen.

[Rz 87] Die Meldepflicht gegenüber dem EDÖB und die ihm eingeräumte Frist zur Bearbeitung ist schliesslich praxisfern und wird die Datenbearbeiter massiv behindern. Ein grosses Pharmaunternehmen aus Basel führt beispielsweise jedes Jahr weit über hundert solche Datenschutz-Folgeabschätzungen durch. Würden sie vom EDÖB ernsthaft geprüft, müsste er alleine für dieses Unternehmen eine eigene Person abstellen. Das wird er nicht und das kann auch nicht sinnvoll sein. Selbst die DSGVO ist weniger streng: Sie verlangt eine Konsultation der Aufsichtsbehörde nur dann, wenn der Verantwortliche zum Schluss kommt, dass trotz der von ihm ergriffenen Schutzmassnahmen ein hohes Risiko der Verletzung der Persönlichkeit der betroffenen Personen verbleibt.[73]

[Rz 88] Die dem EDÖB gewährte Frist zur Beurteilung ist überdies viel zu lange: In der EU muss eine Behörde innert acht Wochen handeln, falls sie sich gegen eine Bearbeitung ausspricht, und die Frist kann nur in komplexen Fällen um sechs Wochen verlängert werden.[74] In der Schweiz soll der EDÖB standardmässig drei Monate Zeit haben, mit der Möglichkeit, durch das Einfordern weiterer Information die Frist jedes Mal von neuem beginnen zu lassen.

[Rz 89] Wird der vorgeschlagene Art. 16 VE DSG tatsächlich so umgesetzt, bedeutet dies für Unternehmen, dass sie bei jedem Projekt, das eine Datenbearbeitung beinhaltet und diese nicht problemlos erscheint, einen Vorlauf von vielen Monaten einplanen müssen, um nach ihrer eigenen Abklärung auch etwaigen Anforderungen des EDÖB gerecht zu werden. Dies wird die Wirtschaft völlig unnötig lähmen und erhebliche Kosten verschlingen. Mag eine Wartezeit in gewissen Projekten noch handhabbar sein, wird sie in anderen Fällen zu erheblichen Schwierigkeiten führen. Man stelle sich zum Beispiel ein ausländisches Gerichtsverfahren oder eine Anfrage einer ausländischen Aufsichtsbehörde vor, für welches bzw. für welche innert Wochen gewisse Unterlagen geliefert werden müssen, die auch Angaben von Mitarbeitern enthalten. Nach der vorgeschlagenen Regelung wäre dies nicht mehr oder nicht sinnvoll möglich. Solche Fälle werden fast immer erhöhte Risiken mit sich bringen, müssten also dem EDÖB vorgelegt werden. Ebenso wird es aber nicht möglich sein, die Monate, die er zur Klärung der möglichen Massnahmen braucht, abzuwarten. Das Unternehmen wird sich entscheiden müssen, dem ausländischen Recht zu folgen und möglicherweise Schweizer Recht zu verletzen bzw. die Konsultation des EDÖB nutzlos werden zu lassen, oder umgekehrt. Dabei sieht die Regelung keine Ausnahmen vor, und dies nicht einmal für den Fall, in welchem alle betroffenen Personen mit der Datenbearbeitung einverstanden sind.

[Rz 90] Auch für den EDÖB wird diese Regelung im Ergebnis nicht angenehm werden. Wird ihm ein Projekt vorgelegt, wird er sich damit zwangsläufig auseinandersetzen müssen, denn tut er es

73 Art. 36 Abs. 1 DSGVO.

74 Art. 36 Abs. 2 DSGVO.

nicht und stellt sich das Projekt später als datenschutzrechtlich problematisch heraus, wird er dafür möglicherweise nicht rechtlich, aber öffentlich und politisch zur Verantwortung gezogen werden, weil er nicht rechtzeitig interveniert hat bzw. keine Einwände äusserte. Dies wird daher auch seinerseits erhebliche Ressourcen binden, über die er aber nicht verfügt bzw. die an anderer Stelle eingespart werden müssen. Sinnvoller wäre, dieses Konsultationsverfahren auf die wirklich heiklen Fälle zu beschränken.

[Rz 91] Zu klären ist weiter die Frage, unter welchen Umständen Datenschutz-Folgenabschätzungen im Rahmen von bestehenden Datenbearbeitungen vorzunehmen bzw. zu wiederholen oder aufzufrischen sind, falls überhaupt. Denn Risiken können sich verändern, die Umstände und Datenbearbeitungen ebenfalls. Der Wortlaut von Art. 16 VE DSG ist diesbezüglich nicht klar, impliziert aber aufgrund von Abs. 1 und 4, dass eine *formalisierte* Abklärung nur jeweils bei der Erstaufnahme einer Datenbearbeitung durchzuführen ist. Dies wäre in der Botschaft in diesem Sinne klarzustellen.

[Rz 92] Im Zusammenhang mit Art. 16 VE DSG sei noch erwähnt, dass diese auf ein Risiko «für die Persönlichkeit oder die Grundrechte» der betroffenen Personen abstellt. Diese Formulierung ist verwirrend. Zwar dient das DSG schon bisher gemäss Art. 1 nicht nur dem Schutz der Persönlichkeit, sondern auch den Grundrechten der betroffenen Personen, doch gilt letzteres nur mit Bezug auf die Datenbearbeitungen durch Behörden im engeren Sinn. Private sind normalerweise nicht zur Wahrung der Grundrechte verpflichtet; in ihrem Bereich dient das DSG – und damit die Datenschutz-Folgenabschätzung – ausschliesslich dem Schutz der Persönlichkeit der betroffenen Personen. Der Verweis auf die «Grundrechte» sollte daher sinnvollerweise überall gestrichen werden. Er hat keinen Mehrwert.

12. Data Breach Notifications

[Rz 93] Was ursprünglich in den USA erfunden wurde, soll es nun auch in der Schweiz geben: *Data Breach Notifications*. Es geht um die Meldung von Datenschutzverstössen, einschliesslich Datenverlust. Eine solche Pflicht bestand bisher nicht, jedenfalls nicht in formalisierter Form. Schon nach heutigem Recht kann es erforderlich sein, im Falle einer Datenschutzverletzung gewisse Sofortmassnahmen wie etwa die Sperrung von abhanden gekommenen Kreditkartendaten auszuführen. Auch die Mitteilung an den EDÖB kann in bestimmten Fällen ratsam sein. Neu soll jedoch *jeder* Datenschutzverstoss dem EDÖB «unverzüglich» gemeldet werden, es sei denn, dieser führe «voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person» (Art. 17 Abs. 1 VE DSG).

[Rz 94] Diese Bestimmung ist insofern bemerkenswert, als sie deutlich über die entsprechende Bestimmung der DSGVO hinausgeht, und zwar ohne ersichtlichen Grund. In der EU wird eine Meldung dann erforderlich sein, wenn im Rahmen einer Datenbearbeitung festgestellt wird, dass eine getroffene Sicherheitsmassnahme verletzt wurde (z.B. ein Einbruch in ein Computernetz oder ein Mitarbeiter, der weisungswidrig Daten auf einen privaten Memorystick kopiert) und diese Verletzung zu einem Bruch oder Verlust des Gewahrsams an den Daten führt.

[Rz 95] In der Schweiz soll die Meldepflicht hingegen jede Datenbearbeitung erfassen, die gegen das DSG verstösst, also z.B. eine zweckentfremdete oder unverhältnismässige Nutzung von Daten oder eine Datenbeschaffung, die in nicht transparenter Weise erfolgt. Solche Fälle kommen in jedem Betrieb erfahrungsgemäss jeden Tag vor. Die Ausnahme, in welchem Fall nicht gemeldet

werden muss, ist dabei schon so formuliert, dass sie im Falle einer Datenschutzverletzung nicht gegeben sein kann, stellt doch eine unbefugte Datenbearbeitung immer eine Persönlichkeitsverletzung dar.

[Rz 96] Selbst wenn nur die etwas schwereren Fälle gemeldet werden müssen, wird die Schweizer Regelung ungleich viel mehr Fälle erfassen, als gemäss der DSGVO der Aufsichtsbehörde gemeldet werden müssen. Sachliche Gründe gibt es dafür nicht. Der logische Grund für die Meldepflicht ist das Bedürfnis, der Aufsichtsbehörde die Möglichkeit zu geben, in den Umgang mit einer Datenschutzverletzung aktiv einzugreifen und zum Beispiel die Benachrichtigung der betroffenen Personen zu verlangen (vgl. Abs. 2). Müsste aber tatsächlich wie vorgesehen gemeldet werden und halten sich die Betriebe auch daran, würde der EDÖB jeden Tag mit einer Vielzahl von Meldungen geflutet werden. Die Idee der Regelung wäre durch sie selbst vereitelt.

[Rz 97] Die im Vorentwurf vorgesehene Meldepflicht bringt aber auch die Mitarbeiter in einem Unternehmen in eine Zwickmühle und sorgt für völlig unverhältnismässigen Druck und letztlich eine Angstkultur: Stellt zum Beispiel der interne Datenschutzverantwortliche eine Datenschutzverletzung im eigenen Betrieb fest und könnte sie zu einem Risiko für die betroffenen Personen führen, muss er sie dem EDÖB melden und damit die dafür verantwortlichen Personen «ans Messer» liefern: Je nach Verstoss werden sie dafür strafrechtlich verfolgt werden müssen[75], da der EDÖB seinerseits eine Anzeigepflicht hat (dazu Rz 119 unten). Tut der Datenschutzverantwortliche dies nicht, muss er selbst mit strafrechtlicher Verfolgung rechnen (Art. 50 Abs. 2 Bst. e VE DSG). Dies wird für ihn, der darauf angewiesen ist, dass andere Mitarbeiter mit ihm offen über Datenschutzprobleme sprechen, eine unhaltbare Situation sein. Doch auch dort, wo der Datenschutzverantwortliche selbst für den Datenschutzverstoss (mit-)verantwortlich ist, sind Konflikte vorprogrammiert (Stichwort *nemo tenetur*, vgl. Rz 125 unten).

[Rz 98] Die Meldepflicht ist daher mindestens auf das Niveau der DSGVO zu reduzieren, und selbst diese geht weit. Auch die strafrechtlichen Sanktionen sind zu überdenken bzw. zu prüfen, inwiefern eine Meldung möglicherweise sogar vor Strafe schützt, um einen möglichst offenen Umgang mit solchen Meldungen zu fördern. Sinnvoll erscheint eine Regelung, in welcher zudem nur Fälle gemeldet werden müssen, die eine Vielzahl von Personen betreffen, da sich ein Eingreifen der Aufsichtsbehörde nur dann wirklich rechtfertigt. Versendet ein Spital zum Beispiel einen heiklen Befund versehentlich an den falschen Patienten, ist das zwar eine gewichtige Persönlichkeitsverletzung, aber weshalb es in einem solchen Fall zum Schutz des betroffenen Patienten nötig sein sollte, dass der EDÖB eingeschaltet wird, ist nicht ersichtlich. Eine Pflicht, die betroffene Person direkt zu informieren, wenn es zum Schutz der betroffenen Person erforderlich ist, ist in Abs. 2 bereits vorgesehen.[76]

[Rz 99] Die Meldepflicht sollte zudem in zeitlicher Hinsicht relativiert werden. Statt einer «unverzüglichen» Meldung sollte eine Meldung ohne unnötigen Verzug stattfinden. Denn zwischen dem Erkennen eines Verstosses und dem Zeitpunkt, an welchem genügend Informationen vorliegen, damit sich der EDÖB ein vernünftiges Bild machen kann, vergeht normalerweise einige Zeit. Es bringt gar nichts, dem EDÖB vorab eine Mitteilung machen zu müssen, dass ein Unternehmen

75 So zum Beispiel die Mitarbeiter der Informatik, welche es unterlassen haben, die zum Schutz der Daten notwendigen Massnahmen zu treffen, was bei vorsätzlicher und fahrlässiger Begehung strafbar sein soll (Art. 51 VE DSG).

76 Der zweite Fall («oder der Beauftragte es verlangt») ist irreführend formuliert und überflüssig. Ist es zum Schutz der betroffenen Person nicht erforderlich, gibt es auch keinen Grund, warum der EDÖB eine Information verlangen sollte.

einen Datenschutzverstoss entdeckt hat, aber noch nicht wirklich sagen kann, was passiert ist, warum und welche Massnahmen es trifft. Der EDÖB ist ohnehin in einer viel schlechteren Lage zu beurteilen, was an Massnahmen sinnvollerweise zu ergreifen ist als das betroffene Unternehmen.

[Rz 100] In Abs. 4 wird schliesslich dem Auftragsbearbeiter die Pflicht auferlegt, den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung zu informieren, wobei nicht klar wird, ob diese Pflicht nur Verstösse in seinem Verantwortungsbereich betrifft oder auch Verstösse, die der Auftragsbearbeiter seitens des Verantwortlichen wahrnimmt. Sachlogisch muss ersteres gelten. Anders als Abs. 1 sieht Abs. 4 allerdings keine Informationspflicht im Falle von Datenverlust vor. Korrekterweise ist der Hinweis auf den Datenverlust zu streichen, denn wenn ein Datenverlust nicht zugleich eine Datenschutzverletzung darstellt, gibt es in der Sache keinen Grund, diesen melden zu müssen.

13. Auftragsdatenbearbeitung

[Rz 101] Im Bereich der Auftragsdatenbearbeitung, die neu in Art. 7 VE DSG geregelt ist, soll sich mit drei Ausnahmen nicht viel ändern:

[Rz 102] Erstens wird nun ausdrücklich festgehalten, dass sich der Verantwortliche vergewissern muss, dass der Auftraggeber nicht nur in der Lage ist, die Datensicherheit zu gewährleisten, wie dies schon bisher ausdrücklich verlangt wurde, sondern neu auch, dass die Rechte der betroffenen Personen gewährleistet sind (Abs. 2). Was dies genau bedeutet, ist nicht wirklich klar, ist die Gewährleistung der Rechte der betroffenen Personen doch primär die Aufgabe des Verantwortlichen. Handelt es sich wie oft beim Auftragsbearbeiter um eine im Hintergrund agierende Person (wie z.B. ein Outsourcing-Dienstleister), tritt sie gegenüber den betroffenen Personen nicht auf und ist auch nicht deren Ansprechpartner. Richtigerweise müsste also sichergestellt sein, dass der Auftragsbearbeiter das in seinem Bereich Erforderliche tut, damit der *Verantwortliche* die Rechte der betroffenen Personen gewährleisten kann. So wird ein Verantwortlicher prüfen müssen, ob der Auftragsbearbeiter ihm den für einen Auskunftsanspruch erforderlichen Datenzugang gewährleistet oder dass er Datenlöschungen, die der Verantwortliche durchführen muss, ausführen kann.

[Rz 103] Zweitens dürfte der Mindestinhalt der Verträge zwischen Verantwortlichem und Auftragsbearbeiter neu indirekt durch die Verordnung zum DSG konkretisiert werden. Es ist zu vermuten, dass dies analog der Regelung der DSGVO erfolgt. Dies wird bedeuten, dass auf das Inkrafttreten des neuen DSG kurzfristig alle Verträge mit Auftragsbearbeitern überprüft werden müssen. Die Kompetenzdelegation in Abs. 2 ist jedoch problematisch: Sie spricht nicht von einer Konkretisierung der in Art. 7 VE DSG geregelten Grundsätze, sondern von «weiteren» Pflichten, was fallengelassen werden sollte: Es gibt keinen Anlass, dem Bundesrat das Recht einzuräumen, für die Auftragsdatenbearbeitung *weitere* Pflichten vorzusehen, als sie das DSG ohnehin schon vorsieht, und diese gehen schon jetzt zu weit. Eine solche Regelung ist überdies aus rechtsstaatlicher Sicht heikel.

[Rz 104] Drittens wird ein Auftragsbearbeiter weitere Auftragsbearbeiter neu nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen beiziehen dürfen (Abs. 3). Diese Regelung entspricht derjenigen der DSGVO, wobei dort klargestellt wird, dass auch eine generelle Einwilligung möglich ist, die noch keinen Bezug auf die einzelnen Unter-Auftragsbearbeiter nimmt. Zu

denken ist etwa an eine generische Klausel im Vertrag zwischen Verantwortlichem und Auftraggeber, in welchem die Zustimmung pauschal erteilt wird. In der DSGVO wird für diesen Fall verlangt, dass der Verantwortliche vor dem Beizug eines bestimmten Auftragsbearbeiters den Verantwortlichen über diesen informiert und ihm ein Vetorecht gibt. Dies sollte an sich auch für die Schweiz gelten, geht aus der neuen Bestimmung in Abs. 3 aber nicht hervor. Da dieses Vetorecht eine sehr spezielle Regelung darstellt, wäre es angezeigt, darauf hinzuweisen; bisher findet sich ein Hinweis lediglich in den Erläuterungen.[77] Ungenau ist auch der Hinweis auf die Notwendigkeit, dass die Zustimmung schriftlich erfolgt, denn wenn es sich dabei um Schriftlichkeit im Sinne von Art. 13 OR handelt[78], was normalerweise der Fall ist, wenn sich aus dem Gesetz nichts Weiteres ergibt, werden z.B. Online-Verträge mit Cloud- und Internet-Providern nicht mehr möglich sein, da diese regelmässig Unterauftragnehmer haben. Wesentlich kann nicht sein, dass die Zustimmung schriftlich im Sinne des OR erfolgt. Wesentlich ist, dass sie in dokumentierter Weise erfolgt, also ein Nachweis durch Text möglich ist.

[Rz 105] Aus der Regel des Zustimmungsvorbehalts in Abs. 3 ergibt sich implizit im Übrigen auch, dass es weiterhin erlaubt sein wird, dass es genügt, wenn die Verträge mit Unterbeauftragten nur mit dem Auftragsbearbeiter abgeschlossen werden, also keine direkte Vertragsbeziehung zum Verantwortlichen erforderlich ist.[79] Das ist in der Praxis ein wichtiger Aspekt und gilt so unter bestehendem Recht und auch in der EU. In diesen Fällen wird dann der Auftragsbearbeiter die Rolle des Verantwortlichen gegenüber dem Unterbeauftragten übernehmen. Bei diesem Fall zeigt sich auch, wie durchdacht und differenziert die bisherige Terminologie des Schweizer Rechts war: Es unterschied die Rolle der Inhaberschaft der Datensammlung (bzw. neu der Funktion des Verantwortlichen) von jener des Auftraggebers, da ein Auftraggeber nicht zwingend der (in letzter Instanz) Verantwortliche ist.

14. Brisant, aber kreativ: Die «Empfehlungen der guten Praxis»

[Rz 106] Die sicherlich kreativste aber auch rechtsstaatlich «speziellste» Neuerung des Vorentwurfs ist das Konzept der «Empfehlungen der guten Praxis» in Art. 8 und 9 VE-DSG. Die Idee ist in jedem Fall begrüssenswert; sie war auch schon im Vorfeld diskutiert worden und ist auch keine Schweizer Erfindung. Das österreichische Recht kennt sie zum Beispiel schon. Es adressiert das Grundproblem des DSG, das mit seinem Konzept «Prinzipien statt Regeln» zwar sehr flexibel ist und so bestens für die jeweiligen Umstände richtig angewandt werden kann, dadurch aber für den nicht bewanderten Leser zu wenig konkret ist und damit gewisse Rechtsunsicherheiten schafft: Er weiss in der Praxis oft nicht, was genau erlaubt ist und was nicht. Dem wurde bisher mit «Soft Law» begegnet. Neu soll es möglich sein, bestimmte Verhaltensweisen vom EDÖB als datenschutzkonform absegnen zu lassen (Art. 8 Abs. 2 VE DSG). Der EDÖB soll aber auch selbst «Empfehlungen» abgeben, wie sich bestimmte Dinge datenschutzkonform tun lassen (Abs. 1). Diese Empfehlungen sollen keine «*best practice*» sein, sondern lediglich «*good practice*», und in

77 Erläuterungen VE DSG, S. 52.

78 Welche Bestimmung in der Regel eine handschriftliche Unterschrift auf einem festen Träger erfordert.

79 Eine «Zustimmung» braucht es sachlogisch nur in Fällen, in welchen die zustimmende Partei selbst nicht Vertragspartei ist.

Art. 9 Abs. 2 VE DSG wird richtigerweise betont, dass sie in keiner Weise zwingend sind und der Datenschutz auch auf andere Weise eingehalten werden kann.

[Rz 107] Der Clou findet sich aber in Art. 9 Abs. 1 VE DSG, wonach die Einhaltung einer vom EDÖB verfassten oder genehmigten «Empfehlung der guten Praxis» für einen Verantwortlichen bedeutet, dass er die damit konkretisierten Bestimmungen des DSG befolgt hat (warum dies nicht auch für einen Auftragsbearbeiter gelten sollte, ist nicht ersichtlich; dies dürfte ein Versehen sein). Es handelt sich rechtstechnisch um eine Fiktion, die auch für die Gerichte bindend sein wird. Spannend ist dabei, dass in keiner Weise vorgesehen ist, wie oder dass der Erlass oder die Genehmigung einer Empfehlung einer rechtsstaatlichen Kontrolle unterliegen soll. Der EDÖB kann bezüglich seiner eigenen Empfehlungen gemäss Vorentwurf tun und lassen, was er will.

[Rz 108] Die Empfehlungen der guten Praxis qualifizieren nicht als Verfügungen und sind daher auch nicht als solche anfechtbar. Verfügungscharakter wird zwar Genehmigung einer Fremdempfehlung haben: Weist der EDÖB eine beispielsweise von einem Branchenverband vorgelegte Empfehlung als ungenügend ab, wird er auf Verlangen des Verbands eine beschwerdefähige Verfügung ausstellen müssen, gegen die der Verband vorgehen kann. Nach Art. 8 Abs. 2 VE DSG besteht ein Anspruch auf Genehmigung, wenn die vorgelegte Empfehlung mit den Vorschriften des DSG «vereinbar» ist. Sind umgekehrt die betroffenen Personen, deren Daten im Einklang mit einer solchen Empfehlung der guten Praxis bearbeitet werden, mit ihr nicht einverstanden, werden sie sich höchstens indirekt wehren können. Wie das gehen soll, ist aber völlig unklar, denn der Vorentwurf sieht hierzu nichts vor. Es ist in der Tat erstaunlich, dass die damit zusammenhängenden Fragen auch in den Erläuterungen nicht diskutiert werden. Dabei kann die Wirkung einer Empfehlung der guten Praxis massiv sein: Ist sie zu Unrecht genehmigt oder erlassen worden, beraubt sie die betroffenen Personen aufgrund der Fiktion der Gesetzmässigkeit der Datenbearbeitung ihrer gesetzlichen Rechte. Dem Autor ist ein vergleichbares Instrument des Schweizer Rechts bisher nicht bekannt. Hier sind eingehende Überlegungen zum Rechtsschutz erforderlich. Dazu gehört zum Beispiel auch eine Befristung der Empfehlungen der guten Praxis, deren Überarbeitung oder deren gerichtliche Überprüfung. Denkbar ist zum Beispiel ein System analog den Angemessenheitsentscheidungen der Europäischen Kommission, die zwar von den nationalen Gerichten nicht überprüft werden können, die Beurteilung eines Einzelfalls jedoch vorbehalten bleibt. So könnte beispielsweise festgehalten werden, dass die Einhaltung der Empfehlung der guten Praxis nicht eine Fiktion der Datenschutzkonformität zur Folge hat, sondern lediglich eine widerlegbare Vermutung.

[Rz 109] Schon vor diesem Hintergrund dürfte die Regelung, wonach der EDÖB alleine über Ausgestaltung oder Genehmigung einer solchen Empfehlung der guten Praxis bestimmen kann, dazu führen, dass er an solche Empfehlungen einen strengen, übergesetzlichen Massstab anlegen wird. Hinzu kommt, dass dem EDÖB inoffiziell die Rolle des «Beschützers» betroffener Personen und eine solche Empfehlung einen generell abstrakten Charakter haben muss und daher die Berücksichtigung der Umstände im Einzelfall gar nicht möglich ist. Empfehlungen der guten Praxis werden daher zweifellos nicht das Minimum dessen umschreiben, was zur Einhaltung des DSG getan werden muss, sondern letztlich trotz allem eine «beste Praxis» sein, nicht nur eine «gute Praxis». Ihre Gefahr wird darin liegen, dass sie von Gerichten möglicherweise als Richtschnur für die korrekte Umsetzung des DSG herangezogen werden und sie daher bewirken, dass diese das DSG im Ergebnis zu Lasten der Interessen der Datenbearbeiter anwenden, wie dies vom Gesetzgeber an sich nicht beabsichtigt war.

[Rz 110] Weiter stellt sich nebst den bereits angeführten Punkten die Frage, ob es nicht erforderlich ist, ein im Gegensatz zum EDÖB *neutrales*, von ihm unabhängiges Gremium über die Geltung von Empfehlungen der guten Praxis bestimmen zu lassen, wie zum Beispiel eine Kommission, in welcher insbesondere auch Vertreter aus der Praxis einsitzen. Denn Praxiswissen ist gerade in diesem Bereich von zentraler Bedeutung, fehlt dem EDÖB aber erfahrungsgemäss oftmals. Eine solche Vorgehensweise würde den EDÖB zudem personell entlasten und wäre vergleichsweise kostengünstig umzusetzen; dagegen spricht, dass eine solche Kommission ein de facto politisches Gremium wäre, während es vorliegend wichtig ist, Entscheide auf einer Sachebene zu fällen.

[Rz 111] Ein möglicher Ansatz wäre auch, dem EDÖB gar nicht zu gestatten, eigene Empfehlungen der guten Praxis erlassen zu dürfen, sondern nur solche zu genehmigen, die ihm von privater Seite vorgelegt werden. Das Instrument hätte dann stärker den Charakter einer Selbstregulierung. Diese Lösung würde auch dem in breiten Kreisen vorhandene Unbehagen begegnen, dass der EDÖB über seine eigenen Empfehlungen der guten Praxis strengere Anforderungen an ein datenschutzkonformes Verhalten einführt, als das Gesetz es verlangt. In der Vergangenheit wurden seitens des EDÖB immer wieder Regelungen als geltendes Recht vertreten, die klar keine gesetzliche Grundlage haben.[80] Mindestens jedoch sollte der EDÖB verpflichtet werden, die betroffenen Verkehrskreise vor dem Erlass einer Empfehlung der guten Praxis zu konsultieren bzw. eine gerichtliche Überprüfung solcher Empfehlungen durch diese vorgesehen werden, analog dem heute gegen unzulässige öffentliche Behauptungen des EDÖB möglichen Vorgehen gegen Realakte.

15. Aufsicht und Sanktionen: Deutlich härtere Gangart

[Rz 112] Die mit Sicherheit am meisten beachtete neue Regelung des Vorentwurfs sind die Sanktionen, die neu eingeführt werden. Heute kennt das DSG keine nennenswerten Sanktionen; sanktioniert werden gewisse Verhaltensweisen im Zusammenhang mit dem Auskunftsrecht, die vorsätzliche Unterlassung der besonderen Informationspflicht bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen und der Kooperations-, Registrier- und Meldepflichten gegenüber dem EDÖB. Sie führten in der Praxis zu so gut wie keinen Verurteilungen.

[Rz 113] Dass sich dies mit dem Vorentwurf ändern würde, war klar, verlangt doch auch die revidierte Konvention 108 die Einführung von «Administrativsanktionen» im Falle einer Datenbearbeitung, welche die Vorgaben der Konvention verletzt.[81] Vor diesem Hintergrund war erwartet worden, dass der Vorentwurf für Datenschutzverletzungen künftig Verwaltungssanktionen einführt, wie sie auch schon diverse andere Gesetze wie etwa das Fernmeldegesetz oder Kartellgesetzt kennen. Diese sehen Bussen von bis zu zehn Prozent des Jahresumsatzes vor. Die DSGVO setzt ebenfalls hauptsächlich auf Verwaltungssanktionen, die dort bis zu vier Prozent des Jahresumsatzes entsprechen dürfen, allerdings bemessen am weltweiten Umsatz des Unternehmens oder der Unternehmensgruppe, dies je nach Lesart der DSGVO.[82]

---

80 So beispielsweise, dass die Bearbeitung von Persönlichkeitsprofilen eine Einwilligung erfordert. Das Gesetz verlangt nur bei der *Bekanntgabe* von Persönlichkeitsprofilen an Dritten eine Einwilligung *oder* einen anderen Rechtfertigungsgrund.

81 Art. 12bis Abs. 2 Bst. c der revidierten Konvention 108 (Entwurf Stand September 2016).

82 Art. 83 DSGVO.

[Rz 114] Es kam anders: Art. 50 ff. VE DSG setzt primär auf private, strafrechtliche Sanktionen gegen die einzelnen, in eine Verletzung des DSG involvierten Organe und Mitarbeiter. Der Vorentwurf geht somit auch hier über die DSGVO und das, was von der Konvention 108 verlangt wird, hinaus. Der Bussenrahmen beträgt CHF 500'000 für die vorsätzliche Begehung der einzelnen Delikte, erfasst aber mit Bussen von bis zu CHF 250'000 auch fahrlässige Datenschutzverstösse. Ein fahrlässiger Verstoss gegen das DSG kann somit gleich massiv geahndet werden wie die fahrlässige Verletzung des Bankgeheimnisses. Zum Vergleich: Die fahrlässige Verletzung des Amts-, Anwalts- oder Arztgeheimnisses ist nicht strafbar.[83]Immerhin: Anstiftung und Gehilfenschaft sind bei Übertretungen wie hier nicht strafbar.

[Rz 115] Art. 53 VE DSG sieht zwar vor, dass von der Ermittlung der strafbaren Person in einem Betrieb abgesehen werden kann, wenn die Busse CHF 100'000 nicht überschreiten wird; in diesem Falle wird das Unternehmen gebüsst. Der einzelnen Person, die sich durch eine Handlung möglicherweise strafbar macht, wird diese Regelung jedoch kaum den nötigen Komfort geben, da ihre Strafbarkeit von einem entsprechenden Entscheid der ermittelnden Behörde abhängt. Da die Sanktionen strafrechtlicher Natur sind, muss damit gerechnet werden, dass sie weder versichert werden können, noch vom Unternehmen für den Gebüssten bezahlt werden dürfen, da dies als eine strafbare Verfolgungsbegünstigung qualifiziert werden könnte.[84]

[Rz 116] Der persönliche, strafrechtliche Charakter der Sanktionen ist unverhältnismässig und nicht zielführend. Speziell diejenigen Personen, die wie etwa betriebliche Datenschutzverantwortliche in ihrer Tätigkeit für den Datenschutz an sich geschützt und gestärkt werden sollten, werden durch die Schaffung eines persönlichen Strafbarkeitsrisikos unnötig unter Druck gesetzt und exponiert (vgl. z.B. Rz 97 oben). Mitarbeiter in den Unternehmen werden sich hüten, in strafrechtlich bedrohten Datenschutzfragen selbst Entscheide zu treffen, ohne sich über externen Rechtsrat durch Spezialisten abgesichert zu haben, was zu einer unnötigen Verteuerung der Datenbearbeitung führt und dazu, dass die Möglichkeiten des DSG zur Datenbearbeitung nicht mehr ausgeschöpft werden. Damit aber kommt der vom Gesetzgeber gewollte Ausgleich zwischen den Interessen der betroffenen Personen und der Datenbearbeiter nicht mehr zum Tragen. Die ersten Reaktionen auf den Vorentwurf lassen vermuten, dass die gegenwärtig vorgeschlagenen strafrechtlichen Sanktionen politisch wenig Chancen haben werden.

[Rz 117] Das gilt ganz besonders für die Strafbarkeit von fahrlässigen Verstössen gegen das DSG. Solche Verstösse sind natürlich nicht hinzunehmen, aber eine Kriminalisierung der einzelnen Mitarbeiter ist stossend, zumal die Delikte in den meisten Fällen «nur» in der Verletzung *flankierender* Massnahmen wie etwa eine unterlassene Datenschutz-Folgenabschätzung oder Dokumentation der Datenbearbeitung bestehen, durch welche die betroffenen Personen zunächst nicht wirklich in ihrer Privatsphäre verletzt sind. Pikanterweise sind jene Fälle, in denen die Persönlichkeit einer betroffenen Person tatsächlich verletzt werden, nicht unter Strafe gestellt. Gebüsst wird nicht derjenige, der Personendaten bewusst zweckwidrig oder unverhältnismässig verwendet, sondern derjenige, der vergisst, diese Datenschutzverletzung dem EDÖB zu melden. Das kann nicht sein.

---

83 Art. 320 f. StGB.

84 Art. 305 StGB; allerdings ist darauf hinzuweisen, dass diese Frage im Falle der Bezahlung einer Geldbusse durch einen Dritten in der Lehre umstritten ist (gegen das Vorliegen einer Begünstigung: Vera Delnon/Bernhard Rüdy, Basler Kommentar, 3. Auflage, Art. 305 StGB, N 20, m.w.H.).

[Rz 118] Einige Stimmen vertreten gar die Ansicht, dass es gar keine Sanktionen braucht, was aus Sicht des Datenschutzes sicherlich stimmt (die Nichteinhaltung einer Verfügung des EDÖB könnte bereits mit der bestehenden Regelung von Art. 292 des Schweizerischen Strafgesetzbuches StGB sanktioniert werden), aber für manche im Widerspruch zum Wortlaut der Konvention 108 steht. Es kann immerhin vertreten werden, dass der Begriff der Administrativsanktion nicht zwingend eine Geldbusse erfordert; auch ein Bearbeitungsverbot könne eine solche sein, wird argumentiert. Allerdings dürften die realpolitischen Chancen, dass das revidierte DSG keine finanziellen Sanktionen enthält, sehr gering sein.

[Rz 119] Wer nach den Gründen der scharfen Regelung im Vorentwurf forscht, dem wird rasch klar, dass sie rein opportunistischer Natur sind: Dem EDÖB soll offenkundig nicht die mit der Sanktionierung von Datenschutzverstössen verbundene (Arbeits-)Last auferlegt werden. Durch eine strafrechtliche Sanktionierung können die Fälle an die Kantone abgeschoben werden.[85] Kommt diese Regelung durch, werden die kantonalen Staatsanwaltschaften künftig auch einen Datenschutzjuristen einstellen müssen, um die betreffenden Fälle zu untersuchen und abzuurteilen. Dies zeigt zugleich, wie ineffizient diese Regelung ist: Zwar ist es denkbar, dass ein Datenschutzverstoss von einer betroffenen Person direkt zur Anzeige gebracht und untersucht wird. Der Regelfall wird jedoch sein, dass ein Fall zunächst vom EDÖB untersucht werden wird (dazu Rz 126 unten). Dieser soll dann im Falle eines strafrechtlich relevanten Verhaltens Anzeige erstatten; Art. 45 VE DSG verpflichtet ihn dazu. Derselbe Fall wird dann von der zuständigen Strafbehörde nochmals untersucht werden müssen. Dies ist auch zwingend erforderlich, da nur so die strafprozessualen Rechte der Beschuldigten gewahrt werden können. Dass sich die Strafbehörden mangels eigener Datenschutzerfahrung wohl auf die Einschätzung des EDÖB abstützen werden, macht die Sache rechtsstaatlich nicht besser.

[Rz 120] Der gewählte Weg der strafrechtlichen Sanktion zwingt auch zur Befassung mit dem strafrechtlichen Bestimmtheitsgebot.[86] Dies dürfte mit ein Grund dafür sein, dass vor allem formelle Pflichten bzw. Massnahmen zur Datenschutz-Governance und –Aufsicht strafrechtlich sanktioniert werden und nicht datenschutzwidrige Datenbearbeitungen selbst. Der gewählte Ansatz ändert jedoch nichts daran, dass viele der sanktionierten Bestimmungen viel zu offen formuliert sind, dass es für den Rechtsunterworfenen schwierig sein wird zu verstehen, was er genau tun darf und was nicht. Dies wird dazu führen, dass er entweder weniger weit geht, als er dies an sich tun können sollte, oder es wird schwierig werden, ihn strafrechtlich zu belangen, weil das DSG das sanktionierte Verhalten zuwenig bestimmt umschreibt.

[Rz 121] Inhaltlich werden die Strafregelungen ebenfalls überarbeitet werden müssen. So sind ein Teil der Delikte nur auf Antrag strafbar, doch ist unklar, wer in solchen Fällen antragsberechtigt sein soll. Beispiele sind die Pflicht zur Dokumentation von Datenbearbeitungen oder die Durchführung einer Datenschutz-Folgenabschätzung (Art. 51 VE DSG). Antragsberechtigt sind jedoch nur Personen, die durch eine solche Unterlassung verletzt werden.[87] Durch die Unterlassung einer Dokumentation oder Folgenabschätzung wird jedoch niemand verletzt, jedenfalls nicht direkt oder höchstens in sehr speziellen Konstellationen. Die Bestimmung bleibt damit toter Buchstabe. Der EDÖB kann ebenfalls nicht sanktionieren, und auch eine etwaige Strafanzeige seinerseits wäre unbeachtlich.

85 Art. 54 VE DSG, welche Bestimmung jedoch überflüssig ist.

86 Art. 1 StGB.

87 Art. 30 Abs. 1 StGB.

[Rz 122] Die Strafbestimmungen in Art. 50 f. VE DSG sind nicht die einzigen, die eingeführt oder angepasst werden sollen:

- Das heute in Art. 35 DSG geregelte «kleine» Berufsgeheimnis, das bisher nur besonders schützenswerte Personendaten und Persönlichkeitsprofile schützte, wird ausgebaut und zu einem allgemeinen Berufsgeheimnis für jeden erweitert, der für die Zwecke seines Berufes geheime Personendaten bearbeiten muss oder solche schlicht zu «kommerziellen Zwecken» bearbeitet. Statt den Verrat nur mit Busse zu sanktionieren, sieht die Norm neu auf Antrag eine Freiheitsstrafe von bis zu drei Jahren oder Geldstrafe vor. Die Bestimmung steht damit dem «grossen» Berufsgeheimnis für Anwälte, Ärzte und Geistliche[88] in nichts mehr nach. Im Gegenteil: Eine Befreiung von der Geheimnispflicht durch eine etwaige Aufsichtsbehörde ist nicht vorgesehen. Die Auswirkungen dieser Anpassung sind noch unklar. Gegenüber Art. 162 StGB grenzt sich die Bestimmung dadurch ab, dass sie nicht nur Geschäftsgeheimnisse, sondern auch «private» Geheimnisse schützt. Weiter kann die Frage gestellt werden, ob die Norm nur dann angewandt werden kann, wenn mindestens implizit zwischen Geheimnisherr und Geheimnisträger eine vertragliche Geheimhaltungspflicht besteht, wie sie Art. 162 StGB verlangt oder zum Beispiel auch das Bankgeheimnis.[89] Soll die Anwendung nicht uferlos werden, wird verlangt werden müssen, dass die Information nicht nur geheim ist, sondern der Geheimnisherr auch eine berechtigte, in einem Vertrag oder sonstigem Verhalten oder Übung begründete Erwartung hat, dass der Geheimnisträger sie auch geheim halten wird. Doch selbst dann hat die Bestimmung einige Sprengkraft, da sie sehr viele Personen, die sich dem gar nicht bewusst sein werden und dies auch nicht erwarten, neu einem strafrechtlich sanktionierten Berufsgeheimnis unterstellt, weil argumentiert wird, dass sie implizit eine Geheimhaltungspflicht haben. So gehen die Erläuterungen offenbar davon aus, dass künftig auch Online-Händler und Betreiber sozialer Netzwerke mit Bezug auf die Daten ihrer Kunden unter diese Regelung fallen und sie etwa zur Anwendung gelangen kann, wenn diese für Marketingzwecke unberechtigterweise verkauft werden.[90] Es wird nicht lange dauern bis argumentiert werden wird, dass eine vorsätzlich datenschutzwidrige Bekanntgabe von nicht jedermann zugänglichen Personendaten in einem Geschäftsbetrieb immer auch eine Verletzung der beruflichen Schweigepflicht darstellt und daher mit bis zu drei Jahren Freiheitsstrafe sanktioniert werden kann. Das erscheint nicht angemessen. Die mit der Anpassung angestrebte Anlehnung an Art. 321 StGB leuchtet nur auf den ersten Blick ein: In den in Art. 321 StGB erfassten Berufen ist es für alle Beteiligten klar, dass Kundendaten grundsätzlich vertraulich zu behandeln sind. Bei einem Online-Shop oder einem sozialen Netzwerk ist das eben nicht der Fall; die beiden Anwendungsvoraussetzungen von Art. 52 VE DSG lösen dieses Problem nicht, da sie beliebig viele Fälle erfassen. Hier wäre entscheidend, dass nur solche Daten der beruflichen Schweigepflicht unterliegen, für welche eine Schweigepflicht unabhängig von Art. 52 VE DSG klar besteht, denn sonst unterliegt so gut wie jeder Berufstätige einer strafrechtlich sanktionierten Schweigepflicht, was unsinnig ist. Es stellt sich die Frage, warum der bisherige Art. 35 DSG nicht einfach beibehalten wird; einen guten Grund für seine Anpassung ist jedenfalls nicht ersichtlich und ein diesbezüglicher Leidensdruck besteht auch nicht wirklich.

88 Art. 321 StGB.

89 Art. 47 BankG.

90 Erläuterungen VE DSG, S. 86.

- Art. 179^{novies} StGB soll ebenfalls ausgeweitet werden und stellt neu jeden auf Antrag unter Strafe, der «unbefugt» Personendaten beschafft, «die nicht für jedermann zugänglich sind». Die Strafandrohung ist mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe deutlich höher als die Bussen, die für sonstige Datenschutzverletzungen vorgesehen sind. Allerdings ist nicht klar, inwiefern die mit der neuen Formulierung zu erfassenden Delikte von den sonstigen Datenschutzverletzungen abgrenzen sollen. Die bisherige Regelung kam nur dann zum Tragen, wenn unbefugt nicht frei zugängliche besonders schützenswerte Personendaten oder Persönlichkeitsprofile aus einer Datensammlung beschafft wurden. Gemeint waren damit allerdings Datendiebstähle aus gesicherten Systemen und Räumen, und nicht eine blosse Verletzung des Datenschutzes, indem eine Person etwa unter Missachtung des Transparenz- oder Verhältnismässigkeitsgrundsatzes Daten erhob, was ja nach Wortlaut ebenfalls erfasst wäre und den Anwendungsbereich der Norm massiv erweitert hätte. Dies scheint trotz einer geringfügigen Anpassung des Wortlauts (neu «für jedermann zugänglich» statt wie heute «frei zugänglich») nicht der Fall zu sein. Die Erläuterungen sprechen jedenfalls lediglich darüber, dass die von der Bestimmung erfassten Datenkategorien erweitert werden sollen.[91] Die «Unbefugtheit» meint somit nicht unbefugt im Sinne einer Verletzung des DSG (wie etwa in Art. 11 VE DSG), sondern ohne Befugnis des für die Daten Verantwortlichen.[92]
- In Art. 179^{decies} StGB neu eingeführt werden soll schliesslich eine Bestimmung zur strafrechtlichen Ahndung des Identitätsmissbrauchs.[93] Er soll dann bestraft werden können, wenn die Identität einer anderen Person dazu verwendet wird, dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen. Diese Bestimmung erscheint sinnvoll, da gegen ein solches Verhalten bisher meist nur zivilrechtlich vorgegangen werden konnte, was wiederum regelmässig daran scheiterte, dass die Identität des Täters ohne strafprozessuale Mittel nicht ermittelt werden konnte.

[Rz 123] Nebst Strafbestimmungen sollen auch die Rechte des EDÖB erweitert werden. Das bisherige System der Sachverhaltsabklärungen, Empfehlungen und Klagen vor Bundesverwaltungsgericht wird, obwohl es gut funktioniert, abgeschafft. Neu soll der EDÖB die Kompetenz erhalten, gegen Datenbearbeiter verwaltungsverfahrensrechtliche Untersuchungen durchzuführen (Art. 41 VE DSG) und gegen diese Verfügungen zu erlassen, sei es in Form von vorsorglichen Massnahmen (Art. 42 VE DSG), sei es, um eine Datenbearbeitung anzupassen, sie zu stoppen, einschliesslich der Bekanntgabe ins Ausland, oder um Daten zu vernichten (Art. 43 VE DSG). Der EDÖB soll offenbar sogar die Kompetenz erhalten, gegen eine Bekanntgabe ins Ausland selbst dann vorzugehen, wenn sie nicht gegen das DSG, sondern gegen ein anderes Gesetz verstösst; was dies bedeuten soll, wird aber nicht näher erläutert.[94]

[Rz 124] Problematisch ist in diesem Zusammenhang, dass Beschwerden gegen vorsorgliche Massnahmen *per se* keine aufschiebende Wirkung haben sollen (Art. 44 Abs. 3 VE DSG). Hierbei ist zu berücksichtigen, dass eine vorsorglich verfügte Einstellung oder Anpassung einer Datenbearbeitung gerade im Bereich der automatisierten Datenbearbeitung massive Kosten bzw. Schäden zur Folge haben kann, die der EDÖB regelmässig nicht einschätzen können wird. Solange der Staat bzw. der EDÖB für diese nicht aufkommt, muss ein Unternehmen die Möglichkeit haben, sich

91 Erläuterungen VE DSG, S. 93.

92 David Rosenthal, Handkommentar DSG, Zürich 2008, Art. 179^{novies} StGB, N 17.

93 Diese Bestimmung geht zurück auf die Motion Comte 14.3288.

94 Erläuterungen VE DSG, S. 80, mit Verweis auf Art. 12 Abs. 2 des Entwurfs der revidierten Konvention 108.

vor einer unabhängigen Instanz gegen ein unverhältnismässiges Vorpreschen des EDÖB wehren zu können. Das bisherige System, dass der EDÖB solche Massnahmen vom Bundesverwaltungsgericht beantragen musste, hat sich bestens bewährt (und gezeigt, dass der EDÖB gewisse vorsorgliche Massnahmen auch unberechtigt verlangt hat[95]).

[Rz 125] Das Verfahren richtet sich neu nach dem Verwaltungsverfahrensgesetz. Gemäss Vorentwurf soll der EDÖB das Recht haben, ohne Vorankündigung Hausdurchsuchungen durchzuführen und sich Zugang zu allen notwendigen Daten und Information zu verschaffen, muss das untersuchte Unternehmen aber vorgängig erfolglos zur Mitwirkung angehalten haben (Art. 41 Abs. 3 VE DSG). Wie das im Einzelnen vor sich gehen soll, bleibt unklar. Nicht wirklich diskutiert sind auch so heikle Fragen wie der Grundsatz *nemo tenetur* – das Recht zu Vorwürfen gegen die eigene Person zu Schweigen bzw. sich nicht selbst belasten zu müssen –, die sich angesichts der Pflicht zur Meldung von Datenschutzverstössen und den strafrechtlichen Konsequenzen akzentuiert stellen.

[Rz 126] Der EDÖB kann jederzeit ein Verfahren eröffnen, wenn Anzeichen bestehen, dass gegen das DSG verstossen wird; es muss nicht mehr eine grössere Zahl von Personen betroffen sein. Eine Pflicht zur Untersuchung besteht allerdings nicht, auch nicht im Falle einer Anzeige einer betroffenen Person. Immerhin muss der EDÖB diese über sein Vorgehen und das Ergebnis einer allfälligen Untersuchung informieren (Art. 41 Abs. 5 VE DSG); Partei ist sie nicht (Art. 44 Abs. 2 VE DSG), aber es steht ihr selbstverständlich offen, gestützt auf das ihr mitgeteilte Ergebnis (und weiteren Informationen, die sie über ein Gesuch nach Öffentlichkeitsgesetz erhält) gegen den Verantwortlichen zivilrechtlich vorzugehen. Diese neuen Bestimmungen sind aufgrund der Vorgaben der revidierten Konvention 108 und der politischen Stimmung erwartet worden. Viele Beobachter gehen jedoch auch davon aus, dass die Neuerungen dem Datenschutz nicht dienen werden: Zwar erhält der EDÖB mehr und schärfere Instrumente zur Aufsicht in die Hand, doch damit verbunden wird ebenso der Aufwand, den er für die entsprechenden Verfahren betreiben muss, deutlich steigen. Da jedenfalls bei der heutigen politischen Grosswetterlage nicht davon auszugehen ist, dass ihm hierfür mehr Mittel zur Verfügung stehen werden, wird er im Ergebnis weniger Fälle durchführen können. Immerhin soll ihm weiterhin das Recht zustehen, auch ausserhalb eines formellen Untersuchungsverfahrens zu überprüfen, ob ein Unternehmen (oder eine Behörde) die Datenschutzvorschriften einhält (Art. 41 Abs. 4 VE DSG). Obwohl in diesen Fällen kein Zwang zur Kooperation besteht, ist ein Widerstand seitens der betroffenen Unternehmen kaum zu erwarten.

16. Und wo bleiben die Übergangsregelungen?

[Rz 127] Schon bei der letzten Revision des DSG im Jahre 2008 stellten sich hinsichtlich der Übergangsregelungen etliche Fragen. Angesichts der noch sehr viel zahlreicheren Neuerungen, die der Vorentwurf vorsieht, erstaunt es daher, dass die Übergangsbestimmungen in Art. 59 VE DSG so mager ausgefallen sind.

95 So im Fall Moneyhouse im Sommer 2012, in welchem eine superprovisorische Sperrung des Dienstes kurze Zeit danach wieder aufgehoben wurde (vgl. https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-45545.html).

[Rz 128] Zwei Jahre Zeit wird gewährt für die Erstellung der Dokumentation der zum Zeitpunkt des Inkrafttretens des revidierten DSG bereits bestehenden Datenbearbeitungen, zur diesbezüglichen Einführung des «*Privacy by Default*» und «*Privacy by Design*» und eines Verfahrens zur Datenschutz-Folgenabschätzung. Warum selbiges zum Beispiel nicht auch für ein Verfahren zur Meldung von Datenschutzverstössen gelten soll, bleibt unklar. Es fehlen auch Übergangsregelung für andere wichtige Punkte wie zum Beispiel die neuen Informations- und Auskunftspflichten, automatisierten Einzelentscheiden und Verträge mit Auftragsbearbeitern.

[Rz 129] Die einfachste Lösung wird daher sein, für die Umsetzung des revidierten DSG eine generelle Umsetzungsfrist von zwei Jahren vorzusehen. Zwar steht die Schweiz unter einem gewissen Druck der EU, ihr Datenschutzrecht anzupassen. Entscheidend wird jedoch sein, dass das Parlament das DSG revidiert, und nicht, wann genau es in Kraft tritt. Überdies hat die EU für die DSGVO ebenfalls eine Umsetzungsfrist von zwei Jahren vorgesehen, und zwar für alle Bestimmungen.

17. Abgrenzung zur DSGVO

[Rz 130] Viele Schweizer Unternehmen sehen sich heute nicht nur mit den Anforderungen eines revidierten DSG konfrontiert, sondern werden auch in den Geltungsbereich der DSGVO fallen. Dies ist nach Art. 3 DSGVO zum Beispiel dann der Fall, wenn sie Daten von Personen in der EU bearbeiten, weil sie diesen dort Produkte oder Dienstleistungen anbieten oder weil sie deren Verhalten analysieren, oder wenn sie deren Daten durch einen Auftragsbearbeiter in der EU (z.B. einen Cloud-Provider) bearbeiten lassen. Damit unterstehen diese Unternehmen zugleich auch der Aufsicht der nationalen EU-Datenschutzbehörden, die zwar nach Art. 55 Abs. 1 DSGVO nur jeweils für ihr «Hoheitsgebiet» zuständig sind, dieser Begriff aber gemäss den Erwägungen der DSGVO extraterritorial zu interpretieren ist.[96] Dies bedeutet für viele Schweizer Unternehmen, die Daten von Personen in der EU bearbeiten, dass sie inskünftig sowohl der Datenschutzaufsicht der Schweiz als auch aller von der Datenbearbeitung betroffenen Mitgliedstaaten der EU (und des EWR) unterstehen.[97] Dies wird zu einer massiven administrativen Zusatzbelastung für Schweizer Unternehmen führen, und überdies zu zahlreichen Rechtsunsicherheiten, da die DSGVO mit Bezug auf ihre Geltung für Unternehmen ausserhalb des Territoriums der EU unsorgfältig redigiert und nicht durchdacht ist.[98] Die Aufsichtstätigkeit der nationalen Datenschutzbehörden der EU-Mitgliedsstaaten auf Schweizer Hoheitsgebiet stellt wiederum die Schweizer Souveränität in Frage und birgt auch für daran mitwirkende Schweizer Unternehmen ein Risiko der Strafbarkeit nach Art. 271 StGB. Die Situation ist also mit anderen Worten konfus und verfahren.

[Rz 131] Vor diesem Hintergrund besteht dringender Abstimmungsbedarf zwischen der offiziellen Schweiz und der EU. Informelle Kontakte diesbezüglich bestehen bereits, und auch die Politik hat den Handlungsbedarf bereits erkannt. Eine Motion «Gegen Doppelspurigkeiten im

96 Erwägung 122 DSGVO.

97 Das Konzept des *One-Stop-Shop* gemäss Art. 56 DSGVO steht für Unternehmen ausserhalb der EU nicht zur Verfügung (vgl. dazu die «Guidelines for identifying a controller or processor's lead supervisory authority» der Artikel-29-Datenschutz-Arbeitsgruppe, WP 244, S. 7).

98 So ist zum Beispiel nicht klar, ob sich ein Schweizer Unternehmen auf Schweizer Recht zur Rechtfertigung einer Datenbearbeitung im Sinne von Art. 6 Abs. 1 Bst. c DSGVO berufen kann; gemäss Art. 6 Abs. 3 DSGVO scheint dies nicht der Fall zu sein, was jedoch zu unbilligen Ergebnissen führt.

Datenschutz»[99] wurde bereits im September 2016 eingereicht und vom Bundesrat zur Annahme empfohlen[100]; der Nationalrat ist dem im Dezember 2016 bereits gefolgt. Im besten Fall kommen die Behörden der beiden Rechtsordnungen überein, dass die (verwaltungsrechtliche) Aufsicht auf dem jeweiligen Hoheitsgebiet alleine Sache der jeweils nationalen Behörde ist, die sie nach ihrem eigenen Recht umsetzt. In diesem Fall wären aufsichtsrechtlich für Datenbearbeitungen durch Unternehmen in der Schweiz einzig der EDÖB zuständig, der sie nach DSG beurteilen würde. Auch die Informations- und Genehmigungspflichten würden für diese Unternehmen nur gegenüber ihm gelten; Schweizer Unternehmen müssten beispielsweise eine Datenschutzverletzung nur ihm und nicht auch allen betroffenen Datenschutzaufsichtsbehörden der jeweiligen EU-Mitgliedsstaaten mitteilen, und zwar nach den Vorgaben des DSG, nicht der DSGVO. Der Informationsfluss zwischen dem EDÖB und den Datenschutzbehörden der EU wäre über die im Vorentwurf ebenfalls vorgesehenen Bestimmungen zur Amtshilfe sichergestellt. Der zivilrechtliche Rechtsschutz bliebe jedoch unberührt, d.h. ein betroffener EU-Bürger könnte auch gegen ein Schweizer Unternehmen gestützt auf DSGVO vorgehen.[101] Dieser Rechtsschutz spielt in der Praxis jedoch eine untergeordnete Rolle.

[Rz 132] Es bleibt zu hoffen, dass die Bundesverwaltung die Gespräche mit der EU möglichst rasch auch offiziell aufnimmt. Zwar gibt es vereinzelt Stimmen, die der Ansicht sind, ein solches Vorgehen habe ohnehin keine Chance, weil die Schweiz gegenüber der EU keine Forderungen stellen könne. Die Realität in der EU zeigt jedoch, dass die EU ebenso an einer Abstimmung mit der Schweiz interessiert ist wie umgekehrt, da mit der Datenschutzaufsicht auch erhebliche Kosten verbunden sind. Kann die Datenschutzaufsicht über Unternehmen mit Sitz in der Schweiz faktisch an den EDÖB «delegiert» werden, kommt dies den einzelnen nationalen Aufsichtsbehörden entgegen, jedenfalls solange die Schweiz über vergleichbare Datenschutzregelungen verfügt und sie ihre Rechte bei Bedarf auf dem Weg der Amtshilfe durchsetzen können, was beides der Fall ist oder noch sein wird. Umgekehrt ist es politisch undenkbar, dass die Schweiz es zulässt, dass EU-Datenschutzbehörden eigene Zwangsmassnahmen nach eigenem EU-Recht durch den EDÖB auf Schweizer Territorium vollziehen lassen oder sogar direkt gegen Unternehmen in der Schweiz durchsetzen.[102] Die britische Regierung wird im Rahmen des BREXIT ähnliche Gespräche führen. Art. 50 Bst. a DSGVO sieht die Kompetenz zur Entwicklung solcher Mechanismen der internationalen Zusammenarbeit zur wirksamen Durchsetzung des Datenschutzes für die Europäische Kommission und die nationalen Aufsichtsbehörden im Übrigen bereits vor.

---

99 Motion Fiala 16.3752.

100 Wenngleich die Begründung des Bundesrats inhaltlich fehlerhaft ist, da sie die Erwägung 122 der DSGVO übersieht. Der Bundesrat geht noch davon aus, dass die EU-Aufsichtsbehörden keine Zuständigkeit für Aktivitäten auf dem Territorium der Schweiz beanspruchen, was falsch ist.

101 Bereits der heutige Art. 139 des Bundesgesetzes über das Internationale Privatrecht (IPRG) gibt einer betroffenen Person weitreichende Wahlrechte mit Bezug auf das Datenschutzrecht, welches auf ihren Fall anwendbar sein soll. Die extraterritoriale Anwendbarkeit, welche Art. 3 Abs. 2 DSGVO neu vorsieht, kennt die Schweiz damit schon lange. Es stellt sich freilich die Frage, ob es sinnvoll wäre, im Zuge der Revision des DSG auch hier gewisse Einschränkungen vorzunehmen und beispielsweise festzuhalten, dass ein ausländischer Erfolgsort (und damit die Anwendbarkeit von ausländischem Datenschutzrecht) nicht allen damit begründet werden kann, dass die Daten im betreffenden Land gespeichert werden. Dies würde beitragen, dass auf Schweizer Unternehmen nicht schon deshalb die DSGVO zur Anwendung kommen könnte, weil sie einen Cloud-Provider in der EU benutzen.

102 Die im Vorentwurf vorgeschlagene Amtshilfebestimmung in Art. 47 VE DSG bleibt diesbezüglich vage. Eine direkte Durchsetzung wäre eine Verletzung von Art. 271 StGB.

18. Schlussbemerkungen

[Rz 133] Im Vorentwurf für ein totalrevidiertes DSG steckt wesentlich mehr verborgen, als es auf den ersten Blick den Anschein macht. Positiv zu vermerken ist, dass die Schweiz der bewährten Tradition, mit Prinzipien statt ausformulierten Regeln zu arbeiten, treu bleiben will. Die Bestimmungen des allgemeinen Teils und des Teils für die Bearbeitung durch Privatpersonen beansprucht neu zwar 25 statt bisher 15 Artikel, doch ist das Gesetzeswerk dennoch erfreulich schlank und kein Vergleich zu den 99, teils furchtbar kompliziert und langwierig verfassten Artikeln der DSGVO.

[Rz 134] Der Vorentwurf erweckt zudem den Eindruck, dass das Bundesamt für Justiz im Datenschutz keine Revolution, sondern eine Evolution suchte mit dem primären Ziel, die Revision der Konvention 108 des Europarats nachzuvollziehen und die Adäquanz der Schweiz im Verhältnis zur EU weiterhin sicherzustellen[103]. Unsinnige Bestimmungen der DSGVO wie etwa jene der Datenportabilität[104] wurden daher zum Glück (vorerst) nicht übernommen, und auch sonst zeigt der Vorentwurf eine gesunde Distanz zur Rechtsetzung in der EU. Denn manches, was diese in der DSGVO umgesetzt hat, ist nicht wirklich durchdacht, und im Bereich der Datenbearbeitung durch Private ist die Schweiz jedenfalls nicht verpflichtet, die Regelungen der DSGVO zu übernehmen. Daher soll bei der Auslegung des DSG richtigerweise nicht einfach die Auslegung der DSGVO herangezogen werden.

[Rz 135] Bei näherer Betrachtung zeigt der Vorentwurf allerdings gewichtige Schwächen, die eine deutliche Überarbeitung erfordern werden. Dies erstaunt etwas, zumal die Vorlage im Rahmen der Ämterkonsultation intensiv kommentiert worden ist, was wohl der Grund für die mehrmonatige Verzögerung des Vorentwurfs ist. Trotz allem macht er einen unausgegorenen, praxisfremden Eindruck. Es entsteht der Anschein, dass mehr Zeit darin investiert worden ist, dem EDÖB genug Spielraum zu verschaffen als die Frage der Praktikabilität und der Auswirkungen auf die Unternehmen zu prüfen, die die neuen Vorgaben umzusetzen haben werden.

[Rz 136] Einige der Mängel sind in diesem Beitrag angesprochen. In etlichen Punkten geht der Vorentwurf zudem ohne guten Grund über die Anforderungen der DSGVO hinaus, auch wenn dies womöglich lediglich Versehen sind oder mit dem heutigen DSG zusammenhängt[105]. Ein solches «Swiss Finish» sollte es aber so oder so nicht geben. Die Wirtschaft wird durch parallele Anwendbarkeit von DSG und DSGVO ohnehin schwer belastet werden. Es sollte ihr daher die Compliance nicht mit einem DSG, das teilweise über die DSGVO hinausgeht, noch schwerer und kostspieliger gemacht werden, als sie in diesem Bereich ohnehin sein wird. In diesen Bereichen wird die Vorlage bei der Erarbeitung der Botschaft hoffentlich zurückgebunden werden.

[Rz 137] Auch wenn ein «Swiss Finish» aus politischen Gründen kaum Chancen haben wird, kommt auf die Schweizer Wirtschaft mit dem revidierten DSG einiges an Mehrarbeit zu. Das betrifft sowohl die Datenschutz-Governance, also die betriebsinternen Massnahmen zur Sicherstellung des Datenschutzes, als auch die Interaktion mit den betroffenen Personen, namentlich was die neuen und stark erweiterten Informations- und Auskunftspflichten betrifft. Dies wird

103 Erläuterungen VE DSG, S. 5 und 32.

104 Art. 20 DSGVO.

105 Dass z.B. auch manuelles Profiling erfasst wird, dürfte darin begründet sein, dass der Begriff den heutigen Begriff des Persönlichkeitsprofils ablöst, das ebenfalls manuell oder automatisiert entstehen kann.

insbesondere auch KMU treffen, die bisher kaum in diesen Bereich investiert haben und die dafür erforderlichen Prozesse und Dokumentationen erst noch schaffen müssen.

[Rz 138] Ob die Revision die Datenschutz-Aufsicht und die Durchsetzung des DSG ebenfalls stärken werden, ist hingegen eine andere Frage. Auf dem Papier wird der EDÖB durch die Verfügungskompetenz und die ausgebauten Untersuchungsmöglichkeiten zweifellos mehr Rechte haben. Die neuen Verfahren werden sein Wirken allerdings auch sehr viel komplizierter machen und von ihm mehr Aufwand abverlangen. Da jedoch bezweifelt werden darf, dass ihm die Politik mehr Mittel in die Hand geben wird, kann es durchaus sein, dass die Datenschutzaufsicht im Ergebnis künftig weniger bewerkstelligen kann, als sie es heute tut. Ob das im Sinne des Erfinders ist, ist allerdings eine andere Frage. Vom revidierten DSG werden vor allem die Datenschutzspezialisten, Sicherheitsexperten und Anwälte profitieren – jedenfalls jene, die sich angesichts der Strafbestimmungen noch trauen, in diesem Minenfeld zu beraten.

David Rosenthal, Lic. iur., Konsulent, Homburger AG, Zürich, Lehrbeauftragter ETH Zürich und Universität Basel; der Autor dankt Barbara Kaiser und Djamila Batache für die Unterstützung und insbesondere die sehr fruchtbaren Diskussionen zum Begriff der «Ausdrücklichkeit» einer Einwilligung.

Amstutz Jonas BJ

Von: Ivo Cathomen <ivo.cathomen@svit.ch>
Gesendet: Mittwoch, 5. April 2017 08:30
An: Amstutz Jonas BJ
Betreff: Vernehmlassung Datenschutzgesetz
Anlagen: svit_vernehmlassungen_datenschutzgesetzes_170404.docx; svit_vernehmlassungen_datenschutzgesetzes_170404.pdf

Sehr geehrter Herr Amstutz

Wegen eines Datenübermittlungsproblems mit dem Word-Formular können wir Ihnen unsere Vernehmlassung leider erst heute übermitteln. Wir mussten die Vorlage in ein neues Dokument umarbeiten.

Freundliche Grüsse
Ivo Cathomen

_____

Ivo Cathomen, Dr. oec. HSG
Stv. CEO SVIT Schweiz
Puls 5, Giessereistrasse 18
CH-8005 Zürich

Telefon +41 44 434 78 82
Mobile +41 79 345 89 15

www.svit.ch
immobilia.svit.ch

Vernehmlassung zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Schweizerischer Verband der Immobilienwirtschaft SVIT Schweiz
Puls 5, Giessereistrasse 18, 8005 Zürich

Ivo Cathomen, Stv. CEO
+41 44 434 78 88
ivo.cathomen@svit.ch

04.04.2017

Allgemeine Bemerkungen

Dem Schweizerischen Verband der Immobilienwirtschaft SVIT Schweiz sind landesweit über 2000 Firmen der Immobilienwirtschaft angeschlossen. Die Dienstleistung der Immobilienbewirtschaftung und damit die treuhänderische Verwaltung von Mietliegenschaften stellt den wichtigsten Wirtschafszweig dar. Art. 253 OR verpflichtet den Vermieter mit dem Mietvertrag, dem Mieter eine Sache zum Gebrauch zu überlassen und den Mieter, dem Vermieter dafür einen Mietzins zu leisten. Das Überlassen der Mietsache setzt ein besonderes Vertrauensverhältnis voraus. Kommt der Mieter seinen Pflichten – unter anderem die Bezahlung der Mieter oder den sorgfältigen Gebrauch der Sache – nicht nach, führt dies in der Regel zu erheblichen Verlusten.

Mietverhältnisse sind Dauerschuldverhältnisse mit besonderem Schutzinteresse. Vermieter sind darauf angewiesen, vor dem Abschluss eines Mietvertrags fundierte Informationen über den Mietinteressenten einzuholen. Dies sind Referenzen, Betreibungsregisterauszüge und namentlich auch Bonitätsauskünfte von entsprechenden Anbietern. Die mangelhafte Verlässlichkeit und Aussagekraft von Betreibungsregisterauszügen ist hinlänglich bekannt. Umso wichtiger sind private Quellen und die Qualität dieser Daten.

Der nun vorliegende Vorentwurf der Totalrevision des Datenschutzgesetzes unterminiert die wirtschaftliche Grundlage unseres Wirtschaftssektors mit über 25'000 Angestellten und stellt einen erheblichen Eingriff in die Wirtschaftsfreiheit dar, indem nicht nur der Datenschutz im öffentlichen, sondern auch im privaten Bereich massiv ausgeweitet werden soll. Rechtsgrundsätze wie Vertragsfreiheit oder der Schutz von Geschäftsgeheimnissen werden tangiert. Der Vorentwurf schiesst weit über das angestrebte Ziel hinaus, ohne dass dafür eine Notwendigkeit besteht. Namentlich ist nicht klar, in welchen Bereichen das bestehende Gesetz europäischem Recht nicht genügt. In welchen Punkten eine Anpassung an die DSGVO 2016/679 und/oder an die Konvention 108 erforderlich ist, und wie weit diese im Einzelfall gehen muss, bleibt offen. Der Erläuterungsbericht verweist meist generell auf das europäische Recht.

Besonders störend ist, dass Unternehmen begründen müssen, wenn sie einen Vertrag nicht abschliessen wollen, was im Mietwesen besonders häufig der Fall ist. Mit dem revidierten Recht hätte jeder Mietinteressent, der den Zuschlag für eine Mietsache nicht erhält, das Recht, Auskunft über den Entscheidungsprozess und die Quellen der dafür herangezogenen Informationen zu erhalten. Im Zuge der Digitalisierung werden auch im Mietwesen automatisierte Prozesse eingesetzt, die Entscheidungen unterstützen. Es geht nicht an, dass Vermieter bzw. Bewirtschafter die von ihnen gesetzten Kriterien für die Mieterselektion offenlegen müssen und damit den Mietvertrag einklagbar machen.

Die administrative Belastung für die KMU (Datenschutzverantwortlicher, Folgeabschätzungen, Informationspflichten, Begründungspflichten usw.) wird ausgeblendet. Ausserdem würden Unternehmen bzw. die Mitarbeiter einem erheblichen Risiko von massiv überhöhten Bussen ausgesetzt, die KMU in ihrer Existenz gefährden könnten.

Der Vorentwurf sieht schliesslich ein kostenloses Klagerecht vor, was zu einer Klageflut führen und die Gerichte massiv belasten wird. Ein solches kostenloses Klagerecht setzt falsche Anreize und verursacht hohe Kosten für den Staat und die beklagten Unternehmen.

Insgesamt fällt die Bilanz zum vorliegenden Vorentwurf deutlich negativ aus. Der vermeintliche, nicht genauer umschriebene Nutzen steht offensichtlichen erheblichen Nachteilen gegenüber, so dass der SVIT Schweiz den Vorentwurf mit aller Entschiedenheit ablehnt. Der Verband fordert, dass die Totalrevision zurückgestellt wird bis Klarheit darüber besteht, wo mit Blick auf das Europarecht tatsächlich Anpassungsbedarf besteht. Sodann ist eine massvolle Umsetzung ohne Swiss Finish an die Hand zu nehmen, die Unternehmen in der Schweiz nicht schlechterstellt als solche im übrigen Europa.

Bemerkungen zur Vorlage im Einzelnen

Der SVIT Schweiz nimmt in erster Linie zu Bestimmungen der Vorlage Stellung, die das Geschäft der Immobilienwirtschaft konkret tangieren.

Art. 3 Ziff. 5

Die Bestimmung ist in dieser allgemeinen Form problematisch. namentlich wenn Vermögensdelikte zur Diskussion stehen, von denen ein künftiger Vertragspartner (z. B. Arbeitgeber) in Kenntnis gesetzt werden müsste.

Art. 3 lit. f

Mit dem Begriff des «Profiling» wird der Katalog auf jede Art von Voraussage ausgedehnt. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als «Persönlichkeitsprofil» qualifiziert worden sind (z. B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich höchst kontraproduktiv, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als «Voraussage» eines späteren Verhaltens interpretiert werden können.

Gerade im Mietwesen sind Rückschlüsse des bisherigen Zahlungsverhaltens auf das zu erwartende künftige Verhalten entscheidend. Es ist davon auszugehen, dass dies als «Profiling» gewertet würde.

Art. 4 Abs. 6

Der SVIT fordert die Streichung des «Profiling» und Beschränkung des Erfordernisses der «ausdrücklichen» Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte.

Art. 8 und Art. 9

Dieser Artikel ist ersatzlos zu streichen. Im Ergebnis werden Datenbearbeiter damit der Willkür des zukünftigen Beauftragten und der «interessierten Kreise» ausgeliefert. Gegen die Empfehlungen des Beauftragten wird kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben.

Art. 13 Abs. 1 und 2

Der SVIT fordert, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z. B. durch Publikation auf einer Webseite oder in den AGB. Im jetzigen Wortlaut ist die Informationspflicht nicht praktikabel.

Art. 13 Abs. 3

Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle Empfängerinnen und Empfänger wird abgelehnt. Die Beziehung von datenverarbeitende Unternehmen und Auftraggeber fällt unter die schützenswerten Geschäftsgeheimnisse. Eine generelle Information muss ausreichend sein.

Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, wo persönlichkeitsverletzende Angaben (z. B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen.

Art. 13 Abs. 5

Dieser Absatz ist ersatzlos zu streichen, weil die Umsetzung in der Praxis zu unverhältnismässig hohem Aufwand führt.

Art. 15 Abs. 2

Dieser Absatz ist ersatzlos zu streichen. Jedes Unternehmen, das über ein strukturiertes Kreditmanagementsystem verfügt, wird inskünftig mit jedem, den es nicht gegen Rechnung beliefern will, Korrespondenz führen müssen, um ihm zu erklären, wie der Entscheid zustande gekommen ist. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse.

Art. 19 lit. b

Die Informationspflicht ist sodann nicht umsetzbar und stellt keinen Nutzen in Aussicht.

Art. 20 Abs. 2 und 3

Namentlich Abs. 2, lit. e und f und Abs. 3 stellen einen Eingriff in die Wirtschaftsfreiheit dar und führen dazu, dass Geschäftsgeheimnisse offengelegt werden müssen. Die Bestimmungen sind in dieser Form abzulehnen.

Art. 24

Die Worte «möglicherweise» und «unmittelbar» sind zu streichen. Der Begriff des überwiegenden Interesses ist weiter zu fassen, wenn nicht unnötig in die Wettbewerbsfreiheit eingegriffen werden soll.

Art. 50 und 51

Die Strafbestimmungen setzen Unternehmen und Mitarbeitende in ihrem wirtschaftlichen Tun einem erheblichen finanziellen und strafrechtlichen Risiko aus. Der SVIT beantragt, dass diese Bestimmungen hinsichtlich ihrer Praktikabilität überprüft werden.

ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundeshaus West
CH–3003 Bern

per E-Mail an jonas.amstutz@bj.admin.ch

Zürich, 24. März 2017

Stellungnahme zum Vorentwurf zur Totalrevision des Datenschutzgesetzes

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Am 21. Dezember 2016 hat der Bundesrat die Vernehmlassung zur Totalrevision des Datenschutzgesetzes (DSG) eröffnet. Diese Revision ist ein sehr anspruchsvolles Projekt. Die Bedürfnisse sämtlicher involvierter Interessen – d.h. der betroffenen Personen, der Bundesorgane und der Wirtschaft (von kleinen KMUs bis hin zu international tätigen Grossunternehmen) – in einem Gesetz zielführend zu berücksichtigen, ist äusserst komplex. Das Versicherungsgeschäft ist vom DSG direkt betroffen. Für den Schweizerischen Versicherungsverband SVV ist deshalb die Revision des DSG von zentraler Bedeutung:

- Der Umgang mit Kundendaten bildet eine unentbehrliche Grundlage des Versicherungsgeschäfts. Versicherer sind auf die Daten ihrer Kundinnen und Kunden angewiesen und die Kunden darauf, dass Versicherer ihre Daten bearbeiten: Dies gilt beim Abschluss eines Versicherungsvertrags (Risikoprüfung und Tarifierung), während des Vertrags und im Schaden- bzw. Leistungsfall sowie für Aktivitäten im Bereich des Marketings.
- Zudem sind Mitgliedgesellschaften des SVV im Sozialversicherungsbereich an der Durchführung von obligatorischen Versicherungen beteiligt.

Gerne nehmen wir deshalb die Gelegenheit wahr, zum Vorentwurf zur Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Wir erlauben uns, Ihnen unsere Überlegungen in zwei Teilen zukommen zu lassen: grundsätzlich und im Detail.

Schweizerischer Versicherungsverband SVV
Conrad-Ferdinand-Meyer-Strasse 14 | Postfach | CH-8022 Zürich | Zentrale +41 44 208 28 28 | Fax +41 44 208 28 00 | www.svv.ch
Franziska Streich | franziska.streich@svv.ch | Direkt +41 44 208 28 63 | Fax direkt +41 44 208 28 07

Management Summary
Der SVV anerkennt den Reformbedarf in Bezug auf das Datenschutzgesetz. Es sind jedoch namhafte Anpassungen und Verbesserungen an der Vorlage notwendig, damit die Unternehmen das neue DSG in der Praxis sinnvoll anwenden und umsetzen können. Unsere zentralen Anliegen sind einerseits grundsätzlicher Natur, wie z.B. Fokus auf Verwaltungssanktionen anstatt Ausbau der Strafbestimmungen und Augenmass bei der Umsetzung der internationalen Verpflichtungen. Andererseits erachten wir unter anderem eine Entschlackung der Informationspflichten, eine praktikable Regelung zum Profiling und eine allgemeine Übergangsbestimmung als zwingend notwendig.

1. Grundsätzliche Bemerkungen

– **Informationspflichten entschlacken**
Ausgangspunkt des Datenschutzgesetzes ist der – im Zusammenhang mit Datenbearbeitungen durch den Staat – verfassungsrechtlich garantierte Schutz der Privatsphäre und der Schutz vor Datenmissbrauch (Art. 13 Bundesverfassung). Gestützt auf diesen verfassungsrechtlichen Ausgangspunkt appellieren wir, den Fokus der Revision auf wesentliche Bedrohungen für die Privatsphäre zu legen.

Deshalb lehnen wir ausufernde Informationspflichten entschieden ab. Das gilt z.B. für Informationspflichten zur Identität und den Kontaktdaten der Auftragsbearbeiter oder beim Beschaffen von Daten bei Dritten (siehe Art. 13 Abs. 4 und 5 VE-DSG). Gleiches gilt für die Informationspflicht gemäss Art. 19 Bst. b VE-DSG. Solche Informationspflichten sind auch aus Kosten-Nutzen-Überlegungen abzulehnen. Informationspflichten, die über Wesentliches hinausgehen, bewirken keinen nennenswerten Beitrag zur Privatsphäre, sondern stiften eher Verwirrung. Es besteht die Gefahr, dass Wichtiges neben Unwichtigem untergeht. Eine Entschlackung der Informationspflichten ist somit dringend angezeigt.

– **Profiling: Information anstatt Einwilligung**
Eine ausdrückliche Einwilligung für das Profiling – wie in Art. 4 Abs. 6 und 23 Abs. 2 Bst. b VE-DSG vorgesehen – ist nicht praktikabel. Zumal der Begriff «Profiling» im VE-DSG sehr breit definiert wird. Die Schweiz geht damit deutlich über die entsprechende Regelung der EU hinaus[1]. Die Regelung zum Profiling wird so zum Innovationshemmnis.

[1] siehe David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017, Rz 7

Die Privatversicherer stehen für Transparenz und Vertraulichkeit im Umgang mit den Daten ihrer Kundinnen und Kunden ein. Beim Profiling sollte eine entsprechende Information genügen. Der Datenschutz wäre damit genügend gewährleistet.

– **Fokus auf angemessene Verwaltungssanktionen legen**

Im Sinne der Verhältnismässigkeit sollte das Strafrecht – als schärfstes Steuerungsinstrument des Staates – nur als «letztes Mittel» (ultima ratio) greifen. Zuvor sind andere Steuerungsinstrumente wie das Zivil- und Verwaltungsrecht auszuschöpfen. Wir sehen deshalb keine Notwendigkeit, neue Straftatbestände einzuführen und die Unternehmen dadurch ohne Not zu belasten. Der aktuelle Vorschlag – der massiv erweiterte Katalog der Strafbestimmungen gemäss VE-DSG – ist unverhältnismässig. Der Compliance- und Verwaltungsaufwand der Unternehmen würde exponentiell zunehmen, da sich die Verantwortlichen und ihre Mitarbeiterinnen und Mitarbeiter gegen die zahlreichen zusätzlichen strafrechtlichen Risiken absichern müssten. Das hemmt bzw. blockiert das unternehmerische Handeln unnötig und belastet die Standortattraktivität der Schweiz.

Wir unterstützen angemessene, griffige Sanktionen. Verwaltungssanktionen mit einer klaren institutionellen Trennung zwischen Untersuchungs- und Entscheidbehörde erachten wir als den besseren Weg.

– **Augenmass bei der Umsetzung von internationalen Verpflichtungen wahren**

Wir anerkennen, dass – unabhängig von der mit der Revision anvisierten Verbesserung des Schutzes der betroffenen Personen – aufgrund von internationalen Verpflichtungen der Schweiz eine Notwendigkeit zur Revision des DSG besteht. Dies betrifft das revidierte Übereinkommen Nr. 108 des Europarates sowie die einschlägigen Rechtsakte der EU.

Bei der Umsetzung dieser internationalen Verpflichtungen ist Zurückhaltung angebracht. Abzulehnen sind Bestimmungen, die das DSG über die internationalen Verpflichtungen hinaus verschärfen. So ist beispielsweise Art. 8 Ziffer 1 Bst. a des revidierten Europarats-Übereinkommens Nr. 108 bei der Übernahme ins Schweizer Recht auf das nötige Minimum zu limitieren. Online-Verträge (sog. automatisierte Entscheide i.S.v. Art. 15 VE-DSG) stellen z.B. keine wesentliche Bedrohung für die Privatsphäre dar. Sie rechtfertigen keine Anhörungspflicht.

– **Aufwand-Ertrag-Überlegungen Rechnung tragen**

Aufwand und Ertrag (Rechte der betroffenen Person, Vertrauen, Sicherheit) der Datenschutzmassnahmen müssen auch für die Wirtschaft in einem angemessenen Verhältnis stehen. Anliegen des Datenschutzes sind selten kostenneutral. So führen zusätzliche Pflichten der Unternehmen (wie z.B. ausufernde Informationspflichten oder eine Anhörungspflicht bei allen Online-Verträgen)

oder zusätzliche Strafbestimmungen – wie bereits erwähnt – zu einer Zunahme des Compliance- und Verwaltungsaufwandes und damit zu einer deutlichen Aufblähung der Kosten, die sich letztlich wieder in den Konsumentenpreisen (Versicherungsprämien) niederschlagen. Sie behindern die Geschäftstätigkeit, die Geschäftsentwicklung und die Zusammenarbeit mit Dritten.

In das neue DSG dürfen daher keine Bestimmungen aufgenommen werden, die für Unternehmen Aufwand bedeuten (mit Kostenfolge für die Kundinnen und Kunden), ohne nennenswerten Beitrag für die Privatsphäre zu leisten. Wir verweisen hierzu auf die Studie des Institutes für Versicherungswirtschaft der Universität St. Gallen, aus der hervorgeht, dass die Zahlungsbereitschaft der Kundinnen und Kunden für mehr Konsumentenschutz gering ist[2].

– **Sozialversicherungsgesetzgebung mit dem neuen DSG harmonisieren**

Das Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG) ist auf die Bedürfnisse der beruflichen Vorsorge zugeschnitten und hat sich bewährt. Das neue DSG darf zu keiner Verwässerung der datenschutzrechtlichen Spezialbestimmungen des BVG führen. Das Bearbeiten von Personendaten ist in der beruflichen Vorsorge unabdingbar. Deshalb ist im Rahmen der Harmonisierung zwischen dem neuen DSG und dem BVG sicherzustellen, dass die Abwicklung und Verwaltung dieses Versicherungszweigs weiterhin reibungslos und rationell erfolgen kann. Die Bearbeitung und Drittbearbeitung von Personendaten ist wie bis anhin vorzusehen. Zudem ist neu auch die Möglichkeit für automatisierte Einzelentscheidungen zu schaffen. Für die Analyse und Weiterentwicklung der beruflichen Vorsorge ist es unerlässlich, dass die vorhandenen Daten ausgewertet werden können. Analoges gilt für die Bundesgesetze über die Unfall- und die Krankenversicherung (UVG bzw. KVG).

2. Zentrale Anliegen im Detail

Wir verweisen auf Beilage 1, in der wir die Anträge und Ausführungen unter den entsprechenden Artikeln des VE-DSG und dem Anhang (Änderung anderer Erlasse) erläutern.

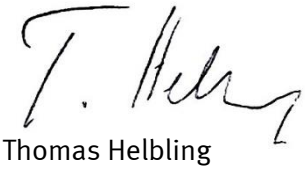
Das revidierte DSG wird in Verordnungen des Bundesrates konkretisiert. Da diese Verordnungen von grosser Tragweite sein werden, ersuchen wir Sie abschliessend, die Wirtschaft (als Gesetzes- bzw. Verordnungsadressat) in deren Erarbeitung miteinzubeziehen.

[2] vgl. «Konsumentenschutz aus Kundensicht», IVW Universität St. Gallen 2015, Seite 9

Wir danken Ihnen für die Berücksichtigung unserer Anträge und Vorschläge bei der weiteren Behandlung der Vorlage. Gerne stehen wir Ihnen für Rückfragen zur Verfügung. Wir sind auch gerne bereit, die Stellungnahme des SVV an einem Treffen zu erläutern.

Mit freundlichen Grüssen

Schweizerischer Versicherungsverband SVV



Thomas Helbling
Direktor

Franziska Streich
Leiterin Recht

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von **Beilage 1**

Name / Firma / Organisation : Schweizerischer Versicherungsverband

Abkürzung der Firma / Organisation : SVV

Adresse : Conrad-Ferdinand-Meyer-Strasse 14, Postfach, CH-8022 Zürich

Kontaktperson : Franziska Streich

Telefon : 044 208 28 63

E-Mail : franziska.streich@svv.ch

Datum : 24. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)					
Name/Firma	**Gesetz**	**Art.**	**Abs.**	**Bst.**	**Bemerkung/Anregung**
SVV	VE-DSG	3			**Begriffe: betrieblicher Datenschutzbeauftragter bzw. Datenschutzverantwortlicher**

					Antrag: Aufnahme einer Definition des betrieblichen Datenschutzbeauftragten bzw. des Datenschutzverantwortlichen in den Katalog von Art. 3 VE-DSG sowie Regelung des betrieblichen Datenschutzbeauftragten an geeigneter Stelle im neuen DSG im Sinne der nachfolgenden Ausführungen. Begründung: Im VE-DSG findet sich keine Bestimmung hinsichtlich eines Datenschutzverantwortlichen. Dies ist enttäuschend, denn die Thematik des Datenschutzverantwortlichen wurde im Normkonzept zur DSG-Revision eingehend diskutiert[1]. Beim Konzept des Datenschutzverantwortlichen handelt es sich um ein bewährtes Modell, welches daher auch im Rahmen der Totalrevision des DSG wieder integriert und berücksichtigt werden soll. Zudem steht dieses Modell im Einklang mit dem Zweck des Gesetzes, namentlich dem Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen. Die Bezeichnung eines Datenschutzverantwortlichen soll jedoch keine Verpflichtung darstellen, sondern eine Möglichkeit bieten (Grundsatz der Freiwilligkeit / keine Benachteiligung). Die Möglichkeit zur Bezeichnung eines Datenschutzverantwortlichen setzt positive Anreize zur Erreichung eines hohen Datenschutzniveaus und unterstützt gleichzeitig das Ziel der Totalrevision des DSG, die Selbstregulierung zu fördern. Von hoher Relevanz ist zudem die Unabhängigkeit des Datenschutzverantwortlichen. Es ist sicherzustellen, dass dieser seine Aufgaben und Pflichten in fachlicher Unabhängigkeit ausüben kann. Stellung und Aufgaben des Datenschutzverantwortlichen sind weiter vom Bundesrat auf Verordnungsstufe zu regeln. Unternehmen, welche die Möglichkeit zur Bezeichnung eines Datenschutzverantwortlichen nutzen, sollten im Gegenzug zu den entsprechenden Bemühungen von gewissen Entschärfungen und Vorteilen profitieren können (Beibehaltung des bewährten Bonusmodells). Bei der Entscheidung über die Verhängung einer Geldbusse und bei der Festsetzung deren Höhe sollte beispielsweise berücksichtigt werden, dass die Unternehmung organisatorische Massnahmen zwecks Gewährleistung eines hohen Daten-

[1] siehe Normkonzept, Seite 21/22 https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf

					schutzniveaus getroffen hat, insbesondere die Ernennung eines Datenschutzverantwortlichen. Art. 16 und 17 VE-DSG würden sich bestens eignen, die Funktionen des Datenschutzverantwortlichen mit einzubeziehen und allfällige Verpflichtungen aus Sicht des Verantwortlichen abzumildern (Bonusmodell).
SVV	VE-DSG	3			**Begriffe: Empfängerinnen und Empfänger / Dritte** An verschiedenen Stellen im VE-DSG wird der Begriff des Empfängers (siehe z.B. Art. 13, 19 oder 47 VE-DSG) und der Begriff des Dritten (siehe z.B. Art. 6, 12 oder 13 VE-DSG) verwendet. Es ist unklar, was der Unterschied zwischen Empfänger und Dritten sein soll. Der Begriff des Empfängers ist zu definieren und von dem des «Dritten» abzugrenzen, sofern er beibehalten wird.
SVV	VE-DSG	3		f.	**Begriffe: Profiling** Antrag: «f. Profiling: jede **automatisierte** Auswertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;» Begründung: Der Begriff «Profiling» wird in Art. 3 VE-DSG sehr breit definiert. Die Schweiz geht damit deutlich über die entsprechende Regelung der EU hinaus[2]. Der Begriff des Profilings sollte analog zur EU-DSGVO nur die automatisierte Auswertung von Personendaten umfassen. Der Geltungsbereich des DSG bezieht sich weiter nur auf Daten natürlicher Personen (Personendaten, siehe Art. 2 VE-DSG). Eine Erweiterung des Geltungsbereichs des DSG in Bezug auf das Profiling wird abgelehnt.
SVV	VE-DSG	4	6		**Grundsätze** Antrag:

[2] siehe David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017, Rz 7

					«[6] … Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen.» Begründung: Eine ausdrückliche Einwilligung für das Profiling – wie in Art. 4 Abs. 6 und 23 Abs. 2 Bst. b VE-DSG vorgesehen – ist nicht praktikabel. Zumal der Begriff «Profiling» im VE-DSG – wie bereits erwähnt – sehr breit definiert wird. Die Schweiz geht damit deutlich über die entsprechende Regelung der EU hinaus[3]. Die Regelung zum Profiling wird so zum Innovationshemmnis. Die Privatversicherer stehen für Transparenz und Vertraulichkeit im Umgang mit den Daten ihrer Kundinnen und Kunden ein. Beim Profiling sollte eine entsprechende Information genügen (z.B. durch Aufnahme einer entsprechenden Informationspflicht in den Katalog von Art. 13 VE-DSG). Der Datenschutz wäre damit genügend gewährleistet. Mit einer Information kann der Datenschutz genügend gewährleistet werden. Eine Information steht im Einklang mit dem Gebot zur Wahl der mildesten Massnahme. Die Informationspflicht sollte analog den Erläuterungen zum Art. 13 VE-DSG ohne Formerfordernis erfüllbar sein (siehe Seite 56 erläuternder Bericht). Beispielsweise müssen im Haftpflichtrecht im Schadenfall nicht nur die Daten der Versicherungsnehmer bearbeitet und ausgewertet werden, sondern auch diejenigen der Geschädigten. Zu denken ist z.B. an Auswertungen bei Strassenverkehrsunfällen, bei welchen die Daten der Fahrzeuge der Versicherungsnehmer sowie der Geschädigten ausgewertet werden. Die Einholung einer Einwilligung bei der geschädigten Person würde einen zusätzlichen Prozess erfordern, der die Schadenbearbeitung unnötig verkompliziert und die Schadenregulierung verzögern oder gar verunmöglichen könnte (falls der Geschädigte seine Einwilligung nicht geben würde).
SVV	VE-DSG	5	5		**Bekanntgabe ins Ausland**

[3] siehe David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017, Rz 7

					Antrag: «[5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens ~~sechs Monate~~ **30 Tage** nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht.» Begründung: Eine Frist von sechs Monaten ist für Unternehmen zu lange und nicht praktikabel. Wenn ein Unternehmen nach Vertragsabschluss bis zu einem halben Jahr warten muss, bevor mit dem Projekt fortgefahren werden kann, behindert dies die Geschäfte stark und kann vor allem für kleinere Unternehmen verheerende Auswirkungen haben.
SVV	VE-DSG	5	6		**Bekanntgabe ins Ausland** Antrag: Streichen von Art. 5 Abs. 6 VE-DSG Begründung: Der Aufwand ist unangemessen. Bei Verwendung von «Model-Clauses» resultiert kein weiterer Nutzen bei einer Information des EDÖB (bspw. zusätzlicher Schutz des Betroffenen). Im Übrigen gibt es keine entsprechende Pflicht in der EU-DSGVO (siehe insbesondere bei Art. 46 EU-DSGVO).
SVV	VE-DSG	6	1	b.	**Bekanntgabe ins Ausland in Ausnahmefällen** Die Bearbeitung im Zusammenhang mit Verträgen sollte analog der EU-DSGVO auch Datenbearbeitungen erfassen, welche lediglich im Interesse der betroffenen Person abgeschlossen oder sonst in die Vertragsabwicklung involviert sind und nicht nur die Bearbeitung von Daten des Vertragspartners selbst.
SVV	VE-DSG	6	2		**Bekanntgabe ins Ausland in Ausnahmefällen**

					Antrag: Streichen von Art. 6 Abs. 2 VE-DSG Begründung: Wir verweisen auf die Überlegungen wie hinsichtlich Art. 5 Abs. 6 VE-DSG.
SVV	VE-DSG	7	3		**Auftragsdatenbearbeitung** Antrag: «[3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger ~~schriftlicher~~ Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen.» Begründung: Im Zeitalter von komplexen Dienstleistungsverhältnissen – wie z.B. Cloud-Computing – ist es nicht praxistauglich, wenn in jedem Einzelfall für den Beizug von Subunternehmern eine schriftliche Zustimmung eingeholt werden muss. Ausserdem bleibt das Grundprinzip, wonach der Verantwortliche für die Sicherstellung des Datenschutzes verantwortlich ist, auch unter dem revidierten DSG unverändert. Daher sollte das DSG im Zeitalter des E-Commerce keine Vorgaben zum Formerfordernis bei der Zustimmung machen und dies der Parteiautonomie überlassen. Die Versicherer unterstehen notabene – im Gegensatz zu anderen Branchen – auch im Bereich Outsourcing der Aufsicht der Finma (Art. 4 Abs. 2 Bst. j und Art. 5 VAG). Es kann zudem verwiesen werden auf Art. 70 Abs. 3 UVG, der für das Outsourcing der Schadenerledigung die Genehmigung der Finma bzw. des BAG verlangt.
SVV	VE-DSG	8	1-3		**Empfehlungen der guten Praxis** Antrag: «[1] Der Beauftragte erarbeitet **unverbindliche** Empfehlungen der guten Praxis, welche die Datenschutz-

					vorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs. ~~sowie den Schutz von besonders schutzbedürftigen Personen. Er~~ **Der Beauftragte** veröffentlicht die von ihm erarbeiteten ~~sowie die von ihm genehmigten~~ Empfehlungen der guten Praxis. [2] Der Verantwortliche sowie interessierte Kreise können ~~die Empfehlungen des Beauftragten ergänzen oder~~ eigene~~n~~ Empfehlungen der guten Praxis ausarbeiten. Sie können **bei der Erarbeitung den Beauftragten konsultieren**. ~~ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie.~~ [3] Streichen des Absatzes und stattdessen Regelung in Absatz 1 (ohne die Genehmigung). <u>Begründung</u>: Die Abänderung des Absatzes 1 beabsichtigt einen stärkeren Einbezug der Verantwortlichen, um so dem Gedanken der Selbstregulierung mehr Rechnung zu tragen. Weiter soll die Regelung nicht dazu führen, dass der Beauftragte Kompetenzen erhält, die ihn in die Nähe des Gesetzgebers rücken. Eine Rechtssetzungskompetenz des Beauftragten wäre rechtsstaatlich bedenklich. Der Begriff «schutzbedürftige Personen» ist an dieser Stelle systemfremd, da es in diesem Kontext um besonders schützenswerte Personendaten geht. Die Berücksichtigung der Besonderheiten des jeweiligen Anwendungsbereichs trägt dem bereits in genügender Weise Rechnung. Die Änderungen des Absatzes 2 ist aus Gründen der Rechtssicherheit geboten, weil unklar ist, was die konkreten Folgen der vorgesehenen Genehmigung wären. Absatz 3 wurde ans Ende von Absatz 1 verschoben, weil dort ein sachlicher Bezug besteht. Die Streichung des Begriffes «Genehmigung» erfolgt aufgrund der Änderungen an Absatz 2.
SVV	VE-DSG	9	1-2		**Einhaltung der Empfehlungen der guten Praxis** <u>Antrag</u>: Streichen von Art. 9 VE-DSG

					Begründung: Es wird auf die Begründung der Änderungen von Art. 8 Absätze 2 und 3 VE-DSG verwiesen. Im Übrigen würden diese Bestimmung faktisch zu einer sachlich nicht gerechtfertigten Benachteiligung von Verantwortlichen führen, welche sich dazu entschliessen, die Compliance mit dem DSG auf andere Art und Weise als durch die Befolgung solcher Empfehlungen sicherzustellen (insbesondere KMUs), weil Art. 9 in diesem Fall bis zu einem gewissen Grad zu einer «Beweislastumkehr» führen würde.
SVV	VE-DSG	11	1		**Sicherheit von Personendaten** Antrag: «[1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch **dem betreffenden Risiko** angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden.» Begründung: Der VE-DSG lässt offen, wie weit die technischen und organisatorischen Massnahmen gehen müssen. Lediglich der Begriff «angemessen» lässt erahnen, dass eine Abwägung zwischen Aufwand und Risiko (wesentliche Bedrohungen für die Privatsphäre) vorgenommen werden soll. Im neuen DSG ist hier – in Übereinstimmung mit Art. 32 Abs. 1 EU-DSGVO – ein risikobasierter Ansatz zu wählen, zumal technische Schutzmassnahmen sehr kostspielig sein können. Es wäre unverhältnismässig, für alle Datenbearbeitungen die gleichen technischen Schutzmassnahmen vorzusehen.
SVV	VE-DSG	12	1-5		**Daten einer verstorbenen Person** Antrag: Streichen von Art. 12 VE-DSG Begründung:

					Die Regelung wurde bislang in der Verordnung zum DSG (Art. 1 Abs. 7) grob umrissen. Sie hat jedoch nichts mit datenschutzrechtlichen Problemstellungen zu tun. Der SVV schlägt vor, die Regelung an anderer Stelle aufzunehmen (z.B. im ZGB/Personenrecht).
SVV	VE-DSG	13	4		**Informationspflicht bei der Nutzung von Auftragsbearbeitern** Antrag: Streichen von Art. 13 Abs. 4 VE-DSG sowie der mit dieser Bestimmung verbundenen Strafbestimmung Begründung: Eine Informationspflicht zur Identität und den Kontaktdaten sämtlicher Auftragsbearbeiter wird abgelehnt. Ausgangspunkt des Datenschutzgesetzes ist der – im Zusammenhang mit Datenbearbeitungen durch den Staat – verfassungsrechtlich garantierte Schutz der Privatsphäre und der Schutz vor Datenmissbrauch (Art. 13 Bundesverfassung). Gestützt auf diesen verfassungsrechtlichen Ausgangspunkt appellieren wir, den Fokus der Revision auf wesentliche Bedrohungen für die Privatsphäre zu legen. Deshalb lehnen wir ausufernde Informationspflichten – wie z.B. in Art. 13 Abs. 4 VE-DSG vorgesehen – entschieden ab. Solche Informationspflichten sind auch aus Kosten-Nutzen-Überlegungen nicht akzeptabel: – Seitens Unternehmen führt eine solche Informationspflicht zweifelsohne zu einer enormen Zunahme des Compliance- und Verwaltungsaufwandes mit Kostenfolge für die Kundinnen und Kunden. Beispielsweise sind bei Versicherungsgesellschaften je nach Bereich zahlreiche Auftragsbearbeiter involviert (z.B. externe Anwaltskanzleien, externe Experten zur Beurteilung von Schadenfällen, wie z.B. Ingenieure, Architekten, Treuhänder, etc.). Hinzu kommt, dass Auftragsbearbeiter wechseln können und grosse Auftragsbearbeiter – wie z.B. das Cloud-Computing-Unternehmen «Salesforce» – eine grosse Anzahl von Subakkordanten einsetzen, die auch von dieser Informationspflicht erfasst wären. – Ein Nutzen für die Kundinnen und Kunden ist nicht erkennbar und im erläuternden Bericht nicht ausgewiesen. Informationspflichten, die über Wesentliches hinausgehen, bewirken keinen nen-

					nenswerten Beitrag zur Privatsphäre, sondern stiften eher Verwirrung. Es besteht die Gefahr, dass Wichtiges neben Unwichtigem untergeht. Eine Offenlegung der Identität und Kontaktdaten der Auftragsbearbeiter gegenüber den Kunden ist schliesslich auch wegen Geschäftsgeheimnissen kritisch. Es gibt diesbezüglich auch keine Vorgabe im revidierten Übereinkommen Nr. 108 des Europarates (siehe Art. 7bis E-SEV 108). Die Informationspflicht betr. Identität und Kontaktdaten der Auftragsbearbeiter ist strafbewehrt (siehe Art. 50 Abs. 1 Bst. b Ziffer 2 und Abs. 4 VE-DSG), sowohl die vorsätzliche wie auch die fahrlässige Verletzung wird strafrechtlich geahndet. Ein Rückgriff auf die Ausnahmen gemäss Art. 14 VE-DSG ist angesichts der Strafandrohung viel zu unsicher.
SVV	VE-DSG	13	5		**Informationspflicht bei der Beschaffung von Personendaten** <u>Antrag</u>: Streichen von Art. 13 Abs. 5 VE-DSG sowie der mit dieser Bestimmung verbundenen Strafbestimmung <u>Begründung</u>: Wir verweisen auf die Ausführungen unter Art. 13 Abs. 4 VE-DSG. Aus den dort genannten Gründen wird auch eine Informationspflicht bei der Beschaffung von Daten bei Dritten abgelehnt. Eine solche Informationspflicht ist nicht praxistauglich. Sie wäre mit einem unverhältnismässigen Aufwand (mit Kostenfolge für Kundinnen und Kunden) verbunden, ohne einen nennenswerten Beitrag für deren Privatsphäre zu leisten. Auch diese Informationspflicht ist strafbewehrt (siehe Art. 50 Abs. 1 Bst. b Ziffer 1 und Abs. 4 VE-DSG), sowohl die vorsätzliche wie auch die fahrlässige Verletzung wird strafrechtlich geahndet. Ein Rückgriff auf die Ausnahmen gemäss Art. 14 VE-DSG ist auch hier angesichts der Strafandrohung viel zu unsicher.
SVV	VE-DSG	14	3	a	**Ausnahmen von der Informationspflicht und Einschränkungen**

					Antrag: «a. ein Gesetz im formellen Sinn **oder ein Vertrag** dies vorsieht; oder» Begründung: In gewissen Konstellationen kann der Verantwortliche verpflichtet sein, Informationen von Drittpersonen einzuholen und darf diese nicht an die betroffene Person weitergeben. Aufgrund des Vertrages mit dem Versicherungsnehmer sind die Versicherer beispielsweise im Haftpflichtrecht an eine gewisse Geheimhaltung gebunden. Um einen Schadenfall des Versicherungsnehmers zu behandeln, sind die Versicherer gezwungen, sowohl Daten des Versicherungsnehmers wie auch des Geschädigten zu bearbeiten. Diese Daten lassen sich nicht immer strikte trennen und auseinanderhalten. Falls die Versicherer immer alle betroffenen Personen darüber informieren müssten, wären sie unter Umständen gezwungen, den Versicherungsvertrag mit dem Versicherungsnehmer zu verletzen.
SVV	VE-DSG	14	4	a	**Ausnahmen von der Informationspflicht und Einschränkungen** Antrag: «a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern ~~und er die Personendaten nicht Dritten bekannt gibt~~;» Begründung: Die konzerninterne Weitergabe von Daten stellt eine Bekanntgabe von Daten an Dritte dar. Die Einschränkung der Informationspflicht muss gewährleistet sein und darf beispielsweise durch Weitergabe / Bekanntgabe innerhalb der Konzerngesellschaften (Dritte) nicht vereitelt werden. Die Einschränkung der Informationspflicht muss aufgrund überwiegender privater Interessen möglich bleiben.
SVV	VE-DSG	15	1–3		**Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung** Antrag: Strikte Limitierung/Streichung der Informations- und Anhörungspflicht bei der Umsetzung von Art. 8 Zif-

					fer 1 Bst. a E-SEV 108 in das neue DSG Begründung: Wie bereits unter Art. 13 Abs. 4 VE-DSG erläutert, appellieren wir gestützt auf den verfassungsrechtlichen Ausgangspunkt des Datenschutzgesetzes, den Fokus der Revision auf wesentliche Bedrohungen für die Privatsphäre zu legen. Art. 8 Ziffer 1 Bst. a E-SEV 108 ist deshalb bei der Übernahme ins DSG auf das nötige Minimum zu limitieren. Alle Verträge haben rechtliche Wirkungen. Sie begründen Rechte und Pflichten der Vertragsparteien – so auch Online-Verträge, wie z.B. eine Online-Reiseversicherung oder eine Bestellung bei coopathome. Verträge werden im Zeitalter des E-Commerce elektronisch abgeschlossen. Ein Online-Abschluss stellt keine wesentliche Bedrohung für die Privatsphäre dar, sondern vereinfacht das Prozedere sowohl für die Unternehmen wie auch für die Kundinnen und Kunden. Gestützt auf das Alternativerfordernis der rechtlichen Wirkungen in Art. 15 Abs. 1 VE-DSG würden alle Online-Verträge einer Informations- und Anhörungspflicht unterstehen. Dies ist nicht nachvollziehbar und wird abgelehnt. Notabene geht der VE-DSG mit dem Alternativerfordernis der rechtlichen Wirkungen über die Vorgabe von Art. 8 Ziffer 1 Bst. a E-SEV 108 hinaus.
SVV	VE-DSG	16	1		**Datenschutz-Folgenabschätzung** Antrag: – «[1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem ~~erhöhten~~ **hohen** Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen.» – Streichen der mit der Bestimmung verbundenen Strafbestimmung Begründung: Gemäss dem erläuternden Bericht ist grundsätzlich dann von einem erhöhten Risiko auszugehen, wenn die spezifischen Eigenschaften der geplanten Datenbearbeitung darauf schliessen lassen, dass die Ver-

					fügungsfreiheit der betroffenen Personen über ihre Daten erheblich eingeschränkt wird oder werden kann. Der Anwendungsbereich ist damit unklar bzw. (zu) weit. Analog der Regelung in der EU-DSGVO ist «erhöhtes Risiko» durch «hohes Risiko» zu ersetzen und damit die Schwelle für eine Datenschutz-Folgenabschätzung entsprechend zu erhöhen. Im Weiteren ist die mit dieser Bestimmung verbundene Strafbestimmung zu streichen.
SVV	VE-DSG	16	3		**Datenschutz-Folgenabschätzung** Antrag: Streichen von Art. 16 Abs. 3 VE-DSG sowie der mit dieser Bestimmung verbundenen Strafbestimmungen Begründung: Die Bestimmung ist zu streichen. Eine Benachrichtigung des EDÖB wird durch den E-SEV 108 nicht vorgeschrieben (siehe Art. 8bis Abs. 2 E-SEV 108).
SVV	VE-DSG	16	4		**Datenschutz-Folgenabschätzung** Antrag: Streichen von Art. 16 Abs. 4 VE-DSG Begründung: Wir verweisen auf den Antrag und die Begründung betreffend Art. 16 Abs. 3 VE-DSG (logische Folge des Streichungsantrags für Art. 16 Abs. 3 VE-DSG).
SVV	VE-DSG	17	1		**Meldung von Verletzungen des Datenschutzes** Antrag: «[1] Der Verantwortliche meldet dem Beauftragten ~~unverzüglich~~ **ohne unnötigen Verzug** einen **n** ~~unbefugte Datenbearbeitung oder den Verlust von Daten~~ **Sicherheitsverstoss**, es sei denn die Verletzung des

					Datenschutzes führt voraussichtlich nicht zu einem **hohem** Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.» Begründung: Die vorliegende Meldepflicht geht weiter, als in den europäischen Regelungen vorgesehen und wird ausgedehnt auf jegliche Datenschutzverletzung. Analog den europäischen Regelungen sollte die Meldepflicht strikt auf Verstösse gegen die Datensicherheit limitiert werden (siehe Art. 7 Ziff. 2 E-SEV 108, Art. 33 i.V.m. Art. 4 Ziff. 12 EU-DSGVO). Eine Meldung sollte zudem ohne unnötigen Verzug erfolgen und damit erst nachdem die Hintergründe und Auswirkungen eines Data Breaches geprüft wurden. Im Weiteren ist die mit dieser Bestimmung verbundene Strafbestimmung zu streichen. Ohne eine Anpassung gäbe es eine immense Menge von Meldungen an den Beauftragten, da jede falsch gesendete Mail mit Personendaten gemeldet werden würde, um Sanktionen zu vermeiden, da die Formulierung «voraussichtlich nicht zu einem Risiko» sehr unbestimmt ist. Der Beauftragte hätte einen unverhältnismässig grossen (kaum gewollten) Aufwand, um all diese Meldungen zu bearbeiten. Zudem ist eine Pflicht zur Selbstanzeige, wie sie hier eingeführt werden soll, dem schweizerischen Rechtssystem fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien. Weshalb der Bereich des Datenschutzes hier eine Ausnahme darstellen soll, ist insbesondere auch deshalb nicht ersichtlich, da der Beauftragte seinerseits gemäss Art. 45 VE-DSG verpflichtet ist, strafbare Handlungen anzuzeigen.
SVV	VE-DSG	19		b.	**Weitere Pflichten** Antrag: Streichen von Art. 19 Bst. b VE-DSG sowie der mit dieser Bestimmung verbundenen Strafbestimmungen Begründung: Wir verweisen auf die Ausführungen unter Art. 13 Abs. 4 VE-DSG. Aus den dort genannten Gründen

					wird auch die hier vorgesehene Informationspflicht abgelehnt. Art. 19 Bst. b VE-DSG ist in der Praxis nicht umsetzbar. Denn es ist nicht möglich, jederzeit sämtliche Empfängerinnen und Empfänger über sämtliche in der Bestimmung erwähnten Schritte (Berichtigung, Löschung oder Vernichtung von Daten, etc.) zu informieren. Bereits der Initialaufwand in den Unternehmen zur Aufsetzung der notwendigen Prozesse muss als absolut unverhältnismässig bezeichnet werden. Wenn die Unternehmen neu verpflichtet würden, die Empfängerinnen und Empfänger von Personendaten über die in Art. 19 Bst. b VE-DSG aufgeführten Schritte zu informieren, wären sie gezwungen, unzählige umfangreiche Prozesse mit einem völlig unverhältnismässigen und äusserst kostspieligen Aufwand aufzusetzen. In gewissen Fällen ist eine Informationspflicht schlichtweg sinnlos, beispielsweise, wenn Personendaten gelöscht werden, weil sie nicht mehr benötigt werden. Gleichzeitig bringt eine Informationsflicht in diesen Fällen auch keinen Mehrwert für den Datenschutz. Eine Informationspflicht, wie in Art. 19 Bst. b VE-DSG vorgesehen, wird notabene durch den E-SEV 108 nicht vorgeschrieben (siehe Seite 65 erläuternder Bericht).
SVV	VE-DSG	20	2	g.	**Auskunftspflicht an Betroffene bei Nutzung von Auftragsbearbeitern** <u>Antrag</u>: «gegebenenfalls die Informationen **nach Artikel 13 Abs. 3.**» <u>Begründung</u>: Wir verweisen auf den Antrag und die Begründung betreffend Art. 13 Abs. 4 VE-DSG. Dementsprechend ist in Bezug auf Art. 20 Abs. 2 Bst. g VE-DSG eine Anpassung nötig.
SVV	VE-DSG	20	3		**Auskunftspflicht bei einer Entscheidung aufgrund einer Datenbearbeitung** <u>Antrag:</u> Streichen von Art. 20 Abs. 3 VE-DSG sowie der mit dieser Bestimmung verbundenen Strafbestimmungen

					Begründung: Eine Auskunftspflicht bzw. «Rechenschaftspflicht» bezüglich Entscheiden, wie dies in Art. 20 Abs. 3 VE-DSG vorgeschlagen wird, ist nicht im Sinne einer liberalen Marktwirtschaft und wird abgelehnt. Die Transparenz betr. automatisierte Einzelentscheidungen ist bereits ausreichend im neuen Art 15 Abs. 1 VE-DSG geregelt. Dadurch erfährt der Kunde, bei welchen Vorgängen automatisierte Einzelfallentscheide getroffen werden. Er kann dann mittels dem Auskunftsrecht gemäss Art. 20 Abs. 1 und 2 VE-DSG überprüfen, ob die über ihn bei einem Unternehmen vorhandenen Daten richtig sind und der automatisierte Entscheid auf einer richtigen Datenbasis getroffen wurde. Eine weitergehende Informations- bzw. Auskunftspflicht in Bezug auf automatisierte Einzelfallentscheidungen stellt eine Überregulierung dar und wird abgelehnt. Hinzu kommt, dass beispielsweise Informationen zum Zustandekommen eines Entscheids dem Geschäftsgeheimnis des Verantwortlichen unterliegen. So unterliegen im Versicherungsbereich die Bestandteile einer Prämienkalkulation dem Geschäftsgeheimnis der Versicherungsgesellschaften. Eine diesbezügliche Offenlegungspflicht für Unternehmen wäre auch kartellrechtlich problematisch. Beispielsweise müsste ein Versicherungsunternehmen auf Anfrage über alle Prämienbestandteile (wie unter anderem Risikoprämie, Risikozuschlag, Verwaltungskosten, etc.) und deren Berechnungsfaktoren inkl. verwendete Algorithmen Auskunft geben und damit faktisch Geschäftsgeheimnisse auch gegenüber möglichen Wettbewerbern offenlegen. Eine Auskunftspflicht, wie in Art. 20 Abs. 3 VE-DSG vorgesehen, wird notabene durch E-SEV 108 nicht vorgeschrieben (siehe Seite 66/67 erläuternder Bericht).
SVV	VE-DSG	23	2	d.	**Persönlichkeitsverletzungen** Antrag: «d. durch Profiling ohne ~~ausdrückliche Einwilligung~~ **Information** der betroffenen Person.»

					Begründung: Wir verweisen auf die Ausführungen zum Art. 4 Abs. 6 VE-DSG. Es muss den Unternehmen beispielsweise weiterhin möglich sein, Angaben von Kundinnen und Kunden bei Bedarf über öffentlich zugängliche Quellen – das Internet/Social Media – zu verifizieren. Es wäre unverhältnismässig, wenn die Unternehmen zwecks Plausibilisierung von Angaben der betroffenen Person im Internet jeweils deren ausdrückliche Einwilligung einholen müssten.
SVV	VE-DSG	24	2		**Rechtfertigungsgründe** Antrag: «Ein überwiegendes Interesse der bearbeitenden Person ~~ist möglicherweise gegeben, wenn dieser insbesondere~~ **fällt insbesondere in Betracht, wenn diese**:» Begründung: Der SVV beantragt die Beibehaltung des geltenden Rechts. Es gibt keinen Anlass, das geltende Recht (Art. 13 Abs. 2 DSG) zu ändern. Ein solcher lässt sich auch dem Erläuternden Bericht nicht entnehmen. Es fehlt darin eine Analyse / Begründung für die vorgeschlagene Änderung (siehe Seite 69 erläuternder Bericht). Der neu eingeschobene Ausdruck «möglicherweise» schafft zudem grosse Rechtsunsicherheit.
SVV	VE-DSG	24	2	a	**Rechtfertigungsgründe** Art. 24 Abs. 2 Bst. a VE-DSG sollte auch die Bearbeitung von Daten weiterer, in den Vertrag involvierter Personen umfassen, wie z.B. Begünstigte eines Lebensversicherungsvertrags.
SVV	VE-DSG	27	2		**Rechtsgrundlagen** Antrag: «[2] Für die Bearbeitung besonders schützenswerter Personendaten~~, das Profiling oder den Erlass einer automatisierten Einzelfallentscheidung nach Art. 15 Abs.1~~ ist eine Grundlage in einem Gesetz im formel-

					len Sinn erforderlich». <u>Begründung:</u> Beim Erlass einer automatisierten Einzelfallentscheidung wie auch beim Profiling ist das Vorhandensein einer Grundlage in einem Gesetz im formellen Sinn zu verzichten. Vielmehr haben sie immer dann als zulässig zu gelten, soweit sie vom Sinn und Zweck des Gesetzes als gedeckt betrachtet werden können. Das Fordern einer expliziten Grundlage in einem Gesetz im formellen Sinn für automatisierte Einzelfallentscheide/Profiling ist praxisfremd und gesetzgebungstechnisch kaum befriedigend umsetzbar. Vielmehr müssen alle automatisierten Einzelfallentscheidungen/Profiling automatisch als zulässig gelten, wenn sie der Durchführung/Abwicklung des Versicherungsvertrages dienen. Mithin darf einzig der datenschutzrechtliche Grundsatz der Zweckbindung die Zulässigkeit der Bearbeitungsarten bestimmen. <u>Beispiel:</u> Die Identifikation und Bearbeitung von Hoch- und Höchstkostenfällen bedingt, dass Kranken-/ Unfallversicherer ihren Datenbestand unter Anwendung eines einschlägigen Regelwerks bearbeiten dürfen. Die Zulässigkeit der Durchführung eines Case Managements dürfte ebenso unbestritten sein wie das Faktum, dass Case Management einen wichtigen Beitrag zur Reduktion der Kranken- und Unfallversicherungskosten leistet. Dennoch enthält das KVG/UVG bereits heute nicht eine einzige gesetzliche Bestimmung über Case Management. Die effiziente Abwicklung des Kranken-/ Unfallversicherungsgeschäfts als Massengeschäft bedingt einen sehr hohen Automatisierungsgrad. Die Leistungsprüfung erfolgt damit zu einem sehr hohen Anteil vollautomatisch anhand vordefinierter Regelwerke. Das KVG/UVG enthält jedoch keine entsprechenden Grundlagen.
SVV	VE-DSG	41 ff.			**Verwaltungsverfahren** Der SVV steht ein für angemessene, griffige Sanktionen. Wir sind aber der Ansicht, dass Verwaltungssanktionen mit einer klaren institutionellen Trennung zwischen Untersuchungsbehörde (der Beauftragte) und Entscheidbehörde (einer noch zu schaffenden Behörde) der bessere Weg sind.
SVV	VE-DSG	44	3		**Verfahren**

					Antrag: «[3] Beschwerden gegen vorsorgliche Massnahmen nach Art. 42 kommt ~~keine~~ aufschiebende Wirkung zu.» Begründung: Im Verwaltungsverfahren hat eine Beschwerde gegen vorsorgliche Massnahmen grundsätzlich aufschiebende Wirkung (vgl. Art. 55 Abs. 1 VwVG). Die aufschiebende Wirkung einer allfälligen Beschwerde kann indessen von der zuständigen Behörde im Einzelfall entzogen werden (Art. 55 Abs. 2 VwVG). Es besteht kein Anlass, von dieser Regelung in Bezug auf datenschutzrechtliche Verfahren abzuweichen. Im Erläuternden Bericht fehlt eine Analyse / Begründung für einen generellen Ausschluss der aufschiebenden Wirkung (siehe Seite 80 Erläuternder Bericht). Ein Ausschluss der aufschiebenden Wirkung von Gesetzes wegen kann in der Praxis erhebliche Konsequenzen nach sich ziehen. Insbesondere wenn dadurch Kernsysteme für unbestimmte Dauer nicht mehr verwendet werden können, liegt der Geschäftsbetrieb als Ganzes darnieder. Auch in Bezug auf datenschutzrechtliche Verfahren muss – wie in Art. 55 VwVG vorgesehen – eine Beurteilung im Einzelfall bzw. die Möglichkeit zur Beantragung einer aufschiebenden Wirkung möglich sein. Konkurrenten könnten zudem die Praxis weiter so handhaben, das betroffene Unternehmen jedoch nicht (da keine aufschiebende Wirkung).
SVV	VE-DSG	45			**Anzeigepflicht des EDÖB** Antrag: «Art. 45 ~~Anzeigeflicht~~ **Anzeige von Verletzungen der Datenschutzbestimmungen** ~~Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.~~ **Der Beauftragte kann Verletzungen der Datenschutzbestimmungen den Strafverfolgungsbehör-**

					den mitteilen. Begründung: Die Bestimmung ist in Zusammenhang mit Art. 50 Abs. 2 VE-DSG zu sehen. Wie im erläuternden Bericht zum VE-DSG ausgeführt wird, sehen die Richtlinie der EU 2016/680 sowie Art. 12bis Abs. 1 Bst. d E-SEV 108 vor, dass die Aufsichtsbehörde Verletzungen der Datenschutzbestimmungen den zuständigen Justizbehörden zur Kenntnis bringen darf. Die EU-Datenschutz-Grundverordnung sieht in Art. 58 Abs. 5 eine analoge Regelung vor. Von einer Verpflichtung zur Meldung ist in den europäischen Regelungen keine Rede (Richtlinie, E-SEV 108). Es ist nicht nachvollziehbar, weshalb im revidierten DSG eine Regelung verankert werden soll, die über diejenige auf europäischer Ebene hinausgeht, nur damit in Abweichung von Art. 22a Bundespersonalgesetz die Anzeigepflicht des EDÖB auf Übertretungen ausgedehnt werden kann. Der Beauftragte ist aufgrund von Art. 22a BPG nämlich «nur» verpflichtet, Verbrechen oder Vergehen den Strafverfolgungsbehörden anzuzeigen.
SVV	VE-DSG	50			**Strafbestimmungen Art. 50-55 VE-DSG** Aufgrund des Grundsatzes der Verhältnismässigkeit sollte das Strafrecht – als schärfestes Steuerungsinstrument des Staates – nur als «letztes Mittel» (ultima ratio) greifen. Zuvor sind andere Steuerungsinstrumente wie das Zivil- und Verwaltungsrecht auszuschöpfen. Der SVV sieht deshalb grundsätzlich keine Notwendigkeit, neue Straftatbestände einzuführen und die Unternehmen dadurch ohne Not zu belasten. Der aktuelle Vorschlag – der massiv erweiterte Katalog der Strafbestimmungen gemäss VE-DSG – ist unverhältnismässig. Der Compliance- und Verwaltungsaufwand der Unternehmen würde exponentiell zunehmen, da sich die Verantwortlichen und ihre Mitarbeitenden gegen die massiv erweiterten strafrechtliche Risiken entsprechend absichern müssten. Das hemmt bzw. blockiert das unternehmerische Handeln unnötig und belastet die Standortattraktivität der Schweiz. Der SVV steht ein für angemessene, griffige Sanktionen. Der aktuelle Vorschlag ist jedoch nur schädlich und behindert die Geschäftstätigkeit der Unternehmen. Wir sind der Ansicht, dass Verwaltungssanktio-

					nen mit einer klaren institutionellen Trennung zwischen Untersuchungs- und Entscheidbehörde der bessere Weg sind. In diesem Sinne sind die Strafbestimmungen dringend zu überarbeiten: – Sie sollten sich gegen die juristischen Personen richten (unter Vorbehalt von vorsätzlich kriminellen Machenschaften von Mitarbeitern, wie z.B. Datendiebstahl). – Es darf nur die vorsätzliche Begehung mit Strafe bedroht werden (keine Fahrlässigkeitstatbestände). – Der Katalog der strafbewehrten Pflichten ist zu überarbeiten. Der SVV sieht keine Notwendigkeit, neue Straftatbestände einzuführen.
SVV	VE-DSG	52			Antrag: Streichen von Art. 52 VE-DSG Begründung: Die Bestimmung ist viel zu offen und unbestimmt formuliert. Sie steht darüber hinaus im falschen Gesetz. Sie gehört ins StGB und nicht ins DSG. Für die Mitarbeitenden der Sozialversicherungen bringt sie grosse Rechtsunsicherheit mit sich. Eine Verschärfung ist zudem nicht nötig, da die Verletzung dieser Pflicht durch die neue Bestimmung von Art. 54 Abs. 1 Bst. d KVAG mit Bussen bis CHF 500'000 bereits heute scharf sanktioniert ist. Dem erläuternden Bericht zum Vorentwurf ist zu entnehmen, dass Art. 52 VE-DSG zum Ziel hat, die Schweigepflicht auch auf Berufe auszudehnen, die nicht unter Art. 321 StGB fallen, «für deren Ausübung der Schutz der Vertraulichkeit aber ebenfalls unerlässlich ist». Der Geheimnisschutz soll auf alle Arten von Personendaten ausgedehnt werden (vgl. Seite 86 erläuternder Bericht). Im Bereich der Sozialversicherungen besteht mit Art. 33 ebenfalls eine Schweigepflicht. Es besteht damit die Gefahr, dass die viel zu offene Formulierung von Art. 52 VE-DSG damit die Sozialversicherungen mitumfassen könnte.
SVV	VE-DSG	59			**Übergangsbestimmung**

					Antrag: – Es ist eine allgemeingültige Übergangsbestimmung für die Umsetzung des revidierten DSG aufzunehmen (keine Beschränkung auf einzelnen Bestimmungen). Es ist eine angemessene Übergangsfrist für Umsetzung des revidierten DSG von fünf Jahren vorzusehen. – Keine Rückwirkung oder beschränkte Rückwirkung der neuen Bestimmungen. Begründung: Die Vernehmlassungsvorlage sieht keine umfassende Übergangsbestimmung vor. Die neuen und revidierten Bestimmungen des DSG werden die Prozesse der Versicherungsgesellschaften bedeutend beeinflussen – etwa in der Produkteentwicklung, bei Kundendokumenten / Versicherungsbedingungen, beim Vertragsmanagement, im Kundenservice, beim Schadenmanagement, in der Betrugserkennung, bei der Ausbildung und im Vertrieb. Eine Übergangsbestimmung ist deshalb zwingend aufzunehmen.
Anhang (Art. 58)					
SVV	12. IPRG	139	3		Antrag: «[3] Absatz 1 ist auch anwendbar auf Ansprüche aus Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten sowie aus Beeinträchtigung des Rechts auf Auskunft über Personendaten. **Dabei kann ein ausländischer Erfolgsort im Sinne von Absatz 1 Buchstabe c nicht allein damit begründet werden, dass die Daten im betreffenden Land gespeichert sind.**» Begründung: Im Rahmen der DSG-Revision sollte auch Art. 139 Abs. 3 IPRG, der die Anwendbarkeit des DSG im internationalen Verhältnis regelt, angepasst werden. Wegen dem weit gehenden Recht des Geschädigten, das anwendbare Recht gemäss Art. 139 Abs. 1 IPRG zu wählen, sind Schweizer Verantwortliche andernfalls auch in Konstellationen potentiell der Datenschutz-Grundverordnung der EU (EU-DSGVO) unterworfen, in denen sich die EU-DSGVO trotz ihren extraterritorialen Bestimmungen (Art. 3) für nicht anwendbar erklärt. Ohne Änderungen würde das IPRG damit zu einer weitergehenden extra-territorialen

					Anwendbarkeit der EU-DSGVO auf ausländische Verantwortliche führen als dies gemäss den weitgehenden betreffenden Bestimmungen der EU-DSGVO selbst der Fall ist. Gleiches gilt für andere ausländische Datenschutzgesetze.
SVV	41 BVG				Es gilt, die als Folge der Revision des DSG notwendigen gesetzlichen Grundlagen im BVG zu verankern.
	41. BVG	85a			**Bearbeiten von Personendaten** Antrag: – Streichen von Art. 85a VE-BVG Einleitungssatz – Ändern von **Art. 85a BVG** Bearbeiten von Personendaten, wie folgt: «Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter **Personend**~~D~~aten **im Sinne von Artikel 3 Buchstaben a und c DSG** ~~und Persönlichkeitsprofile~~, zu bearbeiten oder bearbeiten zu lassen, **das Profiling im Sinne von Artikel 3 Buchstabe f DSG durchzuführen und automatisierte Einzelentscheidungen im Sinne von Artikel 15 DSG zu erlassen, soweit dies notwendig ist,** ~~die sie benötigen,~~ um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:» Begründung: Gemäss VE-DSG soll der Passus «und Persönlichkeitsprofile» in Art. 85a BVG gestrichen werden. Dem erläuternden Bericht zum VE-DSG kann zwar entnommen werden, dass der Begriff «Persönlichkeitsprofil» im revidierten DSG durch den Begriff «Profiling» ersetzt werden soll (siehe Ziffer 8.1.1.3 erläuternder Bericht; Art. 3 Bst. f VE-DSG). Es kann ihm jedoch keine Begründung dafür entnommen werden, weshalb der Begriff im BVG nicht ebenfalls ersetzt, sondern vielmehr ersatzlos gestrichen werden soll. Die ersatzlose Streichung bedeutet eine unnötige, massive Einschränkung im Rahmen der Durchführung des BVG. Denn der Begriff «Profiling» definiert auch die Auswertung von nicht-personenbezogenen Daten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Es ist nicht nachvollziehbar, weshalb dies inskünftig nicht mehr möglich sein soll.

					Im Interesse der Rechtssicherheit sollte auch im BVG von besonders schützenswerten Personendaten die Rede sein, damit die Begriffe im DSG und im BVG einheitlich verwendet werden. Ferner gilt es im Hinblick auf Art. 27 Abs. 2 VE-DSG im BVG eine Grundlage für den Erlass von automatisierten Einzelentscheidungen zu schaffen. Eine Informations- und Anhörungspflicht bei automatisierten Einzelentscheidungen würde zu einem enormen administrativen Mehraufwand mit entsprechenden Kosten führen – und dies ohne den Versicherten einen erkennbaren Nutzen zu bringen.
SVV	41. BVG	86a			**Datenbekanntgabe** Antrag: **Art. 86a Abs. 5 Bst. B BVG** Datenbekanntgabe «b. Personendaten, sofern die betroffene Person im Einzelfall ~~schriftlich~~ **in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht,** eingewilligt hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse des Versicherten vorausgesetzt werden darf.» Begründung: Das Parlament haben in ihrem Rückweisungsbeschluss betreffend die Revision VVG verlangt, dass bei der Erarbeitung einer neuen Vorlage dem elektronischen Geschäftsverkehr Rechnung getragen wird. Dies im Hinblick auf die Tatsache, dass die Digitalisierung im gesamten Versicherungswesen Einzug gehalten hat. Es gilt daher, nicht nur im VVG, sondern auch im BVG die Bestimmungen technologieneutral zu formulieren und Begriffe, die den elektronischen Geschäftsverkehr behindern, konsequent zu eliminieren. Der VE-DSG als solcher behindert den elektronischen Geschäftsverkehr zwar grundsätzlich nicht, da das Erfordernis der Schriftlichkeit nur in einer einzigen Bestimmung betreffend die Auftragsdatenbearbeitung vorgesehen ist. Die Änderung von Art. 86a Abs. 5 Bst. b BVG ist jedoch notwendig, da das BVG als Spezialgesetz dem DSG vorgeht.
SVV	43. UVG				Es gilt, die als Folge der Revision des DSG notwendigen gesetzlichen Grundlagen im UVG zu verankern.

SVV	43. UVG	96			**Bearbeiten von Personendaten** Antrag: – Streichen von Art. 96 VE-UVG Einleitungssatz – Ändern von Art. 96 Bearbeiten von Personendaten, wie folgt: «**[1]** Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter **Personend**~~D~~aten ~~und Persönlichkeitsprofile~~, zu bearbeiten oder bearbeiten zu lassen, **das Profiling im Sinne von Artikel 3 Buchstabe f DSG durchzuführen und automatisierte Einzelentscheidungen im Sinne von Artikel 15 Absatz 1 DSG zu erlassen, soweit dies notwendig ist,** ~~die sie benötigen,~~ um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:» **[2 (neu)] Die mit der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Personendaten im Sinne von Artikel 3 Buchstaben a und b DSG zu bearbeiten oder bearbeiten zu lassen und das Profiling im Sinne von Artikel 3 Buchstabe f DSG durchzuführen, um mit Einwilligung der Versicherten Case-Management-Massnahmen zu ergreifen. Die Einwilligung der Versicherten hat in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht, zu erfolgen.**» Begründung: Absatz 1: Gemäss VE-DSG soll der Passus «und Persönlichkeitsprofile» in Art. 96 UVG gestrichen werden. Dem erläuternden Bericht zum VE-DSG vom 21. Dezember 2016 kann zwar entnommen werden, dass der Begriff «Persönlichkeitsprofil» im revidierten DSG durch den Begriff «Profiling» ersetzt werden soll (siehe Ziffer 8.1.1.3 erläuternder Bericht; Art. 3 Bst. f VE-DSG). Es kann ihm jedoch keine Begründung dafür entnommen werden, weshalb der Begriff im UVG nicht ebenfalls ersetzt, sondern vielmehr ersatzlos gestrichen werden soll. Die ersatzlose Streichung bedeutet eine unnötige, massive Einschränkung im Rahmen der Durchführung des UVG. Denn der Begriff «Profiling» definiert auch die Auswertung von nicht-personenbezogenen Daten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Es ist nicht nachvollziehbar, weshalb dies inskünftig nicht mehr möglich sein

					soll. Im Interesse der Rechtssicherheit sollte auch im UVG von besonders schützenswerten Personendaten die Rede sein, damit die Begriffe im DSG und im UVG einheitlich verwendet werden. Ferner gilt es im Hinblick auf Art. 27 Abs. 2 VE-DSG im UVG eine Grundlage für den Erlass von automatisierten Einzelentscheidungen zu schaffen. Eine Informations- und Anhörungspflicht bei automatisierten Einzelentscheidungen würde zu einem enormen administrativen Mehraufwand mit entsprechenden Kosten führen – und dies ohne den Versicherten einen erkennbaren Nutzen zu bringen. Neuer Absatz 2: Die neue Bestimmung ist notwendig, da Bundesorgane und damit auch UVG-Versicherer gemäss Art. 27 Abs. 3 VE-DSG nur noch im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten dürfen – und auch dies nur unter bestimmten Voraussetzungen. Von «ausnahmsweise» und «im Einzelfall» kann aber bei Case-Management-Massnahmen wohl kaum die Rede sein. Es besteht somit die Gefahr, dass die stetig an Bedeutung gewinnenden Case-Management-Massnahmen als Folge der Revision des DSG nicht mehr zulässig sind, weil sie nicht zu den Aufgaben gehören, die das UVG von Gesetzes wegen den Versicherern überträgt, sondern um freiwillige Wiedereingliederungsbemühungen des UVG-Versicherers. Mit der vorgeschlagenen Ergänzung wird ausdrücklich präzisiert, dass solche Massnahmen die Einwilligung der Versicherten in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht, erfordern.
SVV	UVG	97	1		**Datenbekanntgabe** <u>Antrag:</u> «**b$^{ter\ (neu)}$ Privatversicherern, wenn die Daten für die Koordination der Beurteilung und Berechnung von Leistungsansprüchen erforderlich sind;**» <u>Begründung:</u> Art. 26 Abs. 2 VE-DSG sieht zwar vor, dass der Bundesrat auf dem Verordnungsweg die Kontrolle und die Verantwortung regelt, wenn Bundesorgane zusammen mit anderen Bundesorganen oder mit Privaten Daten bearbeiten. Diese geplante Regelung lediglich der Kontrolle und Verantwortung – und dies

					erst noch nur auf Verordnungsstufe – dürfte aber keine ausreichende Grundlage dafür bilden, um eine notwendige und praktikable Zusammenarbeit zwischen den Grund- und Zusatzversicherern zu garantieren.
SVV	UVG	97	6	b	**Datenbekanntgabe** Antrag: «b. Personendaten, sofern die betroffene Person im Einzelfall ~~schriftlich~~ **in schriftlicher Form oder in einer anderen Form, die den Nachweis durch Text ermöglicht**, eingewilligt hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse des Versicherten vorausgesetzt werden darf.» Begründung: Das Parlament hat im Rückweisungsbeschluss betreffend die VVG-Revision verlangt, dass bei der Erarbeitung einer neuen Vorlage dem elektronischen Geschäftsverkehr Rechnung getragen wird. Dies im Hinblick auf die Tatsache, dass die Digitalisierung im gesamten Versicherungswesen Einzug gehalten hat. Es gilt daher, nicht nur im VVG, sondern auch im UVG die Bestimmungen technologieneutral zu formulieren und Begriffe, die den elektronischen Geschäftsverkehr behindern, konsequent zu eliminieren. Der VE-DSG als solcher behindert den elektronischen Geschäftsverkehr zwar grundsätzlich nicht, da das Erfordernis der Schriftlichkeit nur in einer einzigen Bestimmung betreffend die Auftragsdatenbearbeitung vorgesehen ist. Die Änderung von Art. 97 Abs. 6 Bst. b UVG ist jedoch notwendig, da das UVG als Spezialgesetz dem DSG vorgeht.
SVV	VAG	45	1	e.	Antrag: Streichen von Art. 45 Abs. 1 Bst. e VAG Begründung: Das Versicherungsaufsichtsgesetz (VAG) ist nicht Bestandteil der Vernehmlassungsvorlage. Der SVV würde es aber begrüssen, wenn im Zuge der Totalrevision des DSG diese Sonderbestimmung gestrichen würde. Dem Transparenzerfordernis wird mit dem neuen Datenschutzgesetz genügend entspro-

					chen. Die Informationspflichten des Versicherungsrechts führen zur Rechtsunsicherheit (Frage der lex specialis) und zu Doppelspurigkeiten und sollten daher im Zuge der vorliegenden Revision ersatzlos gestrichen werden.
SVV	VVG	3	1	g.	Antrag: Streichen von Art. 3 Abs. 1 Bst. g VVG Begründung: Das Versicherungsvertragsgesetz (VVG) ist nicht Bestandteil der Vernehmlassungsvorlage. Der SVV würde es aber begrüssen, wenn im Zuge der Totalrevision des DSG diese Sonderbestimmung gestrichen würde. Dem Transparenzerfordernis wird mit dem neuen Datenschutzgesetz genügend entsprochen. Die Informationspflichten des Versicherungsrechts führen zur Rechtsunsicherheit (Frage der lex specialis) und zu Doppelspurigkeiten und sollten daher im Zuge der vorliegenden Revision ersatzlos gestrichen werden.

Association suisse des officiers de l'état civil
Associazione svizzera degli ufficiali dello stato civile
Schweizerischer Verband für Zivilstandswesen

Eidg. Justiz- und Polizeidepartement

Per Mail an:
jonas.amstutz@bj.admin.ch

Zürich, 1. April 2017

Vernehmlassung des Bundes zur geplanten Totalrevision des Datenschutzgesetzes und der weiteren Erlasse zum Datenschutz (DSG)
Stellungnahme des Schweizerischen Verbandes für Zivilstandswesen (SVZ)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Der Vorstand des Schweizerischen Verbandes für Zivilstandswesen nimmt zur eingangs erwähnten Angelegenheit gerne wie folgt Stellung:

Der Schweizerische Verband für Zivilstandswesen schliesst sich vollumfänglich der Stellungnahme der Konferenz der kantonalen Aufsichtsbehörden im Zivilstandsdienst vom 18. März 2017 an.

Wir danken Ihnen für die Berücksichtigung unserer Eingabe.

Freundliche Grüsse

Schweizerischer Verband für Zivilstandswesen

Roland Peterhans
Präsident

Geschäftsstelle Schweizerischer Verband für Zivilstandswesen
c/o bwd, Weiterbildung BV Bern, Papiermühlestrasse 65, 3014 Bern
Tel. 031 330 19 89, Fax 031 330 19 80, E-Mail: zivilstandswesen@bwdbern.ch

Schweizer Werbe-Auftraggeberverband
Utenti Svizzeri Pubblicità
Association Suisse des Annonceurs
Association of Swiss Advertisers

Per E-Mail an jonas.amstutz@bj.admin.ch
Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

3. April 2017

Vernehmlassungsantwort des SWA zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Der Schweizer Werbe-Auftraggeberverband (SWA) ist ein in jeder Hinsicht unabhängiger Verein nach Schweizer Recht. Er vertritt seit 1950 die Interessen der Werbeauftraggeber im Bereich Marketing, Werbung, Medien, Sponsoring und Public Relations. Heute repräsentieren die über 180 Mitglieder des SWA etwa 75% des Schweizer Werbemarktes.

1. Bedeutung des Datenschutzes und der Entwurf als existentieller Standortnachteil

Für jeden Werbeauftraggeber und damit für jedes Unternehmen in der Schweiz ist es von existenzieller Bedeutung, dass er mit seinen aktuellen oder potentiellen Kunden, seinen Zulieferern und sonstigen Partnern möglichst wirkungsvoll kommunizieren kann. Dabei werden naturgemäss auch Personendaten ausgetauscht. Das Kommunizieren ist für Unternehmen der Sauerstoff ihres wirtschaftlichen Tätigwerdens.

Das Datenschutzgesetz hat somit für sämtliche Unternehmen sowie den davon abhängigen Arbeitnehmerinnen und Arbeitnehmer eine existentielle Bedeutung, insbesondere im Bereich der digitalen Kommunikation. Der Bundesrat hat dies erkannt und im Zusammenhang mit dem am 11. Januar 2017 verabschiedeten Bericht „Rahmenbedingungen der digitalen Wirtschaft“ verlauten lassen:

> ***„Der digitale Wandel bietet grosse Chancen für die Schweizer Volkswirtschaft. Der Bundesrat will diese nutzen, um Arbeitsplätze und Wohlstand zu sichern.“***

Der vorliegende Gesetzesentwurf widerspricht diametral diesen Zielsetzungen des Bundesrates zur Förderung des Wirtschaftsstandortes Schweiz und des allgemeinen Wohlstandes! Er bewirkt vielmehr einen im höchsten Masse bedenklichen Standort-

nachteil, der neben Grossunternehmen insbesondere die heimischen KMUs überfordert und existentiell gefährdet.

2. Grundhaltung zum vorliegenden Gesetzesentwurf

Der SWA anerkennt und erachtet es als notwendig, dass das aktuelle DSG insoweit überarbeitet wird, dass die Vorgaben der Europarats-Konvention (E-SEV 108) und ein anerkennungsfähiges Schutzniveau im Lichte der EU-DSGVO erfüllt werden, um den internationalen Datenaustausch zu ermöglichen resp. zu vereinfachen. Diese internationalen Bestimmungen legen ein allgemein anerkanntes Schutzniveau im Bereich Datenschutz fest.

Aus diesen Gründen lautet die Position des SWA wie folgt:

Das Datenschutzgesetz ist nur insoweit zu revidieren, als dies die internationalen Vorgaben zwingend erfordern. Jeder darüber hinausgehender „Swiss Finish"(im vorliegenden Entwurf zum Beispiel im Bereich Profiling und Sanktionensystem besonders gravierend) ist strikte abzulehnen.

3. Einzelne zentrale Punkte

I. Art. 3 Bst. a DSG, Begriff der Personendaten

Die Beibehaltung der Definition von Personendaten ist zu begrüssen.

Unter Einbezug des erläuternden Berichts ist die vorgeschlagene Regelung jedoch unklar und potentiell widersprüchlich. Auf der einen Seite soll der Begriff „Personendaten" gemäss Bericht gegenüber dem geltenden Recht zwar inhaltlich nicht geändert werden. Dabei ist insbesondere die implizite Anerkennung der relativen Methode, wie sie auch in der EU künftig weiterhin gelten soll, zentral und richtig. Auf der andern Seite wird im Bericht jedoch eine natürliche Person als bestimmbar erklärt, wenn sie „über Hinweise auf eine Identifikationsnummer oder eine Online-Identität" identifiziert werden kann.

Diese Formulierung ist gerade in diesem für sämtliche Online-Aktivitäten fundamentalen Punkt missverständlich und je nach Interpretation widersprüchlich. Denn nach der wohl herrschenden Auffassung genügt es unter dem geltendem DSG nicht, wenn Angaben bloss einer bestimmten „eindeutigen Kennung" oder „Identifikationsnummer", wie z.B. einer IP-Adresse oder Cookie-Kennungen zugeordnet werden können, hinter welcher letztlich eine Person steht, diese aber nicht namentlich identifiziert werden kann (sog. Singularisierung). Bei der Qualifikation von IP-Adressen etc. muss daher auch künftig eine Einzelfallbeurteilung entscheidend sein, unter Berücksichtigung des Aufwands zur Identifizierung mit den zur Verfügung stehenden technischen Möglichkeiten (objektive Seite) sowie dem Interesse an der Identifizierung (subjektive Seite).

Insbesondere beim Einsatz von Cookies zur Auslieferung von individualisierter Werbung auf Websites, bei welchem regelmässig auch die IP-Adresse mitbearbeitet wird, besteht dabei kein Interesse an der namentlichen Identifikation des Nutzers, sondern lediglich an der Kategorisierung. Würde hier stets von Personendaten ausgegangen werden müssen, hätte dies erhebliche Auswirkungen auf die gesamten Online-Aktivitäten, sodass letzten Endes zahlreiche heute werbefinanzierte, unentgeltliche Angebote künftig nicht mehr allgemein zur Verfügung stehen würden. Vor diesem Hintergrund ist eine Klarstellung in der Botschaft, dass das Konzept der Singularisierung abgelehnt wird, von zentraler Bedeutung. Der Umstand, dass nach Auffassung einzelner Autoren unter der EU-DSGVO eine Singularisierung für das Vorliegen von Personendaten ausreichen soll, ändert daran nichts. Denn zum einen wird diese Auffassung von anderen Autoren mit überzeugenden Argumenten abgelehnt. Zum anderen

ergibt sich eine derart strenge Auslegung auch nicht aus dem E-SEV 108. Deshalb besteht keine Notwendigkeit, sie im Schweizer Recht einzuführen (Swiss Finish).

II. Art. 3 Bst. f DSG, Begriff des Profiling

Die vorgeschlagene Definition und die damit einhergehende Regelung (siehe dazu Anmerkungen zu Art. 23 unten) des „Profiling" werden abgelehnt. Die Definition geht ohne Not weit über diejenige der EU-DSGVO (Art. 4 Ziff. 4) hinaus (Swiss Finish).
Zudem enthält der E-SEV 108 keinerlei Vorgaben für das Profiling. Vielmehr verlangt dieser nur eine Regelung von automatisierten Entscheidungen (vgl. Art. 8 Abs.1 lit. a). Ausgehend davon sollte auf spezifische Vorgaben für das Profiling verzichtet werden. Wird gleichwohl an einer Regelung festgehalten, sollte diese aber jedenfalls auf automatisierte Bearbeitungen beschränkt bleiben. Keinesfalls darf die Regelung jedoch derart weit gefasst werden, dass die Vorgaben (systemwidrig) sogar für das Profiling mit nicht personenbezogenen Daten gelten. Für die im erläuternden Bericht angesprochenen Bearbeitungen bspw. im Rahmen von Big Data Analysen genügen die übrigen Regelungen vollends. Denn bei einem Profiling, das am Ende zu Personendaten führt, gelten diese ohnehin bereits. Darüber hinaus wird die Unsicherheit, welche konkreten Bearbeitungen in der Praxis als Profiling zu betrachten sind, durch den entsprechenden Zusatz weiter verstärkt.

III. Art. 6 Abs. 1 Bst. b DSG, Begriff der Einwilligung

Die vorgeschlagene Änderung hinsichtlich des überaus zentralen Begriffs der „Einwilligung" ist unter Einbezug des erläuternden Berichts unklar. Gemäss erläuterndem Bericht (S. 47) ermöglicht die Neuformulierung eine terminologische Annäherung an die DSGVO. Es wird allerdings nicht klargestellt, ob damit eine inhaltliche Annäherung bezweckt wird. **Die Definition ist nicht nur, aber in besonders ausgeprägter Form gerade für die Werbebranche von fundamentaler Bedeutung, weshalb eine klare Regelung und damit Rechtssicherheit erforderlich ist.** Die Übernahme der gegenüber der E-SEV 108 unnötig strengen Vorgaben der EU-DSGVO in Bezug auf die „Freiwilligkeit der Einwilligung" (Art. 7 Abs. 4) hätte jedenfalls eine massive Verschärfung der Rechtslage gegenüber dem geltenden Recht sowie eine erhebliche Beschränkung der Vertragsfreiheit zur Folge, die unnötig und daher abzulehnen ist. Der E-SEV 108 (Art. 5 Abs. 2) verlangt denn auch lediglich, dass die Einwilligung freiwillig sein muss („free consent"), ohne eine derart strenge Interpretation, wie sie die EU-DSGVO enthält, vorzuschreiben. In der Botschaft muss deshalb eine entsprechende Klarstellung aufgenommen werden.
Darüber hinaus sind die Ausführungen im erläuternden Bericht zur „ausdrücklichen Einwilligungen" unklar bzw. unvollständig. Es geht daraus letztlich nicht hervor, welche Anforderungen konkret an eine solche Einwilligung gestellt werden, was gerade aufgrund des (noch) übermässig weit gefassten Begriffs des Profiling und dessen Bedeutung für die Werbebranche besonders problematisch ist. Es ist daher in der Botschaft auch klar zu stellen, dass – wie nach geltendem Recht – eine Einwilligung dann ausdrücklich ist, wenn die Datenbearbeitung, in welche eingewilligt wird, also z.B. das Profiling, bspw. in der Datenschutzerklärung beim Namen genannt wird und es insofern nicht genügen würde, wenn bloss aus den Umständen auf ein Profiling geschlossen werden müsste.
Schliesslich ist in der Botschaft auch festzulegen, dass – entsprechend dem geltenden Recht – eine **Einwilligung in Datenbearbeitungen auch durch Zustimmung zu einem Dokument, das weitere Informationen erhält (wie z.B. AGB oder Datenschutzerklärungen), erteilt werden kann und keine separate Information bzw. Einwilligung erforderlich ist.**

IV. Art. 7 DSG, Auftragsdatenbearbeitung

Die grundsätzliche Beibehaltung der geltenden Rechtslage hinsichtlich der Auftragsdatenbearbeitung ist zu begrüssen. Abzulehnen ist jedoch die unbeschränkte Delegation an den Bundesrat zur Festlegung weiterer Pflichten. Zudem ist Abs. 3 zu streichen. Eine zwingende

Zustimmung zum Beizug von Sub-Auftragsdatenbearbeiter ist weder durch die internationalen Verpflichtungen gefordert, noch entspricht sie der bisher geltenden Rechtslage (Swiss Finish). Sie wäre in der Praxis auch nicht praktikabel. Sollte daran festgehalten werden, müsste die Bestimmung zumindest dahingehend angepasst werden, dass nicht „Schriftlichkeit" erforderlich ist, sondern eine Form, die den „Nachweis durch Text" ermöglicht. Andernfalls wäre die Ermächtigung zur Einsetzung von Unterauftragnehmern namentlich in Verträgen, die Online abgeschlossen werden, nicht mehr möglich.

V. Art. 12 DSG, Daten einer verstorbenen Person

Die Einführung einer Regelung zu Daten verstorbener Personen ist im Hinblick auf die Angemessenheit des Schweizer Datenschutzrechts nicht zwingend erforderlich und führt für die Unternehmen zu einem erheblichen administrativen Mehraufwand **(Swiss Finish). Auf die Regelung ist daher zu verzichten.**

VI. Art. 13 und Art. 15 DSG Informationspflicht

Die Einführung einer generellen Informationspflicht ist mit Blick auf den E-SEV 108 zwingend und insofern richtig. **Allerdings gehen diverse Punkte der vorgeschlagenen Regelung zu weit und sind daher abzulehnen** (vgl. dazu die eingehende Stellungnahme des Schweizer Dialogmarketing Verband SDV).

VII. Art. 16 Datenschutz-Folgenabschätzung

Die Anknüpfung an das Vorliegen „erhöhter Risiken" führt zu einem viel zu weit gefassten Anwendungsbereich und geht unverständlicherweise sogar über die Vorgaben in der EU-DSGVO (Art. 35) hinaus (Swiss Finish).

VIII. Art. 23 Abs. 2 Bst. d, Profiling nur mit Einwilligung

Das generelle Erfordernis der ausdrücklichen Einwilligung für das Profiling stellt eine der problematischsten Schweizer Verschärfungen dar und ist zwingend zu streichen (Swiss Finish). Für die Werbewirtschaft hat diese Anforderung erhebliche Konsequenzen, welche unnötig, unangemessen und unzweckmässig sind. Denn nach dem E-SEV 108 ist eine entsprechende Vorgabe nicht verlangt. Ferner ist auch nach der EU-DSGVO nicht für jegliche Form des Profiling eine Einwilligung erforderlich. Aber auch in der Sache besteht keine Notwendigkeit, das Profiling per se als Persönlichkeitsverletzung einzustufen. Solange die Datenbearbeitungsgrundsätze eingehalten werden, ist nicht ersichtlich, wieso neben der Information stets zusätzlich auch eine Einwilligung erforderlich sein soll.
Wird diese Vorschrift Gesetz verunmöglicht sie faktisch einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung / Marketing und stellt eine Bedrohung für den Standort Schweiz dar. Profiling und damit personalisierte Werbung wäre dann faktisch nur noch den grossen (insbesondere internationalen) Log-in Giganten wie Facebook, Google, Apple und Co. vorbehalten. Diese Unternehmen können sich meist problemlos auf eine ausdrückliche Einwilligung im Rahmen der Account-Registrierungen stützen. Das Ergebnis wäre sodann auch aus kartellrechtlichen Überlegungen höchst problematisch.

IX. Art. 50 ff. Sanktionensystem

Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt. Es ist in höchstem Mass innovationshemmend und etabliert eine Kultur des Denunziantentums in den Unternehmen. Es führt zu einem ganz erheblichen Standortnachteil der Schweiz. Kein innovatives digitales Start-Up beispielsweise wird bereit sein, seine Gründer und Mitarbeiter solch drasti-

schen strafrechtlichen Risiken auszusetzen. Gute Mitarbeiter werden nicht mehr bereit sein Verantwortung in den Unternehmen mitzutragen.

Für die Berücksichtigung der Anliegen der Werbebranche zur Schaffung einer verhältnismässigen und praxistauglichen Datenschutzregulierung danken wir Ihnen im Voraus und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Schweizer Werbe-Auftraggeberverband SWA

Roger Harlacher
Präsident

Roland Ehrler
Direktor

Swico
Josefstrasse 218
CH-8005 Zürich

Tel. +41 44 446 90 90
www.swico.ch
info@swico.ch

Eidgenössisches Justiz-
und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

Zürich, 3. April 2017

Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Namens des Swico bedanken wir uns für die Möglichkeit, unsere Position zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz darzulegen und reichen hiermit unsere Stellungnahme ein.

1. Legitimation und Betroffenheit

Swico ist der Verband der ICT-Anbieter der Schweiz. Swico vertritt die Interessen von 450 ICT-Anbieterfirmen, welche 56'000 Mitarbeitende beschäftigen und einen Umsatz von jährlich CHF 40 Milliarden erwirtschaften.

Datenschutz spielt in der ICT-Branche, deren Interessen Swico vertritt, eine ganz zentrale Rolle. Die Unternehmen der ICT-Branche sind daher auf eine diesbezügliche praxisnahe und wirtschaftsfreundliche Regelung besonders angewiesen und von dieser Vernehmlassungsvorlage unmittelbar betroffen.

2. Vernehmlassung

2.1 Grundsätzliches

Eine Angleichung an die Rechtslage in der EU ist dort sinnvoll und zu begrüssen, wo diese für die Geschäftstätigkeit der Unternehmen in der Schweiz sowie den Zugang und Austausch in den EU-Raum notwendig und für ein angemessenes Datenschutzniveau angebracht ist. Entsprechend ist auch eine Förderung der Selbstregulierung in diesem Sinne zu befürworten. Mit allem Nachdruck abzulehnen sind durch den Vorentwurf neu eingeführte oder erweiterte Pflichten, die als „Swiss Finish“ über den Stand des durch die DSGVO harmonisierten europäischen Datenschutzes hinausgehen.

2.2 Stellungnahme zu einzelnen Artikeln

Für die Stellungnahme zu einzelnen Artikeln des Vorentwurfes, bei welchen aus unserer Sicht hauptsächlicher Handlungsbedarf besteht, verweisen wir auf das offizielle Formular für die Stellungnahme in der Beilage, welches integrierender Bestandteil dieser Stellungnahme ist.

3. Fazit und Antrag

Wir beantragen die Rückweisung des Vorentwurfes zur Überarbeitung im Sinne der Erwägungen gemäss Stellungnahmeformular.

Insbesondere folgende Punkte sind zu überarbeiten:

- Begriffe
- Empfehlungen der guten Praxis
- Informationspflicht bei der Beschaffung von Personendaten
- Datenschutz-Folgenabschätzungen
- Meldepflicht von Datenschutzverstössen
- Profiling
- Betrieblicher Datenschutzbeauftragter
- Strafbestimmungen

Grosse Fragezeichen bestehen auch bezüglich einer praktikablen Umsetzbarkeit dieses Vorentwurfes in der Schweizer Wirtschaftsstruktur, insbesondere für KMU, Kleinstfirmen und auch die in unserer Branche so wichtigen Start-Ups. Diesen drohen grosse Zusatzkosten und administrative nutzlose Auflagen wie strafbewehrte Anzeige- und Meldepflichten an Datenschutzbehörden, welche letztlich die Innovationskraft entscheidend hemmen würden.

Wir danken Ihnen für eine Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Swico

Dr. Peter K. Neuenschwander
Vorsitzender Kommission IT Recht

Christa Hofmann
Head Legal & Public Affairs

Beilage: offizielles Formular für die Stellungnahme

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Swico, Verband der ICT-Anbieter der Schweiz

Abkürzung der Firma / Organisation : Swico

Adresse : Josefstrasse 218, 8005 Zürich

Kontaktperson : Christa Hofmann

Telefon : 044 446 90 87

E-Mail : Christa.Hofmann@swico.ch

Datum : 3. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Swico	Legitimation und Betroffenheit Swico ist der Verband der ICT-Anbieter der Schweiz. Swico vertritt die Interessen von 450 ICT-Anbieterfirmen, welche 56'000 Mitarbeitende beschäftigen und einen Umsatz von jährlich CHF 40 Milliarden erwirtschaften. Datenschutz spielt in der ICT-Branche, deren Interessen Swico vertritt, eine ganz zentrale Rolle. Die Unternehmen der ICT-Branche sind daher auf eine diesbezügliche praxisnahe und wirtschaftsfreundliche Regelung besonders angewiesen und von dieser Vernehmlassungsvorlage unmittelbar betroffen.
Swico	Das geltende Datenschutzgesetz hat die Digitalisierung der Schweiz begleitet und seinen Zweck bestens erfüllt. Diese positive Entwicklung darf nun nicht durch eine überschiessende Schweizer Datenschutzregulierung gefährdet werden. Grundsätzlicher Antrag: **Nichteintreten** auf den „Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz“ und Rückweisung zur Überarbeitung im Sinne der Erwägungen, v.a. ohne überschiessenden „Swiss Finish“. Danach ist nochmals eine Vernehmlassungsfrist vorzusehen mit erneuter Gelegenheit zur Stellungnahme.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Swico	DSG	3		a	Gewisse Begriffe allgemein sind teils unbestimmt und zu weitgehend umschrieben. Diese Begriffe sind zu schärfen und präzisieren. Personendaten: Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Hier ist insbesondere auch näher zu definieren was unter bestimmbar zu verstehen ist.
Swico	DSG	3		f	Profiling: umfasst gemäss VE jede Auswertung von Daten (sogar nicht personenbezogene Daten) und auch das manuelle Profiling „von Hand“. Antrag: Der Begriff „Profiling“ ist analog zu DSGVO und E-SEV 108 einzuschränken auf die automatisierte Auswertung von Personendaten.
Swico	DSG	4	6		Ausdrückliche Einwilligung beim Profiling Auch stillschweigendes Verhalten hat als gültige Einwilligung zu gelten, damit weiterhin die im Massengeschäft unumgänglichen Allgemeinen Geschäftsbedingungen (AGB) verwendet werden können. Antrag: Das Erfordernis der ausdrücklichen Einwilligung für das Profiling ist gänzlich zu streichen.
Swico	DSG	5			Feststellung durch den Verantwortlichen – nicht den Bundesrat Die neu vorgesehene Feststellung durch den Bundesrat, ob Daten im Ausland genügend geschützt sind, bedeutet eine unsachliche und unnötige Einschränkung. Diese Feststellung hat nicht durch den Bundesrat, sondern durch den Verantwortlichen, gestützt auf dessen eigene Abklärungen und Kenntnisse, zu erfolgen.
Swico	DSG	5	3	d	Binding Corporate Rules Binding Corporate Rules sollen eine Genehmigung durch den EDÖB benötigen. Jedoch stellen diese eine

					Untergruppe der spezifischen Garantien dar. Für Garantien ist jedoch lediglich eine Informationspflicht vorgeschrieben. Dies ist widersprüchlich. Es sollte zwischen Standardverträgen und anderen Verträgen/Garantien unterschieden und die Pflichten entsprechend angepasst werden.
Swico	DSG	5	5		Die Frist von sechs Monaten zur Genehmigung für Binding Corporate Rules durch den EDÖB ist viel zu lange, nicht praktikabel und führt zu grosser Rechtsunsicherheit. Hier ist auf die bisherige Regelung von 30 Tagen abzustellen.
Swico	DSG	6	2		Diese Meldepflicht an den EDÖB hat faktisch zur Folge, dass Unternehmen dem EDÖB auch sensible Geschäftsgeheimnisse offenzulegen hätten; sogar in den Fällen, in welchen der Datenexport durch Vertragsabschluss oder Vertragserfüllung oder ein ausländisches Rechtsverfahren gerechtfertigt wird. Darüber hinaus sind diese dem EDÖB gelieferten Unterlagen gemäss Öffentlichkeitsgesetz öffentlich einsehbar sind. Diese Meldepflicht ist auch zu weit, da sie auch den Auftragsbearbeiter zur Meldung verpflichtet, nicht nur den Verantwortlichen. Antrag: Diese Bestimmung, die auch dem EU Recht fremd ist, ist ersatzlos zu streichen.
Swico	DSG	7	2		Der Verantwortliche muss sich neu insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, sowohl die Datensicherheit als auch die Rechte der betroffenen Person zu gewährleisten. Diese Vergewisserungspflicht führt zu massivem Mehraufwand beim Outsourcing der Datenbearbeitung. Auch ist unklar, welche Pflichten dem Auftragsbearbeiter überbunden werden sollen. Antrag: Abs. 2 zu streichen
Swico	DSG	7	3		Diese Bestimmung der vorgängigen schriftlichen Zustimmung des Verantwortlichen ist praxisfremd und auch in der EU nicht vorgesehen. Es kann sich hier nicht um Schriftlichkeit i.S.v. Art. 13 OR handeln. Eine in schriftlicher, elektronischer oder vergleichbarer Form abgegebene generelle Einwilligung zur Übertragung an einen anderen Auftragsbearbeiter und eine Information im konkreten Fall ist ausreichend.
Swico	DSG	8 und 9			Empfehlungen der guten Praxis Die Problematik besteht darin, dass eigene Empfehlungen der interessierten Kreise nur mittels Genehmigung durch den EDÖB festgelegt werden können. Der EDÖB hat zudem die Kompetenz,

					Empfehlungen auf eigene Initiative selbst auszuarbeiten. Dann ist auch unklar, ob es sich bei der Genehmigung um eine Verfügung handelt; so ist kein Rechtsmittel gegen den Erlass oder die Verweigerung der Zustimmung des EDÖB vorgesehen. In der DSGVO ist die Ausarbeitung von Verhaltensregeln nur durch die Verbände und andere Vereinigungen vorgesehen. Dies muss auch hier der Fall sein und die Initiative also zwingend von den Verbänden ausgehen. Wie es der Begriff schon andeutet, kommen die „Empfehlungen der guten Praxis“ gerade aus der Praxis, also „bottom-up“.
Swico	DSG	13	4		Informationspflicht bei der Beschaffung von Personendaten Der VE DSG geht über die DSGVO hinaus: Nach Art. 13 Abs. 4 VE DSG muss der Verantwortliche bei der Weitergabe an einen Auftragsbearbeiter auch über die Identität und Kontaktdaten der Auftragsbearbeiter informieren. Diese Bestimmung ist als Swiss Finish zu streichen.
Swico	DSG	13	5		Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden. Diese Regelung ist unsinnig und praxisfremd. In der Praxis werden die Daten gleich mit der Beschaffung gespeichert und wohl nachher überhaupt erst gelesen. Antrag: Regelung wie in der DSGVO: Frist von bis zu einem Monat.
Swico	DSG	16			Datenschutz-Folgenabschätzung Auftragsbearbeiter: Hier wird der Auftragsbearbeiter gleich wie der Verantwortliche in die Pflicht genommen. Dem Auftragsbearbeiter selbst jedoch ist es meist gar nicht möglich, aus eigenem Antrieb oder in eigener Verantwortlichkeit diesen Pflichten nachzukommen. Der Auftragsbearbeiter ist dazu auf den Verantwortlichen angewiesen. Antrag: Streichung des - auch diesbezüglich in Art 35 DSGVO nicht vorgesehenen - „Auftragsbearbeiters“ aus dieser Bestimmung.
Swico	DSG	16	1-3		Datenschutz-Folgenabschätzung Art. 16 VE schreibt die vorgängige Durchführung einer Datenschutz-Folgenabschätzung vor in allen Fällen, in welchen eine vorgesehene Datenbearbeitung „voraussichtlich zu einem erhöhten Risiko“ für die Persönlichkeit der betroffenen Personen führt. Diese extrem weite Definition würde dazu führen, dass für

					die allermeisten Datenbearbeitungen vorab entsprechende, aufwändige Abklärungen durchgeführt werden müssten. Das heisst für die Unternehmen, dass sie bei jedem Projekt, das eine Datenbearbeitung beinhaltet und diese nicht als unproblematisch erscheint, eine Vorlaufsfrist von einigen Monaten einplanen müssten; dies nur um nach den eigenen Abklärungen auch allfälligen Anforderungen des EDÖB gerecht werden zu können. Dies stellt eine völlig sinnlose Belastung der Wirtschaft dar und hätte erhebliche Kosten zur Folge. Antrag: Der Verweis auf die Grundrechte ist zu streichen. Im privaten Bereich dient das DSG ausschliesslich dem Schutz der Persönlichkeit der betroffenen Personen. Antrag: Führt die die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen (~~erhöhten~~) Risiko für die Persönlichkeit der betroffenen Person, so muss der Verantwortliche vorgängig eine Datenschutz-Folgenabschätzung durchführen.
Swico	DSG	16	4		Die Ergebnisse der Folgenabschätzung müssen dem EDÖB mitgeteilt werden. Der EDÖB teilt dem Verantwortlichen innerhalb von drei Monaten mit, falls er gegen die Massnahmen Einwände hat. Antrag: Streichung resp. Ersatz durch angemessene Frist von 1 Monat. Ausnahmemöglichkeit Die Möglichkeit der Einführung eines betrieblichen Datenschutzbeauftragten sollte vorgesehen werden als Option für die Unternehmen, kombiniert mit der Freistellung von allfälligen Meldepflichten gegenüber dem EDÖB (z.B. hier bei der Datenschutz-Folgenabschätzung). Dies ist auch als eine sinnvolle Entlastung des EDÖB zu begrüssen. Antrag: Der betriebliche Datenschutzbeauftragte ist hier auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen.
Swico	DSG	17	1		Meldung von Verletzungen des Datenschutzes (Data Breach Notifications) Diese Meldepflicht ist viel zu weit gefasst und geht deutlich über die DSGVO Regelung hinaus. Gemäss VE soll die Meldepflicht an den EDÖB jede Datenbearbeitung erfassen, die gegen das DSG verstösst, z.B. auch eine zweckentfremdete oder unverhältnismässige Nutzung von Daten. Folglich würde jede geringfügige Unregelmässigkeit in alltäglichen Datenbearbeitungsvorgängen eine Datenschutzverletzung

					darstellen, die gemeldet werden müsste. Dies würde zu einer nicht mehr durchführbaren Meldeflut an den EDÖB führen und ist sinnlos, unverhältnismässig und würde auch viel mehr Anwendungsfälle umfassen als gemäss der DSGVO der Aufsichtsbehörde gemeldet werden müssen. Darüber hinaus ist gerade für solche geringfügige Unregelmässigkeiten das unternehmensinterne IKS vorgesehen. Die Meldepflicht an den EDÖB ist somit auf Datenschutzverstösse mit gravierenden Folgen zu beschränken. Antrag: Meldepflicht an den EDÖB ist auf Datenschutzverstösse mit gravierenden Folgen zu beschränken.
Swico	DSG	17	4		Das Erfordernis der „unverzüglichen“ Meldung ist nicht umsetzbar, da zuerst genügend Informationen gesammelt werden müssen. Zudem besteht die Gefahr, durch vorschnelles Handeln Geschäfts- oder Berufsgeheimnisse zu verletzen. Die DSGVO sieht eine Frist von bis zu 72 Stunden vor. Antrag: Frist analog DSGVO.
Swico	DSG	19		b	Neu muss bei einer Berichtigung, Löschung oder Vernichtung von Daten etc. der Verantwortliche und Auftragsbearbeiter die Dritten, denen sie zuvor die betroffenen Daten zugänglich gemacht haben, diese Berichtungen etc. mitteilen, soweit dies nicht oder nur mit „unverhältnismässigem“ Aufwand möglich ist. Der VE geht über die DSGVO deutlich hinaus. Unklar ist, ob nur die meldepflichtigen Datenschutzverletzungen darunter fallen oder alle Datenschutzverletzungen (vgl. Wortlaut). Diese Informationspflicht an den Empfänger ist weder nützlich noch praktikabel. So müsste wohl jedes Unternehmen, beim Bereinigen seiner Archive, dauernd prüfen, wem es die Daten schon einmal mitgeteilt hat und diese sogar über eine simple Löschung informieren. Antrag: Mitteilung zu beschränken auf die Fälle, wo diese Nachinformation aus berechtigen Gründen verlangt wird.
Swico	DSG	23	2	d	Eine Persönlichkeitsverletzung soll insbesondere vorliegen durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person. Im Gegensatz zur DSGVO ist auch das Profiling per Hand (manuelle Bearbeitung) erfasst (z.B. Ausfüllen einer Mitarbeiterbeurteilung). Dies ist überschiessend und geht zu weit. Antrag: Das Erfordernis der ausdrücklichen Einwilligung beim Profiling ist zu streichen. Das Profiling ist auf die automatisierte Auswertung von Personendaten zu beschränken (vgl. Bemerkungen

					zu Art. 3 vorstehend).
Swico	DSG	50-55			<u>Strafbestimmungen</u> Abzulehnen sind die geplanten Strafbestimmungen: Die Mitarbeiter eines Unternehmens geraten durch die persönliche Strafbarkeit zu stark in den Fokus der Sanktionen. Verschärft wird dies durch die Möglichkeit der Bestrafung fahrlässigen Handelns. Da es sich um strafrechtliche Sanktionen handelt, muss damit gerechnet werden, dass diese weder versichert werden können, noch vom Unternehmen für den Gebüssten bezahlt werden dürften. Die Strafbestimmungen nach Art. 50 ff. VE DSG widersprechen überdies dem elementaren strafrechtlichen Grundsatz der „nulla poena sine lege scripta stricta praevia“, welcher in Art. 1 StGB seinen Niederschlag gefunden hat. Datenschutzregeln, welche den bearbeitenden Stellen ein erhebliches Ermessen bei der Beurteilung des Vorhandenseins von Pflichten aus dem Datenschutz auferlegen, eignen sich aufgrund des die Strafverfolgung beherrschenden ”Legalitätsprinzips“ grundsätzlich nicht zur Aufstellung einer Strafnorm. Das trifft nach hier vertretener Auffassung für folgende Datenschutzvorschriften und der damit verbundenen Strafdrohung zu: - Art. 5 Abs. 1 iVm Art. 51 Abs. 1 Bst. a VE DSG Beurteilung des Risikos für die Persönlichkeit der betroffenen Personen bei einer Ausland-Bekanntgabe - Art. 7 Abs. 1 und 2 iVm Art. 51 Abs. 1 Bst. b VE DSG: Sorgfaltspflichten bei der Erteilung eines Auftrages für das Outsourcing der Datenbearbeitung - Art. 11 iVm Art. 51 Abs. 1 Bst. c VE DSG: Unterlassung angemessener technischer und organisatorischer Massnahmen zur Datensicherung - Art. 13 und Art. 14 Abs. 2 Bst. b iVm Art. 50 Abs. 1 Bst. a und b VE DSG: Strafdrohung trotz möglicher Freistellung von der Informationspflicht - Art. 15 Abs. 1 VE DSG: Beurteilung der Auswirkung einer automatisierten Einzelentscheidung iVm der Strafdrohung nach Art. 50 Abs. 1 Bst. b VE DSG - Art. 16 Abs. 1 VE DSG: Beurteilung des Vorhandenseins einer Pflicht zur Durchführung einer Datenschutz Folgenabschätzung iVm Art. 50 Abs. 1 Bst. c und Art. 51 Abs. 1 Bst. d VE DSG - Art. 17 Abs. 1 und Abs. 4 VE DSG: Beurteilung der Voraussetzungen für die Meldung einer Datenschutz-Verletzung an den Beauftragten iVm Art. 50 Abs. 2 Bst. e und abs. 3 Bst. b VE DSG - Art. 18 iVm Art. 51 Abs. 1 Bst. e VE DSG: Unterlassung der Anwendung datenschutzfreundlicher

					Vorkehrungen - Art 19 Bst. b VE DSG: Pflicht zur Informierung von Daten-Empfängern über Datenschutz-Verletzungen iVm Art. 50 Abs. 3 Bst. a VE DSG Darüber hinaus ist es nach wie vor störend, dass in einem Gesetz, welches sowohl für die Bearbeitung von Personendaten durch private Verantwortliche und Auftragsbearbeiter wie auch durch Angehörige der Bundesverwaltung gilt, nur privatrechtlich tätige bearbeitende Stellen mit Strafsanktionen bedroht werden. Im Weiteren verweisen wir hierzu auf den breit abgestützten Vorschlag der Wirtschaftsverbände: Grundsatz: verwaltungsrechtliche Sanktionen gegen Unternehmen Das DSG soll bei Verstössen gegen die Datenschutzbestimmungen eine Sanktionierung der Unternehmen vorsehen. Anknüpfungspunkt: Organisationsmängel im Unternehmen. Wenn, dann soll lediglich subsidiär eine strafrechtliche Verfolgung von Mitarbeitenden im Rahmen der im BT StGB bereits vorhandenen Strafbestimmungen vorgesehen werden. Anzeigen sollen in der Regel durch die Unternehmen selbst erstattet werden. Im Ergebnis würde eine Anpassung des Sanktionsziels die Situation für die Datenbearbeitenden im Sinne einer Verbesserung des Datenschutzes im Unternehmen massgeblich entschärfen. Sanktionierung der Mitarbeitenden: sollte entsprechend nur bei direkt vorsätzlichem Handeln, das sich gegen die Interessen des Unternehmens und/oder der betroffenen Person richtet, vorgesehen sein. Die schon im BT StGB vorgesehenen Strafbestimmungen dürften für die Bestrafung der natürlichen Person meist schon ausreichen (z.B. Verletzung des Geschäftsgeheimnisses und unbefugte Datenbeschaffung). Der Kreis der potentiell strafrechtlich verantwortlichen Mitarbeitenden müsste zum Vornherein eingeschränkt werden (entsprechend Art. 29 StGB).
Swico	DSG	59			Übergangsbestimmungen: Antrag: Hier ist, analog der Regelung in der DSGVO, eine generelle Übergangsfrist von zwei Jahren vorzusehen.

Swiss Data Alliance
c/o LAUX LAWYERS AG
Attorneys-at-Law
Postfach 360
8024 Zürich

per Email zu Handen: jonas.amstutz@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundeshaus West
3003 Bern

4. April 2017

Stellungnahme zum Vorentwurf zur Totalrevision des Datenschutzgesetzes

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Swiss Data Alliance nimmt hiermit Stellung zur Vernehmlassungsvorlage betreffend Totalrevision des Datenschutzgesetzes (VE-DSG, gemäss Mitteilung des Bundesrats vom 21. Dezember 2016).

Die Swiss Data Alliance wurde am 22. März 2017 als Verein gegründet. Sie setzt sich für eine zukunftsorientierte Datenpolitik ein, damit Daten ihr innovatives Potenzial in der Schweiz voll entfalten können. Unser Kernanliegen ist die richtige Balance zwischen den Ansprüchen der Unternehmen nach Schutz ihrer Investitionen und freier Nutzung ihrer Geschäftsdaten, der Individuen nach Schutz ihrer Privatsphäre und Partizipation an der Verwertung ihrer persönlichen Daten und der Öffentlichkeit nach offenem Zugang zu den von ihr finanzierten Daten der Verwaltung und Forschung (siehe Grundlagendokument, Beilage 4, und Orientierung der Gründerorganisationen, Beilage 5).

Eine Arbeitsgruppe der Swiss Data Alliance hat sich in den letzten Wochen mit der Vorlage beschäftigt und ist dabei zum Schluss gekommen, dass die Totalrevision grundsätzlich überarbeitet werden sollte. Die Arbeitsgruppe empfiehlt, im Interesse einer kurzfristigen Lösung auf Basis des geltenden Datenschutzgesetzes nur die absolut zwingenden Mindestanpassungen anzupacken (Umsetzung der Europaratskonvention 108, Sicherstellung des Schengen-Besitzstands, Erhalt der Gleichwertigkeit im Rahmen einer Teilrevision). Parallel dazu ist die Totalrevision auf der Basis zukunftsorientierter Prinzipien neu zu planen.

Die Überlegungen, welche die Arbeitsgruppe der Swiss Data Alliance zu diesem Schluss geführt haben, werden in den Beilagen erläutert (Prinzipien, Beilage 1; Grundsätzliche Ausführungen, Beilage 2). Zudem werden einzelne Artikel des Vorentwurfes gemäss vorgegebenem Raster kommentiert (Beilage 3).

Mit vorzüglicher Hochachtung

André Golliez, Präsident

Christian Laux, Vizepräsident

Beilagen:

1 Prinzipien
2 Grundsätzliche Kommentierung zum Gesetzgebungsvorhaben
3 Detaillierte Kommentierung zu Einzelbestimmungen zum VE-DSG
4 Grundlagendokument Swiss Data Alliance
5 Orientierung der Gründerorganisationen

Beilage 1: Prinzipien zu Schutz und Nutzung von Personendaten

Dieses Dokument zeigt auf, welche Prinzipien in einer Datenschutzgesetzgebung abgebildet sein sollten:

1. Schutzprinzipien

a) Prinzip 1: Schutz der freien Willens- und Meinungsbildung und Meinungsäusserung in einer Demokratie.

Umsetzung im VE-DSG: Das geltende DSG ist dem VE-DSG diesbezüglich zumindest ebenbürtig.

b) Prinzip 2: Schutz des Einzelnen vor "Blossstellung" dadurch, dass Datenspuren öffentlich bekannt werden.

Umsetzung im VE-DSG: Diesbezüglich führt der Vorentwurf zu keiner Verbesserung. Bereits heute sind einige Aspekte bereits geregelt. Zwar fehlt heute im schweizerischen Recht eine Regelung von Gefährdungen, die nicht absichtlich bewirkt werden (siehe z.B. Art. 173 StGB). Die vom Vorentwurf vorgeschlagene Regelung zur Sanktionierung von unabsichtlich bewirkten Gefährdungen knüpft an Verletzungen der Datensicherheit an (Art. 51 Abs. 1 lit. c VE-DSG). Diese Regel führt zu Rechtsunsicherheit. Der Regelungsansatz von Art. 51 Abs. 1 lit. c VE-DSG (der als „Strafbarkeit von zu wenig Sicherheit" bezeichnet werden kann) ist zu diffus.

c) Prinzip 3: Schutz des Einzelnen vor Missbrauch durch einen privaten Verantwortlichen.

Umsetzung im VE-DSG: Diesbezüglich führt der Vorentwurf in erster Linie zu mehr administrativem Aufwand, ohne allerdings materiell erhebliche Vorteile zu erwirken. Der Gewinn an Transparenz ist zwar klar ausgewiesen, allerdings führt die erwartete Zunahme von Meldungen an das betroffene Datensubjekt zu keiner vorteilhaften Wirkung. Die Informationsflut dürfte sich im Gegenteil nachteilig auswirken. Zwar sind zentrale Neuerungen der EU-DSGVO in den schweizerischen Vorentwurf eingeflossen; diese vermögen am Gesamturteil aber nichts zu ändern, weil die dadurch bewirkte Verbesserung nicht substantiell ist. Zentrale, wirklich innovative Neuerungen sind im Entwurf nicht enthalten; namentlich fehlt ein Recht auf Kopie.

d) Prinzip 4: Kein Missbrauch durch den Staat (wenn der Staat Verantwortlicher ist).

Umsetzung im VE-DSG: Diesbezüglich führt der Vorentwurf zu keiner nennenswerten Verbesserung, da bereits der Status Quo ausreichenden Schutz bietet.

2. Nutzungsprinzipien

a) Das Prozessieren von Daten in Systemen ist grundsätzlich kein Krankheitssymptom, sondern gesellschaftliche Chance, die jedoch vor negativen Auswüchsen zu schützen ist („Missbrauchsgesetzgebung", siehe oben zu den Schutzprinzipien).

b) Die digitale Welt steigert den Wert von geteilter Information innerhalb von Communities, d.h. in Ökosystemen von Nutzern auf Plattformen, Software, Netzwerken und in bestimmten Branchen. Das Teilen von Information bedingt, dass man in Kauf nehmen muss, dass das erste Schutzziel des Datenschutzrechts – „Zugang", d.h. keine Freigabe von personenbezogener Information – sich nicht halten lässt. Man sollte das akzeptieren und besser darauf achten, dass mit personenbezogener Information kein Missbrauch betrieben wird.

c) Kontrolle über Missbräuche bedingt technische, organisatorische und konzeptionelle Mindestinfrastrukturen, welche gesamthaft ein Kaleidoskop ergeben, das sich als Nationale Dateninfrastruktur beschreiben lässt. Im Zentrum derselben steht die elektronische Identität, welche ihrerseits wieder fragmentierte, technische Schutzmassnahmen ermöglicht.

d) Zusammenfassend: Die Antwort auf das Unwohlsein im Datenschutz liegt nicht in erster Linie im Rechtlichen, sondern im Technischen. Dies bedingt, dass die Schweiz datenschutzfreundliche Systeme fördert.

e) Swiss Data Alliance fordert in diesem Sinne einen holistischen Ansatz.

* * *

4. April 2017

<u>Beilage 2</u>: Grundsätzliche Kommentierung zum Gesetzgebungsvorhaben Datenschutzgesetz

Swiss Data Alliance unterbreitet hiermit **grundlegende Kritik zum VE-DSG**, und zwar wie folgt:

A. Fokus der Kommentierung

1 Die nachstehende Kommentierung von Swiss Data Alliance beschränkt sich bewusst auf Themen, die der Frage nachgehen, **ob der VE-DSG die Themen der Zukunft richtig löst**.

2 Swiss Data Alliance <u>kommentiert nicht</u>: Auslandübermittlung, Auftragsdatenbearbeitung, gute Praxis, Datenschutzzertifizierung, Sicherheit von Personendaten oder die Datenbearbeitung durch Bundesorgane, obwohl auch diesbezüglich Kritik angeführt werden könnte und obwohl auch in diesen Bereichen für die Digitalisierung wichtige Weichen gestellt werden könnten.

3 Die Kommentierung von Swiss Data Alliance beschränkt sich namentlich auf die Diskussion, ob:

a. der Vorentwurf den Datenschutz zu einer sinnbefreiten Compliance-Übung verkommen lässt (z.B. in Form von übersteigerten Hinweispflichten, mit denen Datensubjekte fortan „geflutet“ zu werden drohen),

b. die aus Sicht der Wirtschaft im Digitalen notwendig erscheinenden Datennutzungen möglich sind (Big Data Auswertung, andere Formen von Analytics) und der Markt Schweiz entsprechend wettbewerbsfähig bleibt (auch für KMU; auch unter Berücksichtigung der Strafbestimmungen),

c. gleichwohl zentrale Schutzgrundsätze in Bezug auf Personendaten erfüllt sind, und

d. die Gesetzgebungsziele des Bundesrats umgesetzt werden.

4 Soweit die vom Bundesrat angestrebten **Ziele dieser Totalrevision** des DSG (Vernehmlassungsbericht des Bundesrats (S. 17 f.)) angesprochen sind, geht es um Folgendes:

a. **Ziel #1: Materielle Verbesserung**, um dem technischen Wandel Rechnung zu tragen

b. **Ziel #2:** Erhaltung und Stärkung der **Wettbewerbsfähigkeit** der Schweiz

c. **Ziel #3:** Umsetzung der Vorgaben der **Europaratskonvention 108**

d. **Ziel #4:** Nachvollzug des **Schengen-Acquis** (Richtlinie [EU] 2016/680)

e. **Ziel #5:** Erhältlichkeit eines **Gleichwertigkeitsbescheids der EU-Kommission** und damit Angleichung an die EU-Datenschutzgrundverordnung

B. Inhaltliche Stellungnahme zum Vorentwurf (VE-DSG)

1. In Bezug auf die Revisionsziele

5 Swiss Data Alliance bewertet die Ziele des Bundesrats (siehe Rz. 4) grundsätzlich positiv. In Bezug auf die Frage, ob die Revisionsziele umgesetzt sind, lässt sich Folgendes festhalten:

- **Ziel #1**: Die zentralen Schutzgrundsätze im Datenschutzrecht werden grundsätzlich verbessert; man könnte diesbezüglich aber noch zielgerichteter wirken. Das Ziel wird zwar erreicht; Swiss Data Alliance ist diesbezüglich aber nicht euphorisch.

- **Ziel #2**: Die Schweiz droht mit dem Entwurf an Wettbewerbsstärke zu verlieren. Ausserdem verkommt der Datenschutz immer mehr zur „Compliance-Übung", was hohe Kosten ohne materiellen Nutzen nach sich ziehen wird. Ziel #2 wird klar nicht erreicht. Swiss Data Alliance ist diesbezüglich sehr besorgt.

- **Ziele #3 - #5**: Erreicht. Teilweise allerdings mit überschiessendem Swiss Finish. Swiss Data Alliance lehnt Swiss Finish ab.

2. In Bezug auf die Gleichwertigkeit mit der Regelung der EU

6 Für Ziel #5 (die Gleichwertigkeit) sind unseres Erachtens die folgenden Elemente zentral:

a. Beibehalten der Achtung von Datenschutz in „institutionalisierter Form" (Verfassungsbestimmung mit DSG als grundlegendes Gesetz);

b. Rechtsstaatlicher Umgang mit Datenschutz;

c. Achtung von Datenschutz innerhalb der Behördentätigkeit;

d. Verlässlichkeit des Schweizerischen Rechtssystems;

e. Existenz von unabhängigen Aufsichtsbehörden (oder einer solchen Behörde)

f. Einhaltung der Mindeststandards der Europaratskonvention 108, namentlich neu: Automatisierte Einzelfallentscheidungen, Regelungen betr. Data Breaches;

g. Ernsthaftigkeit von Sanktionen.

7 Mit Blick darauf, dass z.B. auch ein Regelwerk wie jenes des Privacy Shield genügt, um Gleichwertigkeit herzustellen, muss es Motto für die schweizerische Gesetzgebungstätigkeit sein, ernsthaft und verbindlich zu regulieren, aber nicht zu „überschiessen". Die vorstehend bezeichneten sieben Eigenschaften (Rz. 6, a.-g.) weist die schweizerische Datenschutzgesetzgebung im Übrigen auf. Es ist zu erwarten, dass der Schweiz die Gleichwertigkeit auch nach der Revision zugesprochen werden wird.

3. In Bezug auf die Kernprinzipien (gemäss unserem Anhang 1)

8 Der Vorentwurf löst die in unserem Anhang 1 beschriebenen Aufgabenstellungen nicht.

4. In Bezug auf den Fokus der Kommentierung von Swiss Data Alliance

9 Der vorn genannte Kommentierungsfokus von Swiss Data Alliance (vorn, Rz. 3) resultiert zusammenfassend in den folgenden Aussagen:

- **„Compliance"** (Rz. 3, Punkt a.): Das Regelungskonzept des VE-DSG beschränkt sich auf Korrekturmassnahmen an den Stellschrauben „Informationspflicht" und „Einwilligung". Visionäre Weiterentwicklung geht dem Vorentwurf ab. Damit fördert der Vorentwurf die nicht unproblematische Tendenz, dass Datenschutz zu einer „Compliance-Übung" verkommt.

- **Data Analytics** (Rz. 3, Punkt b.): Der Vorentwurf enthält – namentlich mit dem in Anhang 3 im Einzelnen kritisierten Begriff des „Profiling" (bzw. seiner Ausgestaltung) – Bestimmungen, die Data Analytics praktisch verunmöglichen. Data Analytics stellt eine zentrale, für die Wirtschaft notwendig erscheinende Datennutzung dar. Aus dem Vorentwurf resultiert somit eine Beeinträchtigung der Wettbewerbsfähigkeit der Schweiz. Davon ist abzusehen.

- **Schutz von Personendaten** (Rz. 3, Punkt c.): Grundsätzlich wäre der Datenschutz in der Schweiz auch bei Annahme des VE-DSG gewährleistet. Allerdings ist auf eine zusätzliche negative Wirkung des bereits vorstehend kritisierten „Compliance-Aspekts" hinzuweisen: Wer reguliert, ohne dass dem Rechtsunterworfenen klar wird, warum die regulierten Massnahmen notwendig wird, provoziert Gegendruck oder fehlende Akzeptanz auch dort, wo die Regulierung (hier: das Datenschutzrecht) berechtigt oder sogar zwingend erforderlich ist (siehe zu den Kernprinzipien unseren Anhang 1). Das „Überschiessen" in Bezug auf Compliance-Aspekte erweist „echtem" Datenschutz also einen Bärendienst.

- **Gesetzgebungsziele** (Rz. 3, Punkt d.): Siehe hierzu bereits Rz. 5.

C. Empfehlungen

10 Insgesamt kommt Swiss Data Alliance zur folgenden Empfehlung: Der Vorentwurf sollte fundamental überarbeitet werden. Im Einzelnen empfiehlt Swiss Data Alliance Folgendes:

1. Totalrevision mit Orientierung an Kernprinzipien

11 Die Swiss Data Alliance steht einer Totalrevision grundsätzlich positiv gegenüber. Allerdings stellt Swiss Data Alliance Folgendes fest: Die zentralen Fragen, die für die Datenwirtschaft und –gesellschaft in der Schweiz gelöst werden müssen, sind im Vorentwurf nicht adressiert (siehe soeben Ziffer 3, Rz. 8, und Anhang 1).

12 Der Bundesrat hat die **EU-DSGVO** offenbar als Verschärfung wahrgenommen. Das ist verständlich, stellt aber eine einseitige Wahrnehmung bzw. Gewichtung von zwei gegenläufigen Strömungen in der EU-DSGVO dar. Während die EU-DSGVO zusätzliche Rechte geschaffen hat, muss man doch betonen, dass die EU-DSGVO innereuropäisch in nicht unerheblicher Weise als Abbau von Hürden verstanden wird.

Abbau von Hürden:

- Abbau von Genehmigungen und Notifikationen, namentlich beim Beizug von Dienstleistenden (siehe z.B. für einen Überblick über die bisher geltenden Pflichten zu Notifikationen und Genehmigungen https://cloudprivacycheck.eu/at/tool) („Auftragsdatenbearbeitung“)
- Vereinheitlichung der länderübergreifenden Zusammenarbeit der Aufsichtsbehörden

Neue Rechte:

- Privacy by Design (Artikel 25 EU-DSGVO: „Datenschutz durch Technikgestaltung“)
- Privacy by Default (Artikel 25 EU-DSGVO: „Datenschutzfreundliche Voreinstellungen“)
- Bearbeitungsreglement (Artikel 30 EU-DSGVO)
- Datenschutzfolgeabschätzung (Artikel 35 EU-DSGVO)
- Datenschutzverantwortlicher (Artikel 37 EU-DSGVO)
- Data Breach Notifications (Artikel 33 f. EU-DSGVO)
- Pflichten bei Vorliegen oder Abstellen auf Genehmigte Verhaltensregeln (Artikel 40 EU-DSGVO)
- Datenübertragbarkeit (Artikel 20 EU-DSGVO)
- Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall (Artikel 21 und 22 EU-DSGVO)
- Profiling (Artikel 22 EU-DSGVO)

13 Das Thema „Verschärfung“ der Informationspflichten und dergleichen sollte – auch mit Blick auf das Verständnis in der EU – nicht im Zentrum stehen. Vielmehr sollte sich die Totalrevision an den folgenden Prinzipien orientieren:

a. Swiss Data Alliance empfiehlt, sich im Rahmen einer erneuten Überarbeitung an den Kernprinzipien gemäss Anhang 1 zu orientieren. Datenschutz soll nicht zu einer „Compliance-Übung“ verkommen.

b. Erhalt der Gleichwertigkeit zur EU (Angemessenheitsbeschluss): Swiss Data Alliance empfiehlt, den Mindestinhalt des zu revidierenden DSG entlang der in Rz. 6 genannten Punkte festzulegen, das DSG ansonsten aber von unnötigem Ballast frei zu behalten.

c. Die Wettbewerbsfähigkeit der Schweiz ist zu erhalten (siehe namentlich auch die nachstehenden Empfehlungen betr. KMU-Tauglichkeit und „Swiss Finish“).

2. Datennutzungsregelung in Ergänzung zu den Schutzprinzipien

14 Swiss Data Alliance empfiehlt, die Chance einer Totalrevision dazu zu nutzen, nicht nur die *Datenschutz*-, sondern ergänzend auch die *Datennutzungs*gesetzgebung voranzubringen.

15 Ob die zu schärfende Datennutzungsregelung im Datenschutzgesetz stehen muss, ist letztlich eine formale Frage. Aber es bietet sich jetzt eine grosse Chance: Der Datenschutz kann entschlackt und geschärft werden. Gleichzeitig sollten benachbarte Themen mit Datenbezug angepackt werden (namentlich: Datennutzungsfragen). Mit einem solchen Ansatz erhielte die Schweiz eine datenbezogene Regulierung, die für die Zukunft vorbereitet ist.

16 Dieser Ansatz steht im Einklang mit der Forderung der OECD von Oktober 2015 (Data Driven Innovation:

> *„Seizing the benefits from DDI [= Data Driven Innovation] requires government action. […] They thereby need to strike the right balance between the social benefits of enhanced reuse and sharing of data and analytics, and individuals’ and organisations’ legitimate concerns about such openness […].”*

3. Berücksichtigung der Bedeutung des Revisionsvorhabens für KMU

17 Swiss Data Alliance fordert, die Auswirkungen des VE-DSG für kleinere KMU's ("Micro-Unternehmen") besser auszutarieren. Es dürfen keine Regeln im Entwurf stehen, welche die grosse Zahl der für die Schweiz wichtigen Kleinstunternehmen in übermässiger Weise belasten. Es ist zu prüfen, ob die Umsetzbarkeit der im Vorentwurf vorgeschlagene Normen für solche Unternehmen machbar ist. Andernfalls sind spezielle Lösungen für kleinere Unternehmen vorzusehen, welche diese von Pflichten entlasten, die für sie nicht erforderlich sind. Diese Forderung steht im Einklang mit dem Bericht Data Driven Innovation der OECD von Oktober 2015:

> *„Governments should […] focus on **small and medium enterprises** […]. They must address shortages of **data specialist skills**, which points to missed opportunities for job creation."*

18 Unter der EU-DSGVO bestehen Erleichterungen zum Erlass von Bearbeitungsreglementen für Unternehmen von weniger als 250 Mitarbeitenden (Art. 30 Abs. (5) EU-DSGVO: "Verzeichnis von Verarbeitungstätigkeiten"). In Bezug auf Compliance-Dokumentation, die erhebliche Kosten auslösen können, gibt es zwar auch unter EU-DSGVO keine ergänzenden Erleichterungen. Aber jedenfalls die Schweiz sollte diesbezüglich vorausschauend regulieren. Die Schweiz muss für Startups attraktiv bleiben.

19 Swiss Data Alliance empfiehlt dem Bundesrat, diesbezüglich Vereinfachungen vorzusehen, die Startup-Gründungen sowie die erfolgreiche Führung von Startups ermöglichen.

4. Verzicht auf unnötig verschärfende schweizerische Besonderheiten (kein unnötiger „Swiss Finish")

20 Es wäre konzeptionell verfehlt, über die Standards der Europaratskonvention 108 sowie der DSGVO hinauszugehen. Solches „Überschiessen" wird hier als „Swiss Finish" bezeichnet.

21 „Swiss Finish" sollte im Zweifel unterbleiben. „Swiss Finish" sollte nur dann in Betracht gezogen werden, wenn im Vergleich zur Regelung im Ausland der Abweichungsbedarf klar ausgewiesen ist. In Bezug auf die konkrete Regelung muss mit anderen Worten der Nachweis erbracht worden sein, dass dank der Schweizerischen Eigenart:

- eine materielle Verbesserung der Regelung erzielt werden kann (**Ziel #1**). Das heisst: Die neue Regelung muss ein sich heute stellendes Problem vorausschauend lösen;
- die Regel eines der Kernprinzipien im Datenschutz betrifft (dazu die Prinzipien 1-4, siehe sogleich) und nur mit der Regel eine tragfähige Lösung für die Zukunft möglich scheint (**Ziel #1**);
- eine Erhaltung bzw. Stärkung der Wettbewerbsfähigkeit der Schweiz erreicht werden kann (**Ziel #2**);
- die Regel im Vergleich zur Regel im Ausland für alle involvierten Personen zu einer Erleichterung führt (mit anderen Worten: Verschärfungen sind vermutungsweise schädlich) (Wettbewerbsfähigkeit Schweiz, **Ziel #2**);
- die Regel zwar zu einer Verschärfung führt, dafür aber andere Regeln über Bord geworfen werden können (mit anderen Worten: Effizienzsteigerung) (Wettbewerbsfähigkeit Schweiz, **Ziel #2**).

22 Demgegenüber muss Folgendes festgehalten werden: „Swiss Finish", der ohne Rechtfertigung auf Verschärfungen (im Sinne von zusätzlichen Hürden für private Verantwortliche) im Vergleich zum EU-Niveau hinausläuft, führt vermutungsweise zu einer Verschlechterung der Wettbewerbsfähigkeit der Schweiz[1]. Dem Ziel #2 (Rz. 4) steht unnötig verschärfender Swiss Finish klar entgegen.

---

[1] In Beilage 3 findet sich solcher Swiss Finish in den folgenden Punkten: SWIDA-6 (Art. 3 lit. f), SWIDA-7 (Art. 3 lit. i), SWIDA-8. (Art. 5 Abs. 5), SWIDA-9. (Art. 5 Abs. 6), SWIDA-10. (Art. 7 Abs. 3), SWIDA-11. (Art. 12), SWIDA-12. (Art. 13 Abs. 4),

D. Insbesondere: Recht auf Datenportabilität bzw. Recht auf Kopie (Empfehlung)

1. Vorbemerkungen

23 Der Bericht zum VE-DSG hält fest, dass das Recht auf Datenübertragbarkeit, wie es Artikel 20 der Verordnung (EU) 2016/679 vorsieht, "mehr darauf ausgerichtet (ist), den betroffenen Personen die Wiederverwendung ihrer Daten zu ermöglichen, um den Wettbewerb spielen zu lassen, als ihre Persönlichkeit zu schützen. Es scheint daher problematisch, eine entsprechende gesetzliche Regelung zu erlassen." (Bericht zum VE-DSG, Seite 22). Zusätzlich sieht der Bericht Schwierigkeiten bei der Umsetzung dieses Rechtes, "da es die gegenseitige Abstimmung unter den Verantwortlichen und zweifellos eine – zumindest implizite – Einigung über die verwendeten Datenträger und Informatikstandards voraussetzt." (Bericht zum VE-DSG, Seite 22). Eine Regulierungsfolgenabschätzung habe zudem gezeigt, dass sich die Einführung eines Rechtes auf Datenübertragbarkeit als sehr kostenintensiv erweisen könnte. Daher seien "die Ergebnisse der Erfahrungen innerhalb der Europäischen Union abzuwarten, bevor die Einführung eines Rechts auf Datenportabilität in Betracht gezogen wird." (Bericht zum VE-DSG, Seite 22).

24 **Swiss Data Alliance teilt diese Sichtweise nicht.**

25 Die Datenübertragbarkeit ist ein Kernelement der neuen EU Datenschutzgrundverordnung. Diesen Punkt von der Revision des DSG auszuschliessen, widerspricht der expliziten Zielsetzung der Revision, die Schweizer Datenschutzgesetzgebung der Verordnung der EU anzunähern (siehe vorn, Rz. 4, Punkt e., **Ziel #5**, und Bericht zum VE-DSG, Seite 5).

26 **Swiss Data Alliance fordert, dass mit der laufenden Gesetzgebung auch ein Recht auf Kopie in die Schweizerische Gesetzgebung eingeführt wird.** In den nachfolgenden Abschnitten führt Swiss Data Alliance Ergänzendes bzw. Erläuterndes zur Begründung an.

2. Begriffliches zum Recht auf Kopie bzw. Recht auf Datenportabilität

27 Das „Recht auf Kopie" sowie das „Recht auf Datenportabilität" sind zwei Teilgehalte des „Rechts auf Datenübertragbarkeit" gemäss Art. 20 EU-DSGVO:

- Das Recht auf Kopie ist der umfassendere Anspruch, weil ein Herausgaberecht (im massgeblichen Datenformat) unter dem Recht auf Kopie voraussetzungslos und ohne Nachweis einer Weiterverwendungsabsicht oder –möglichkeit bzw. ohne Angabe einer Zielinfrastruktur besteht (bestehen muss). In der EU-DSGVO kommt das Recht auf Kopie in der folgenden Formulierung zum Ausdruck: „*Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten*".

- Das Recht auf Datenportabilität gemäss Art. 20 EU-DSGVO ergänzt das Recht auf Kopie um zwei Aspekte: erstens wird dem (bisherigen) Anbieter verboten, die Weiterverwendung von „bereitgestellten Daten" im Sinne von Art. 20 EU-DSGVO vertraglich zu untersagen bzw. zu beschränken; zweitens hat die betroffene Person das Recht zu erwirken, „dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist" (wobei dieses Wahlrecht im Moment des Herausgabeentscheids ausgeübt werden muss).

SWIDA-13. (Art. 15 Abs. 1), SWIDA-14. (Art. 16), SWIDA-15. (Art. 17 Abs. 1), SWIDA-20. (Art. 20 Abs. 3), SWIDA-22 (Art. 23 Abs. 2 lit. d), SWIDA-24. (Art. 50 ff.).

3. Bedarf nach ergänzender Analyse und Diskussion

28 Swiss Data Alliance fordert, die Diskussion zum Recht auf Kopie mit verbesserten Detailkenntnissen zu führen.

29 Der Nutzen eines Rechts auf Kopie im Schweizerischen Recht, und zum Risiko defensiver Regulierung:

- Paradigmenwechsel. Das Recht auf Datenportabilität ist ein grundsätzlicher Paradigmenwechsel in der Datenbearbeitung: das Individuum ist nicht länger nur Objekt der Datenbearbeitung durch Unternehmen und Organisationen ("Datenobjekt"), das vor dem Missbrauch dieser Daten durch Dritte zu schützen ist, sondern es wird zum aktiven Subjekt, das sein Recht zur eigenständigen Nutzung der Daten, die sich auf seine Person beziehen, in Anspruch nimmt ("Datensubjekt"). Damit kann jede Person an der Verwertung ihrer Daten partizipieren. Die Kontrolle des Einzelnen über die Zweitnutzung seiner eigenen Daten bringt zudem neue Innovationsmöglichkeiten in der Nutzung von Daten, da nur die einzelne Person die unterschiedlichsten Daten miteinander verbinden kann. Der Bericht ignoriert diesen fundamentalen Paradigmenwechsel hin zur digitalen Selbstbestimmung, der sich ohne Zweifel in den kommenden Jahren durchsetzen wird.

- Verbesserte Datennutzung: Insbesondere bietet die Datenportabilität der betroffenen Person auch die Möglichkeit, weitere Daten mit ausgewählten Unternehmen zu teilen. Unternehmen können so neue und bessere Dienstleistungen anbieten und es entstehen dadurch neue Innovations- und Geschäftsmöglichkeiten. Über ein Dutzend britischer Grossbanken hat bereits vor zwei Jahren mit der Einführung des Midata-Standards für die Datenportabilität gezeigt, dass solche Lösungen mit relativ geringem Aufwand realisiert werden können und bei den Kunden auf grossen Anklang stossen.

- Relevanz für den Persönlichkeitsschutz. Das Recht auf Datenportabilität ist gerade mit Blick auf den Persönlichkeitsschutz von zentraler Bedeutung, d.h. also nicht nur in Bezug auf den Wettbewerb (unter Anbietenden). Ein Nutzer hat mit diesem Recht die freie Wahl, eine Plattform zu verlassen, wenn diese ihre Persönlichkeitsrechte nicht ausreichend schützt, bzw. eine andere Plattform einen besseren Schutz anbietet. Die Datenportabilität ist geeignet, im Wettbewerb jene Anbieter zu fördern, die dem Nutzer einen besseren Persönlichkeitsschutz anbieten. Wird dieses Recht nicht eingeführt, ist der Nutzer, der seine Daten nicht mitnehmen kann, auf Gedeih und Verderb dem jeweiligen Anbieter ausgeliefert, der seine Daten kontrolliert.

- Sowieso-Anwendbarkeit. 80% aller Schweizer Unternehmen, welche zumindest mit einem EU-Land geschäftliche Beziehungen unterhalten, werden ab Mai 2018 in jedem Fall dazu gezwungen sein, die Datenportabilität gemäss Artikel 20 der EU-Datenschutzgrundverordnung im Rahmen dieser Geschäftsbeziehungen zu gewährleisten.

- Gefährdung des Standorts Schweiz. Eine defensive und abwartende Haltung, wie im Bericht vorgeschlagen, ist kurzsichtig und setzt den Standortvorteil der Schweiz bezüglich Datenschutz und der informationellen Selbstbestimmung grobfahrlässig aufs Spiel. Würde sich die Haltung des VE-DSG durchsetzen, würde dies dazu führen, dass Privatpersonen bezüglich ihrer Datenrechte gegenüber Schweizer Anbietern schlechter gestellt wären als gegenüber solchen der EU. Die zunehmend datenbewussten Kunden werden daher zu EU-Anbietern abwandern und die Schweiz wird ihren anerkannten Vorsprung auf dem Gebiet des Datenschutzes in kurzer Zeit verlieren. Um eine solche Entwicklung zu vermeiden, benötigt die Schweiz eine aktive und pragmatische Vorwärtsstrategie bezüglich der Datenportabilität.

30 Swiss Data Alliance fordert, den Nutzen von Datenportabilität bzw. vom Recht auf Kopie zur Kenntnis zu nehmen und diesbezüglich gesetzgeberisch tätig zu werden.

4. Kommentar zum Vorgehen (Abschreibung des Postulats Derder) (15.4045)

31 Im November 2015 hat der Bundesrat das Postulat **Recht auf Kopie** von NR Fathi Derder (15.4045) entgegengenommen, um eine Antwort im Rahmen der nun vorliegenden Gesetzesrevision zu erteilen. Bis jetzt ist diese Antwort nicht erfolgt. Der Bericht führt das Postulat Derder unter der Rubrik der teilweise abgeschriebenen parlamentarischen Vorstösse auf und hält dazu fest: "Nach Auffassung des Bundesrates ist es nicht wünschenswert, bei der Revision des DSG ein Recht auf Datenportabilität einzuführen" (Bericht zum VE-DSG, Seite 38). – Die Swiss Data Alliance ist wie gesagt inhaltlich nicht dieser Meinung und hält die Einführung des Rechtes auf Datenportabilität im Sinne eines Rechtes auf Kopie in der Schweizer Datenschutzgesetzgebung vielmehr für dringend notwendig.

32 Swiss Data Alliance stellt in dieser Hinsicht eine unangemessene Reaktion des Bundesrats auf das Postulat Derder (15.4045) fest und fordert diesbezüglich eine transparente und formelle Beantwortung des Postulats Derder.

5. Ergänzendes

33 Swiss Data Alliance führt sodann Ergänzendes technischer und organisatorischer Art sowie Umsetzungshinweise an:

- Swiss Data Alliance weist darauf hin, dass die Datenportabilität (als Teilgehalt der Datenübertragbarkeit, wie vorn umschrieben) die betroffenen Daten als Einheit (rivalisierendes Gut) versteht. Daten würden gemäss „Datenportabilität" (wie vorn als Teilgehalt definiert) von A nach B verschoben (unter gleichzeitiger Löschung des Datenstands am Ort A), dürften (aus der Optik des Anbieters) bzw. könnten (aus der Optik des Nutzers bzw. Datensubjekts) dann aber nicht mehr an beiden Orten (A und B) gleichzeitig (und allenfalls unterschiedlich) genutzt werden.

- Das Recht auf Kopie (ebenfalls als Teilgehalt der Datenübertragbarkeit, wie vorn umschrieben) betont demgegenüber die Kopierbarkeit der Daten. Das Recht auf Kopie überlässt die Daten dem Ersteller (Arzt, Spital, Unternehmen), ermöglicht aber gleichzeitig, dass das Datensubjekt mit der Kopie über Zweitnutzungen verfügen kann. Da das Datensubjekt dazu legitimiert ist, unterschiedlichste Typen persönlicher Daten zusammenzuführen, können unter seiner Kontrolle neue Wertschöpfungs- und Innovationsmöglichkeiten entstehen. Darin besteht der eigentliche Wert des Rechts auf Kopie.

- Da der VE-DSG die vorstehend bestehenden Differenzierungen nicht vornimmt, verpasst der VE-DSG eine Chance.

- Das Recht auf Kopie sowie das Recht auf Datenportabilität bedürfen tatsächlich gemeinsamer **Informatikstandards** der Anbieter, damit die Übertragung der Daten mit möglichst geringem Aufwand durchgeführt werden kann. Der Bericht befürchtet in diesem Zusammenhang in erster Linie Schwierigkeiten bei der Umsetzung und nimmt auch hier eine defensive und kurzsichtige Haltung ein. Vorausschauende und kundenorientierte Unternehmen werden den Vorteil solcher Standards erkennen und deren Einführung als kompetitiven Vorteil gegenüber zögerlichen oder abwehrenden Konkurrenten nutzen.

34 Swiss Data Alliance spricht sich für eine aktive Vorwärtsstrategie zum Recht auf Kopie und ggf. zum Recht auf Datenportabilität aus.

35 Zur Kostenargumentation im Begleitbericht: Im Bericht werden schliesslich die Kosten moniert, welche mit der Einführung der Datenportabilität verbunden wären. Dazu Folgendes:

- Der Bericht bezieht sich dabei auf eine Regulierungsfolgenabschätzung, die bis anhin nicht öffentlich zur Verfügung steht. Dies nimmt dem Einwand von vornherein Überzeugungskraft.

- Die im VE-DSG angeführten Aussagen zu den kostenseitigen Regulierungsfolgen dürfen grundsätzlich angezweifelt werden. Unternehmen und Organisationen sind im Zeitalter von Big Data ohnehin mit steigenden Kosten für das Management ihrer Daten konfrontiert. Der Anspruch auf Datenportabilität ist nur einer unter zahlreichen Herausforderungen in der Datenwirtschaft. Die monierten Kosten müssen in diesem grösseren Zusammenhang betrachtet werden, und dürfen nicht als isolierte Einzelmassnahme verstanden werden. Insbesondere setzt ja bereits das Informationsrecht voraus, dass persönliche Daten in einem lesbaren Format eingesehen werden können.

- Weil der VE-DSG Kostenüberlegungen bzw. Regulierungsfolgen zur Begründung anführt, obwohl diese Begründungen ganz offensichtlich auf einer zu wenig differenzierenden Sicht der technischen und wirtschaftlichen Ausgangslage beruhen, ist der VE-DSG in dieser Hinsicht von vornherein wenig überzeugend. Konkret: Wird ein blosses Recht auf Kopie begründet, entstehen beim neuen Dienstleister („am Ort B") zunächst einmal gar keine Kosten. Beim bestehenden Dienstleister (am Ort A) entstehen zwar Kosten. Diese können aber gering behalten werden, wenn eine flexible Gesetzgebung umgesetzt und dem Bundesrat eine Verordnungskompetenz gegeben wird, die Regulierung auf sich verbessernde Standards anzupassen. Dem Bundesrat sollte die Kompetenz zur Regelung von Standardisierungsfragen per Verordnung gegeben werden.

36 Swiss Data Alliance spricht sich für eine aktive Vorwärtsstrategie zum Recht auf Kopie und ggf. zum Recht auf Datenportabilität aus.

37 Zum Zeitpunkt der Neuregelung: Es ist von grosser Bedeutung, das Recht auf Kopie bereits mit der jetzt laufenden Revision des Datenschutzgesetzes im Schweizerischen Recht zu regeln. Dies aus den folgenden Gründen:

a. Das Recht auf Kopie hat zwar eine teilweise breitere Stossrichtung als das ausschliesslich auf persönliche Aspekte bezogene Datenschutzrecht, aber es weist vielfältige Bezugspunkte dazu auf (siehe die Kommentare in Beilage 3 zum Profiling, zu Art. 12 VE-DSG, etc.[2]). Diese Bezugspunkte sind nicht zufällig (siehe sogleich, Punkt 37b).

b. In der Informationsgesellschaft hat jede Form von Information einen vielfältigen Bezug zu vielen Lebensbereichen. Eine rein formale Trennung in „personenbezogene" und „nicht personenbezogene" Information ist in der Praxis oft zufällig. Entsprechend ist es auch nicht zulässig, die Regelung des Rechts auf Kopie mit der Begründung zu verzögern, dass es nicht klassisches (Personen-)Datenschutzrecht beschlägt. Das Recht auf Kopie muss jetzt angegangen werden.

38 Ob das Recht auf Kopie formal im Datenschutzgesetz zu regeln ist oder in einer Nebengesetzgebung, ist von untergeordneter Bedeutung. Der Schluss, dass das Recht auf Kopie deswegen nicht in die laufende Revision des Datenschutzgesetzes gehörte, wäre aber eine wenig überzeugende Position (siehe zur Begründung vorn, Rz. 37). Inhaltlich hielte Swiss Data Alliance eine solche Position für nicht akzeptabel.

* * *

Swiss Data Alliance / Zürich, 4. April 2017

---

2 Siehe in Beilage 3 die Kommentare SWIDA-6., SWIDA-11., SWIDA-22.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Swiss Data Alliance (Verein), Zürich

Abkürzung der Firma / Organisation : SWIDA
Adresse : c/o LAUX LAWYERS AG, Seegartenstrasse 2, Postfach 360, 8024 Zürich
Kontaktperson : RA Dr. Christian Laux
Telefon : 044 880 24 24
E-Mail : christian.laux@lauxlawyers.ch
Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 .Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen	
Name/Firma	**Bemerkung/Anregung**
Swiss Data Alliance [SWIDA-1.]	Wir verweisen hier auf unser Begleitschreiben und die diesem angehängten Separatdokumente. Wir bitten Sie höflich um inhaltliche Auseinandersetzung mit diesen und würden uns freuen, diese im Gespräch bei Bedarf zu verdeutlichen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Swiss Data Alliance [SWIDA-2.]	VE-DSG	3		e	Antrag: Korrektur der folgenden Definitionen: **Bekanntgabe / Bekanntgeben**: Offenbaren von Personendaten an einen Dritten, der nicht Auftragsdatenbearbeiter ist. Begründung: **Für die vorgenannten, wesentlichen Begriffe, fehlen z.T. Definitionen, was in der Praxis der Digitalisierungsbestrebungen von Unternehmen teilweise zu Problemen führt.** Die Begriffe „Übermittlung", „Übertragung" und „Bekanntgabe" sollten konsequent mit unterschiedlichem Gehalt verwendet werden, wobei zusätzlich der Begriff der Offenbarung als wesentliches Abgrenzungskriterium definiert werden sollte (zur Abgrenzung zwischen code layer und content layer siehe Weber/Laux/Oertly, Datenpolitik als Rechtsthema, Zürich 2016, 5), wie folgt: • Übermittlung: Übermittlung liegt vor, wenn einer der folgenden Vorgänge gemeint ist: (i) Verschiebung Daten von einem Datenträger auf einen anderen Datenträger, sei es nun ein eigener Datenträger oder ein Datenträger eines Dritten, ungeachtet des Umstands, ob ein Offenbaren resultiert (auf dem content layer) oder nicht (z.B. wenn nur verschlüsselte Daten übermittelt werden); (ii) Offenbaren von Informationen (Personendaten) an einen Dritten ausserhalb einer Datenspeicherung (blosse Einsichtnahme). Dieser Begriffsgehalt dürfte in Art. 5 und 6 VE-DSG gemeint sein. • Übertragung: Übertragung meint den der Auftragsdatenbearbeitung vorgelagerten Vorgang, wobei nach der bisher geltenden Rechtslage keine Differenzierung vorgenommen wurde danach, ob (a) der Auftragsdatenbearbeiter nur intransparente Daten bearbeitet (d.h. im Normalbetrieb ohne Zugriff auf die Inhaltsebene, wie es z.B. für einen modern organisierten Betreiber von Rechenzentren der Fall ist) oder ob (b) der Auftragsdatenbearbeiter in einer für ihn transparenten Weise auch die Inhaltsebene (content layer) bearbeitet (wie es z.B. für einen Dienstleister der Fall ist, der eine Versicherungsgesellschaft im Underwriting unterstützt). Übertragung ist ein Unterfall der Übermittlung. • Bekanntgabe: Bekanntgabe meint das Zugänglichmachen von Personendaten bei gleichzeitiger Offenbarung (oder Möglichkeit zur Kennntnisnahme) ohne dass ein Fall der Auftragsdatenbearbeitung gemäss Art. 7 VE-DSG (d.h. eine „Übertragung") vorliegt. Der Begriff der Bekanntgabe wird in Art. 5 und 6 sowie in Art. 13 und 14 VE-DSG thematisiert. Bekanntgabe ist ebenfalls ein Unterfall der Übermittlung. • Offenbaren: Einsichtnahme in den content layer von Personendaten, d.h. unter tatsächlicher Möglichkeit des Erkennens des inhaltlichen Gehalts von Personendaten (z.B. Ansicht über eine Applikation, über einen Bildschirm, oder dergleichen). Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzept im DSG
Swiss Data Alliance [SWIDA-3.]	DSG	3		Neu	Antrag: Aufnahme der folgenden Definition: **Übermittlung / Übermitteln**: Zugänglichmachen von Personendaten in Form der Bekanntgabe, der Übertragung. Eine Übermittlung liegt auch vor, wenn Personendaten in Verbindung mit

					Massnahmen, die eine Offenbarung ausschliessen, einem Dritten zugänglich gemacht werden. Begründung: siehe den Kommentar zu Art. 3 lit. e VE-DSG. Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzept im DSG
Swiss Data Alliance [SWIDA-4.]	DSG	3		Neu	Antrag: Aufnahme der folgenden Definition: **Übertragung / Übertragen**: Einbezug eines Auftragsbearbeiters in die Bearbeitung von Personendaten, mit oder ohne Offenbarung der Personendaten gegenüber dem Auftragsbearbeiter. Begründung: siehe den Kommentar zu Art. 3 lit. e VE-DSG. Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzept im DSG
Swiss Data Alliance [SWIDA-5.]	DSG	3		Neu	Antrag: Aufnahme der folgenden Definition: **Offenbarung / Offenbaren**: Ermöglichen der Einsichtnahme in die in Personendaten enthaltenen Angaben (content layer). Begründung: siehe den Kommentar zu Art. 3 lit. f VE-DSG. Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzept im DSG
Swiss Data Alliance [SWIDA-6.]	DSG	3		f	Antrag: Art. 3 lit. f ist wie folgt zu ändern: *Profiling:* jede automatisierte Auswertung von ~~Daten oder~~ Personendaten um wesentliche persönliche Merkmale einer betroffenen Person zu analysieren oder Entwicklungen einer betroffenen Person vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität Begründung: Die im VE-DSG vorgeschlagene Definition von „Profiling“ ist **zu breit**: Bereits eine „von Hand“ bearbeitete Mitarbeiterbeurteilung würde als “Profiling“ nach Art. 23 Abs. 2 Bst. d VE-DSG gelten. Das kann nicht gewollt sein. **Swiss Finish**: Der Begriff „Profiling“ gemäss VE-DSG soll die Auswertung von Daten verbieten. Die EU-DSVGO (Art. 22 Abs. 1 EU-DSGVO) schützt demgegenüber nur vor Entscheiden, welche ihr [sc.: d.h. der betroffenen Person] gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise [sc.: wie durch rechtliche Wirkung] erheblich beeinträchtigt“. Mit anderen Worten wäre die neue Regelung im VE-DSG wohl wie folgt zu verstehen: • Es wäre auch nach dem VE-DSG nicht bzw. nur im Rahmen der Bearbeitungsgrundsätze von Art. 4 VE-DSG verboten, Daten zu sammeln. • Wer jedoch aufgrund von gesammelten Daten Erkenntnisse mit Personenbezug ableitet (d.h. „Wissen“), ist gemäss Vorentwurf des VE-DSG im Anwendungsbereich des Begriffs „Profiling“. **Kritik**: Wissen ist ein unscharfer Begriff. Wissen betrifft den Gedankenhorizont eines Verantwortlichen oder von Mitarbeitenden des Verantwortlichen (Wissenszurechnung). Wissen als Resultat von „Auswertung“ soll nach dem VE-DSG ohne Rechtfertigungsgrund auch dann verboten sein, wenn es ohne Folgen für die betroffene Person bleibt. Das ist umständlich. Der Anknüpfungspunkt ist unklar und ausserdem widerspricht diese Konstrukt etabliertem Rechtsverständnis („Die Gedanken sind frei.“). Ausserdem sind

					Analyse bzw. Auswertung sind keine Datenbearbeitungen, die sich per se negativ auf die Persönlichkeitsrechte der betroffenen Personen auswirken. **Im Resultat** hat die Begriffsbestimmung in Art. 3 lit. f VE-DSG die folgenden Wirkungen: • es resultiert ein Gefährdungstatbestand, der dem Datenschutzrecht fremd ist • Data Analytics zur Auswertung von Kundenverhalten und daraus abgeleitetes Business Consulting würden praktisch verunmöglicht • Schweizerische Unternehmen könnten das Potential von Big Data Analysen nicht nutzen. • Beispiel: Zur Abwehr von Geldwäschereiverdacht könnten z.B. Finanzinstitute Verhalten ihrer Kunden nicht ohne ausdrückliche Einwilligung analysieren. Dies würde dazu führen, dass ein Bankkunde viel längere Einwilligungserklärungen unterzeichnen müsste. Es bestehen erhebliche Zweifel an der Sinnhaftigkeit dieser Rechtsfolge. **Für einen Gefährdungstatbestand besteht kein Anlass**. Von einem solchen Swiss Finish ist abzusehen. **Erläuterung zum Alternativvorschlag**: Als „Anreicherung" ist jede Verknüpfung von Daten zu dem Datensatz zu verstehen, welche die betroffene Person dem Verantwortlichen überlassen hat. Eine Verknüpfung liegt vor, wenn Daten einer betroffenen Person als „zutreffend", „anwendbar" oder dergleichen zugeordnet sind, sei dies statisch oder dynamisch (z.B. mittels eines Reports, der im Geschäftsbereich des Verantwortlichen tatsächlich vorhanden ist, egal ob die Reportingmöglichkeit im Alltag eingesetzt wird oder nicht). Einordnung in Kürze: • Swiss Finish • Es besteht ein Bezug zum Recht auf Kopie
Swiss Data Alliance [SWIDA-7.]	DSG	3		i	Antrag: Anpassung von Art. 3 lit. i wie folgt: *Auftragsdatenbearbeiter: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.* Begründung: Anpassung an die Begrifflichkeiten in der europäischen Gesetzgebung. Inhaltlich ist die in der EU gebräuchliche Begriffsverwendung zutreffender. Es geht beim Auftragsdatenbearbeiter nicht darum, dass er *irgendeinen* Auftrag des Verantwortlichen ausführt, sondern es geht darum, dass der Auftrag sich auf die Bearbeitung von Daten (Personendaten) bezieht. Die möglicherweise aus sprachlichen Gründen gewollte Vereinfachung ist ein unnötiges Abweichen vom EU-weiten Verständnis. Einordnung in Kürze: • Swiss Finish (nur Begriffliches)
Swiss Data Alliance [SWIDA-8.]	DSG	5	5		Antrag: Reaktionsfrist des Beauftragten ist auf 30 Tage zu reduzieren. Einordnung in Kürze: • Swiss Finish
Swiss Data Alliance [SWIDA-9.]	DSG	5	6		Antrag: Art. 5 Abs. 6 ist ersatzlos zu streichen. Begründung:

					Die pauschale Informationspflicht bietet weder der betroffenen Person noch dem EDÖB einen Mehrwert; die EU GDPR kennt eine entsprechende Informationspflicht auch nicht (Art. 5 Abs. 6). Einordnung in Kürze: • Swiss Finish
Swiss Data Alliance [SWIDA-10.]	DSG	7	3		Antrag: Präzisierung dahingehend, dass vor Beizug von Subunternehmern nicht jeweils eine Zustimmung im Einzelfall erforderlich ist, sondern eine pauschale Genehmigung des Beizugs – wie in Art. 28 EU-GDPR – genügt. Begründung: Eine vorgängige schriftliche Zustimmung ist in der Praxis kaum umsetzbar. Die Regelung sollte analog Art. 28 Abs. 2 DSGVO ausgestaltet werden, wonach die Zustimmung zur Übertragung an einen anderen Auftragsbearbeiter in allgemeiner Form erfolgen kann, mit einem Einspruchsrecht des Verantwortlichen bei Änderungen. Dem VE-DSG ist zu Gute zu halten, dass dies wohl auch so gemeint ist und eine Abweichung zur EU-DSGVO gar nicht beabsichtigt ist. Allerdings ist die Präzisierung notwendig. Einordnung in Kürze: • Swiss Finish
Swiss Data Alliance [SWIDA-11.]	DSG	12			Antrag: Streichung von Art. 12 VE-DSG. Dieses Recht sollte im Kontext des Rechts auf Kopie gesamthaft geregelt werden. Begründung: Die Regelung ist erbrechtlicher Natur und verallgemeinert Szenarien, die sich letztlich auf die Herausgabe von Daten von Social Media Plattformen beziehen. Die allgemeine, dahinter stehende Regel lautet „Recht auf Kopie“. Ausserdem könnte man (andernorts) regeln, ob ein Profil auf einer Plattform einen Marketingwert hat / haben kann, und wenn ja, wem dieser Marketingwert (in Form von Beziehungen zum Knotenpunkt „Erblasser“) nach dem Tod einer Person zustehen soll (Bsp.: Das Social Media-Profil eines Musikers auf einer alternativen Musikvermarktungsplattform könnte als Vermögenswert verstanden werden; die Erben würden die Vertragsbeziehung womöglich gerne mit der Plattform fortsetzen, um weiterhin das alternative Geschäftsmodell fortsetzen zu können, ohne „neu beginnen“ zu müssen). Darüber wurde bislang noch nicht viel nachgedacht. Dies ist wohl nachzuholen. Die Diskussion über das Recht auf Kopie bietet hier einen idealen Rahmen. Einordnung in Kürze: • Swiss Finish • Recht auf Kopie
Swiss Data Alliance [SWIDA-12.]	DSG	13	4		Antrag: Streichung. Begründung: Die Bestimmung ist systemwidrig. Die Auftragsdatenbearbeitung basiert auf dem Konzept einer Privilegierung (der Auftragsdatenbearbeiter ist der „lange Arm“ des Verantwortlichen; alles, was der Verantwortliche darf, darf er auch durch einen Auftragsdatenbearbeiter ausführen lassen). Damit ist nur die Bekanntgabe (Übermittlung von Personendaten an Dritte ohne Bindung) datenschutzrechtlich relevant. Dieses Konzept würde mit einer Informationspflicht bei Einsetzen eines Dritten durchbrochen. Solange der Verantwortliche einen Auftragsdatenbearbeiter rechtmässig und unter Einhaltung der gesetzlich vorgeschriebenen Sicherungsmassnahmen beizieht, besteht kein Anlass für eine Information.

					Die Bestimmung hat neben anderen, nachteiligen Wirkungen insbesondere auch **bremsenden Einfluss auf die Digitalisierung der Schweiz**, namentlich wenn es um den Einsatz von IT-Dienstleistern als Auftragsdatenbearbeiter geht: Die Möglichkeit, IT-Dienstleister – namentlich Cloud-Anbieter – beizuziehen, ist von zentraler Bedeutung (Erhöhung der Agilität und der technischen und organisatorischen Sicherheit bei einem spezialisierten Anbieter). Bereits Art. 7 Abs. 4 VE-DSG zeigt (wie das bisherige Recht), dass jedenfalls der IT-Dienstleister nicht als Dritter zu bezeichnen ist. Die (wie erwähnt) systemwidrige Einführung einer Informationspflicht im Fall einer Bearbeitung von Personendaten über einen Auftragsdatenbearbeiter (z. B. Speicherung von Daten in den Rechenzentren eines spezialisierten Anbieters) würde völlig zu Unrecht suggerieren, dass aus einer Auftragsdatenbearbeitung per se zusätzliche Risiken resultieren und umgekehrt beispielsweise der Betrieb eigener Rechenzentren (nota bene ggf. auch ohne die dazu notwendigen internen Kompetenzen) sicherer ist, als die Auslagerung diese Aufgabe an einen spezialisierten Anbieter. Dies wäre offensichtlich falsch und somit ist Art. 13 Abs. 4 VE-DSG geradezu gegenläufig zu den Interessen der betroffenen Person (das Gesetz muss den Beizug von spezialisierten IT-Dienstleistern begünstigen, nicht erschweren). Einordnung in Kürze: • Systemwidrige Regelung • Swiss Finish
Swiss Data Alliance [SWIDA-13.]	DSG	15	1		Antrag: Formulierung von Art. 15. Abs. 2 VE-DSG wie folgt: Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese ~~rechtliche Wirkungen oder~~ erhebliche Auswirkungen auf die betroffene Person hat. Begründung: Die in dieser Bestimmung zum Ausdruck kommende Definition der «Automatisierten Einzelentscheidung» geht zu weit. Folgendes wäre auch erfasst: ● Automatisierte Kreditvergabe – Kommentar: Sollte nicht erfasst sein (ist Konsumentenschutz). ● Firewall Regeln – Kommentar: Auszuschliessen, weil sicherheitstechnisch bedingte Massnahme wohl vom Vorentwurf nicht im Fokus der Regel stehen sollten. ● Ländercode-Beschränkungen bei File-Downloads oder Streaming-Providern – Auszuschliessen, ist v.a. im Bereich Urheberrecht relevant. ● Online-Vertragsabschlüsse. Diese Folgen ergeben sich aus der im VE-DSG als „Swiss Finish“ eingefügten Formulierung „rechtliche Wirkungen“. Diese Passage ist entsprechend zu streichen. So kann die Formulierung strikt auf Art. 8 Ziffer 1 Bst. a der Konvention 108 zu beschränkt werden. Einordnung in Kürze: • Zu breit formulierter Anwendungsbereich • Swiss Finish
Swiss Data Alliance [SWIDA-14.]	DSG	16			Antrag: Art. 16 ist als Ganzes zu streichen. Begründung: Die Datenschutzfolgenabschätzung muss nicht und sollte nicht gesetzlich vorgeschrieben sein. Die Forderung von Art. 8bis der Konvention 108, bei geplanten Datenbearbeitung die Risiken einzuschätzen, wird durch Art. 11 des Vorentwurfs (Datensicherheit) bereits erfüllt. Das Instrument führt zu unnötigem Aufwand und ist bestenfalls Arbeitsbeschaffung für Consulting-Dienstleister. Die interne

					Dokumentationspflicht nach Art. 19 lit. a VE-DSG ist ausreichend. Selbst das europäische Recht verlangt nicht, die Aufsichtsbehörden von jeder Datenschutz-Folgenabschätzung zu informieren. Art. 36 Abs. 1 DSGVO verlangt eine Meldung im Gegenteil nur dann, wenn die Datenschutz-Folgenabschätzung ergibt, dass trotz der vorgesehenen Massnahmen ein hohes Risiko verbleibt. Einordnung in Kürze: • Swiss Finish
Swiss Data Alliance [SWIDA-15.]	DSG	17	1		Antrag: Art. 17 Abs. 1 ist wie folgt neu zu formulieren: Der Verantwortliche meldet dem Beauftragten ~~unverzüglich~~ ohne übermässige Verzögerung einen ~~unbefugte Datenbearbeitung oder den Verlust von Daten~~Sicherheitsverstoss, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu ~~einem Risiko~~ einer erheblichen Beeinträchtigung für die Persönlichkeit. Begründung: Die Pflicht sollte auf hohe Risiken eingeschränkt werden; insbesondere aufgrund der vorgesehenen Sanktionierung (vgl. Art. 50 Abs. 2 lit. d VE-DSG). Würde – in Ausweitung der EU-DSGVO – „jegliche unbefugte Datenbearbeitung“ sanktioniert, wäre bereits eine Verletzung der Datenbearbeitungsgrundsätze (Art. 4 VE-DSG) zu melden. Das kann nicht gewollt sein. Das Wort „unverzüglich“ steht nicht im Einklang mit den Vorgaben in der Europaratskonvention, Art. 7 Abs. 2. Auch Bagatellmeldungen fallen gemäss VE-DSG unter diese neue Bestimmung (z.B. der Fehlversand eines Emails an die falsche Adresse). Bagatellmeldungen sind klar auszuschliessen. Ganz generell muss man betonen, dass die Blossstellungssanktion der Data Breach Notification systematisch zunächst nur in der US-amerikanischen Rechtsordnung sinnvoll ist (in den USA gilt ein stärker „transaktionaler“, d.h. auf Transaktionen fokussierender Datenschutz, während das CH-Recht (und auch das EU-Recht) mit der Begründung von subjektiven Datenschutzansprüchen einen anderen Ansatz verfolgt. Einordnung in Kürze: • Swiss Finish
Swiss Data Alliance [SWIDA-16.]	DSG	17	2		Antrag / Begründung: Art. 17 Abs. 2 („oder der Beauftragte es verlangt.“) macht die Anordnung scheinbar voraussetzungslos möglich. Das wäre unschweizerisch / willkürlich, was der Erläuternde Bericht festhält. Die Ausführungen im Erläuternden Bericht sind zwingend und müssten mindestens in die Botschaft überführt werden. Einordnung in Kürze: • Gesetzesredaktion (Überführung der Grundsätze aus dem Erläuternden Bericht)
Swiss Data Alliance [SWIDA-17.]	DSG	17	4		Antrag: Art. 17 Abs. 1 ist wie folgt neu zu formulieren: Der Auftragsdatenbearbeiter informiert den Verantwortlichen unverzüglich über einen ~~unbefugte Datenbearbeitung~~Sicherheitsverstoss. Begründung: Es ist folgerichtig, die Meldepflicht hinunterzureichen auf den Auftragsdatenbearbeiter. Dieser meldet Verstösse, wenn sie den von ihm verantworteten Aufgabenbereich betreffen. Der Auftragsdatenbearbeiter ist aber nicht verantwortlich für Datenschutzverstösse, die im Verantwortungsbereich des Verantwortlichen

					auftreten (z.B. ein Mitarbeitender des Verantwortlichen greift unbefugt auf Bereiche einer Softwareplattform zu, weil der Verantwortliche die Einstellung in der Softwareplattform falsch eingestellt hat). Einordnung in Kürze: • Systematik (Pflichten des Auftragsdatenbearbeiters)
Swiss Data Alliance [SWIDA-18.]	DSG	19		b	Antrag: Art. 19 lit. b ist zu streichen, mitsamt der entsprechenden Strafbestimmung. Begründung: Nicht umsetzbar, führt zu Informationsflut. In gewissen Fällen ist die vorgesehene Informationspflicht schlichtweg sinnlos, z.B., wenn Personendaten gelöscht werden, weil sie nicht mehr benötigt werden. Einordnung in Kürze: • Praktikabilität / Sinnhaftigkeit der Regelung • Schädliche Überinformation / mehr Information resultiert nicht in mehr Datenschutz
Swiss Data Alliance [SWIDA-19.]	DSG	20	2	g	Antrag: Art. 20 Abs. 2 lit. g VE-DSG ist auf die Streichung von Art. 13 Abs. 4 VE-DSG anzupassen: g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 ~~und 4~~ Begründung: Eine Rechenschaftspflicht hat im Verhältnis zwischen der betroffenen Person und dem Verantwortlichen nichts zu suchen. Rechenschaftsberichte lösen erheblichen Aufwand aus und führen so zwar zu „nuisance value“ und „indirekter Bestrafung“ allein deswegen, *dass* der Verantwortliche Daten bearbeitet. Genau in diese Denkhaltung darf die Digitale Schweiz nicht verfallen. Einordnung in Kürze: • Systematik (Umsetzung der Streichung in Art. 13 Abs. 4 VE-DSG)
Swiss Data Alliance [SWIDA-20.]	DSG	20	3		Antrag: Art. 20 Abs. 3 VE-DSG ist zu streichen Begründung: Eine Rechenschaftspflicht hat im Verhältnis zwischen der betroffenen Person und dem Verantwortlichen nichts zu suchen. Rechenschaftsberichte lösen erheblichen Aufwand aus und führen so zwar zu „nuisance value“ und „indirekter Bestrafung“ allein deswegen, *dass* der Verantwortliche Daten bearbeitet. Genau in diese Denkhaltung darf die Digitale Schweiz nicht verfallen. Einordnung in Kürze: • Swiss Finish
Swiss Data Alliance [SWIDA-21.]	DSG	20	1		Antrag: Art. 20 Abs. 1 VE-DSG ist wie folgt zu ändern: Jede Person kann vom Verantwortlichen ~~kostenlos~~ Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Begründung: Das allgemeine Auskunftsrecht ist im Kern unbestritten. Die Ausweitung des Auskunftsrechts auf hängige Verfahren (Art. 2 Abs. 3 VE-DSG) ist jedoch unangebracht. Ausserdem müssen Unternehmen vor querulatorischen, kosten- und ressourcenintensiven Anfrage zu reinen Schikanezwecken geschützt

					werden. Aus diesen Gründen darf auch nicht volle Kostenfreiheit gewährt werden. Die Erfahrung zeigt, dass bereits geringe Gebühren leicht steuernde Wirkung haben. Einordnung in Kürze: • Änderung des Anwendungsbereichs
Swiss Data Alliance [SWIDA-22.]	DSG	23	2	d	Antrag: Art. 23 Abs. 2 lit. d VE-DSG sollte geändert werden, zugleich sollte die Regelung im Kontext des Rechts auf Kopie durchdacht werden (z.B., wer Profiling vornimmt. Der Inhalt der Regelungen ist zu diskutieren. Begründung: Die vorliegende Kommentierung bezieht sich auf die Forderung zu Art. 3 lit. f VE-DSG, mit dem Swiss Data Alliance Präzisierungen zum Begriff des Profiling fordert. Swiss Data Alliance lehnt den Entwurf in Bezug auf das Profiling ab: • einen Gefährdungstatbestand, wie er aus Art. 3 lit. f. VE-DSG und Art. 23 Abs. 2 lit. d VE-DSG resultiert, braucht es nicht. • eine Einwilligung für das Profiling braucht es auch nicht (wäre ohne Bedürfnis schwer zu handhaben und in der Wirkung wirtschaftsschädlich) Swiss Data Alliance regt an, das Recht auf Kopie zum Ausgleichstatbestand zu machen. Anbieter, welche Profilings anlegen, sollten der betroffenen Person jederzeit die so angelegten Daten herausgeben. Diese Regelung führt zu einer freiheitlich geprägten Kontrollwirkung, die wie folgt wirken würde: • für jedes Profiling muss ein Anbieter dafür sorgen, dass das Profil in dem vorgeschriebenen Format exportierbar ist; je weitergehend das Profiling ist, desto weiter geht auch die Exportpflicht und desto weitergehende Kosten muss der Anbieter tragen. Anbieter haben insofern einen Anreiz, weniger Profile anzulegen; • je mehr Profilings ein Anbieter anlegt, desto mehr Daten muss er dem Kunden auf Wunsch aushändigen; • je mehr Daten ein Anbieter einem Kunden aushändigen muss, desto mehr Daten werden vermutungsweise auch Konkurrenten ausgehändigt werden; so können Konkurrenten anhand von Re-Engineering-Massnahmen erkennen, welche Analysen „die Konkurrenz“ vornimmt; eine Vergütung erhält der Anbieter hierfür nicht. • wenn ein Verantwortlicher Profilings anlegt, aber das Recht auf Kopie nicht „bedient“, obwohl er müsste, sollte der Verantwortliche im Rahmen des Sanktionensystems bestraft werden können. Einordnung in Kürze: • Swiss Finish • Es besteht ein Bezug zum Recht auf Kopie
Swiss Data Alliance [SWIDA-23.]	DSG	44	3		Antrag: Art. 44 Abs. 3 VE-DSG ist zu löschen. Begründung: Vorsorgliche Massnahmen im Bereich von Datenbearbeitungen können zerstörerische Konsequenzen für Unternehmen haben. Sie können einen Betrieb lahmlegen. Es sollte dem Gericht aufgrund des konkreten Einzelfalles überlassen sein zu entscheiden, die aufschiebende Wirkung zu entziehen. Einordnung in Kürze: • Unbegründeter Eingriff in das Prozessrecht
Swiss Data	DSG	50 ff.			Antrag:

Alliance [SWIDA-24.]					Das Sanktionenkonzept ist gesamthaft zu überdenken. Strafsanktionen gegen Individuen sind nicht vorzusehen, es sei denn, es solle ganz direkt kriminelle Energie eines Einzelnen ausserhalb seiner organisatorischen Stellung im Unternehmen z.B. des Verantwortlichen sanktioniert werden. Swiss Data Alliance schliesst sich in Bezug auf das Sanktionenkonzept dem von der economiesuisse erarbeiteten Sanktionenmodell an. Begründung: Art. 50 ff. VE-DSG enthalten eigentliche Strafbestimmungen, im Gegensatz zu den entsprechenden europäischen Regelungen, die Verwaltungssanktionen vorsehen. Einordnung in Kürze: • Swiss Finish • Bedeutung für Angemessenheitsbeschluss der EU

Swiss Data Alliance

Für eine zukunftsorientierte Datenpolitik in der Schweiz

Grundlagendokument, Januar 2017

Vorwort

Daten sind eine Ressource, von der alle profitieren können. Sie bieten grosse Chancen für Innovation, Forschung und wirtschaftliches Wachstum. Damit in der Schweiz Daten als Ressource in den kommenden Jahren erfolgreich und zum Wohl der ganzen Gesellschaft genutzt werden können, braucht es eine zukunftsorientierte und breit abgestützte Datenpolitik. Mit dieser Überzeugung haben wir auf Einladung des Vereins Opendata.ch in den vergangenen Monaten das vorliegende Grundlagendokument erarbeitet und wollen auf dieser Basis in den kommenden Monaten die Swiss Data Alliance als gemeinsame Initiative von Unternehmen, zivilgesellschaftlichen Organisationen, Wirtschaftsverbänden Bildungs- und Forschungsinstitutionen sowie Einzelpersonen ins Leben rufen.

André Golliez (Redaktion)
Doris Albisser
Abraham Bernstein
Adelheid Bürgi-Schmelz
Claudio Dionisio
Felix Frei
Hannes Gassert
Balthasar Glättli
Edith Graf-Litscher
Franz Grüter
Peter Grütter
Ernst Hafen
Jean-Marc Hensch
Andreas Hugi
Tom Kleiber
Denise Koopmans
Christian Laux
Alessia Neuroni
Hans-Rudolf Sprenger
Matthias Stürmer

Januar 2017

Inhaltsverzeichnis

1. Ausgangslage und Absicht

Daten[1] sind eine Basis für Innovation und wirtschaftliches Wachstum

Die umfassende Digitalisierung der gesellschaftlichen und wirtschaftlichen Tätigkeiten führt zu einem explosionsartigen Wachstum der Datenbestände. Innerhalb einer Woche werden zurzeit mehr Daten produziert als im ganzen 20. Jahrhundert. Die rasante Zunahme an Smartphones und weiterer datenintensiver Geräte sowie die Entwicklung des Internets der Dinge (IoT) werden diesen Trend in den nächsten Jahren noch verstärken.

Um von diesen Daten für Innovation, wirtschaftliches Wachstum und soziale Wohlfahrt profitieren zu können, fordert die OECD[2] die Regierungen und Unternehmen zum Handeln auf. [3] Die Publikation und Wiederverwendung der Daten („Open Data") muss gefördert werden, und Hindernisse für den grenzüberscheitenden Datenfluss sind zu reduzieren. Dabei ist die richtige Balance zwischen dem gesellschaftlichen Nutzen der Offenheit der Daten auf der einen und den berechtigten Vorbehalten der Individuen und privaten Organisationen gegenüber einer Offenlegung, z.B. aus Gründen des Schutzes der Privatsphäre oder des Geschäftsgeheimnisses, auf der anderen Seite zu finden. Datenspezialisten müssen in genügend hoher Zahl zur Verfügung stehen, und es braucht weitsichtige Massnahmen im Hinblick auf die grundsätzlichen gesellschaftlichen und wirtschaftlichen Veränderungen, welche die datengetriebenen Innovationen längerfristig mit sich bringen.

Die Datenwirtschaft in der Schweiz wird bisher nicht systematisch entwickelt

Die Schweiz hat ohne Zweifel beste Voraussetzungen, datenbasierte Innovationen für wirtschaftliches Wachstum und soziales Wohlergehen zu nutzen. Dazu zählen u.a. eine hoch entwickelte IKT-Infrastruktur, die Qualität der datenintensiven administrativen Prozesse in Unternehmen und öffentlichen Verwaltungen sowie die hohen Standards bezüglich Datenschutz und Datensicherheit. Diese positiven Standortfaktoren haben u.a. den rasanten Ausbau von RZ-Infrastrukturen und -Dienstleistungen in der Schweiz in den letzten Jahren begünstigt.

Nimmt man hingegen die Bereitstellung offener Daten durch Verwaltung und Unternehmen des öffentlichen Sektors als Massstab für den Entwicklungsstand der Datenwirtschaft, fällt die aktuelle Bilanz der Schweiz eher negativ aus. Auch auf der Seite der Nutzung offener Daten gehört die Schweiz nicht

[1] Wikipedia definiert den Begriff „data" wie folgt: „Data is a set of values of qualitative or quantitative variables; restated, pieces of data are individual pieces of information. Data is measured, collected and reported, and analyzed, whereupon it can be visualized using graphs or images. Data as a general concept refers to the fact that some existing information or knowledge is represented or coded in some form suitable for better usage or processing." (siehe https://en.wikipedia.org/wiki/Data, 8.4.2016).

[2] Bereits 2011 hatte die OECD im Rahmen ihres Projektes „New Sources of Growth: Knowledge-based Capital (KBC)" digitale Daten und Informationen als immaterieller Bestandteil des wissensbasierten Kapitals identifiziert und damit begonnen, deren Auswirkungen auf wirtschaftliches Wachstum und soziale Wohlfahrt zu untersuchen. Als Resultat hat die OECD im Oktober 2015 unter dem Titel „Data-driven Innovation for Growth and Well-being" einen umfangreichen Bericht publiziert: OECD (2015), Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing, Paris.
http://dx.doi.org/10.1787/9789264229358-en.

[3] OECD (2015), „Data-Driven Innovation for Growth and Well-Being. What Implications for Governments and Businesses?", Directorate for Science, Technology and Innovation Policy Note, October 2015.

zur europäischen Spitzengruppe.[4] Partielle Ansätze vereinzelter Startup-Firmen oder unternehmensinterner „Big Data"-Projekte konnten sich bisher nicht zu einer offenen und dynamischen Datenwirtschaft entwickeln.

In der Schweiz ist bis anhin die Datenwirtschaft weder in der breiten Öffentlichkeit noch auf oberster politischer oder wirtschaftlicher Führungsebene ein Thema. Datenbezogene Initiativen wie das Nationale Forschungsprogramm NFP 75 zum Thema „Big Data und Internet der Dinge", die Expertenkommission des Bundes zur Zukunft der Datenbearbeitung oder die aktuelle Revision des Datenschutzgesetzes folgen keiner erkennbaren gemeinsamen strategischen Vision zur Datenwirtschaft in der Schweiz. Es fehlt daher auch ein gemeinsamer Aktionsplan, wie die Datenwirtschaft in der Schweiz in den nächsten Jahren entwickelt werden soll.

Die Swiss Data Alliance als datenpolitische Initiative

Am 20. April 2016 hat der Bundesrat die Strategie „Digitale Schweiz" verabschiedet, damit die Schweiz in den nächsten Jahren „die Chancen der Digitalisierung in allen Lebensbereichen konsequent nutzen" kann[5]. Diese Strategie „gilt ab sofort und soll im Dialog mit Wirtschaft, Wissenschaft, Forschung und Zivilgesellschaft laufend weiterentwickelt werden."[6] [7]

Dem Thema „Daten und digitale Inhalte" ist ein ganzes Kapitel gewidmet[8], worin eine „kohärente und zukunftsorientierte Datenpolitik" (Kapitel 4.2.1), eine „nationale Dateninfrastruktur" (Kapitel 4.2.2) sowie die „Kontrolle der Einwohnerinnen und Einwohner der Schweiz über ihre eigenen Daten" (Kapitel 4.2.4) postuliert werden.

Mit der Strategie „Digitale Schweiz" und der Auslegeordnung zur Datenpolitik hat der Bundesrat einen allgemeinen Rahmen abgesteckt, um in den kommenden Monaten die Zukunft der Datenwirtschaft in der Schweiz zu definieren. Damit die Datenpolitik der ganzen Wirtschaft und Gesellschaft zugutekommt, braucht es das Engagement von Bürgern, Unternehmen, zivilgesellschaftliche Organisationen und weitere Institutionen, welche sich für eine innovative und faire Nutzung der Daten in der Schweiz aktiv einsetzen. Zu diesem Zweck soll die Swiss Data Alliance als überparteilicher Zusammenschluss von Unternehmen, Wirtschaftsverbänden, zivilgesellschaftlichen Organisationen, Forschungsinstitutionen und Einzelpersonen ins Leben gerufen werden.

---

[4] Seit der Verabschiedung der Open-Government-Data-Strategie Schweiz 2014 bis 2018 im April 2014 durch den Bundesrat wurden über das nationale OGD-Portal über 2000 Datensätze als Open Data publiziert. Wichtige Datenbestände wie Firmenregister oder die Ausgaben der öffentlichen Verwaltung gehören allerdings nicht dazu. Im Rahmen des jährlich erhobenen Global Open Data Index liegt die Schweiz 2015 auf dem 29. Rang (Siehe http://index.okfn.org/place/switzerland/) und auch im Open Data Maturity Report 2015 des European Data Portal befindet sich die Schweiz bloss in der Gruppe der „Followers". Finnland, Dänemark, Estland und weitere Länder liegen als „Trend Setters" der Datenwirtschaft gemäss diesen Studien deutlich vor der Schweiz.

[5] Siehe https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-61417.html.

[6] ebenda

[7] Das Postulat „Auswirkungen des digitalen EU-Binnenmarkts auf die Schweiz" von Ständerat Beat Vonlanthen wurde am 6.6.2016 vom Ständerat entgegen der Empfehlung des Bundesrates angenommen. Dies zeigt die Dringlichkeit, welche die Politik digitalen Themen beimisst (siehe https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=37303)

[8] Siehe Strategie „Digitale Schweiz", Kapitel 4.2, Seite 5 f.

2. Prinzipien

Damit die Schweiz einen maximalen Nutzen aus den ihr zur Verfügung stehenden Daten ziehen kann, ist ein gemeinsames Verständnis notwendig, was Daten sind und worin ihr wirtschaftlicher und sozialer Wert besteht (1), weshalb der Zugang zu den Daten möglichst offen zu regeln ist (2), welche Rechte der einzelnen Person, auf welche sich die Daten beziehen, zustehen (3), dass Personendaten vor übermässigem staatlichem Zugriff zu schützen sind (4) und welchen Anspruch die Öffentlichkeit auf die Daten von allgemeinem Interesse hat (5).

1. Daten sind eine Ressource, von welcher alle profitieren können

Die umfassende Digitalisierung aller Lebensbereiche bringt eine enorme Anhäufung von Daten mit sich. Daten, sobald sie einmal erhoben und gespeichert sind, lassen sich mit geringstem Aufwand kopieren und für verschiedenste Zwecke wiederverwenden. Entsprechende Daten-Infrastrukturen ermöglichen es, dass Daten als wertvolle wiederverwendbare immaterielle Ressourcen Unternehmen, Verwaltungen, Forschungsinstitutionen und Zivilgesellschaft zur Verfügung stehen. Daten lassen sich im Prinzip von einer unbegrenzten Anzahl Akteure gleichzeitig nutzen und haben dadurch das Potenzial, zu einem Gemeingut zu werden, von welchem die zur Nutzung berechtigten Individuen, Unternehmen, Verwaltungen, Forschungsinstitutionen und zivilgesellschaftliche Organisationen gleichermassen profitieren können.

Daten sind eine wichtige Basis für wirtschaftlichen Erfolg, soziales Wohlergehen und wissenschaftliche Erkenntnisse. Sie geben Auskunft über Verkehrsströme, Energieverbrauch, Umweltbelastungen, öffentliche Finanzen und viele weitere wirtschaftliche, soziale und kulturelle Entwicklungen in unserer Gesellschaft. Sie ermöglichen wissenschaftliche Analysen und Prognosen und unterstützen politische und wirtschaftliche Entscheidungsprozesse. Eingebettet in Applikationen leisten Daten individuelle Orientierungs- und Entscheidungshilfe bei der Auswahl von Produkten und Dienstleistungen. Soziale Gruppen können anhand von Daten ihre Aktivitäten koordinieren und im Hinblick auf gemeinsame Ziele optimieren.

2. Offen zugängliche Daten erzeugen einen maximalen Nutzen für Volkswirtschaft und Gesellschaft

Damit Daten ihre positive Wirkung auf Volkswirtschaft, Gesellschaft und Wissenschaft voll entfalten können, sollten sie möglichst offen zugänglich und nutzbar sein. Dabei sind die Rechte und Pflichten der verschiedenen Anspruchsgruppen zu berücksichtigen. Personen haben ein Interesse am Schutz persönlicher Daten, Unternehmen möchten ihre Investitionen in die Datenerhebung oder in die Entwicklung von neuen Algorithmen schützen und die öffentliche Hand muss beispielsweise im Sicherheitsbereich Geheimhaltung wahren. Unter Berücksichtigung dieser Ansprüche sollen Daten, die im Rahmen von staatlichen Aufgaben anfallen und von der öffentlichen Hand finanziert werden, offen zugänglich gemacht werden. Möglichst viele Daten, die von Unternehmen oder Privaten erhoben werden, sollen auf freiwilliger Basis auf geeigneten Datenaustauschplattformen zugänglich gemacht werden.

3. Jedes Individuum hat das Recht auf eine digitale Kopie der Daten zu seiner Person

Jede Person soll eine Kopie der Daten, an deren Entstehung/Erfassung sie im Rahmen einer Transaktion mitgewirkt hat, erhalten und über deren weitere Verwendung (Zweitnutzung) eigenständig verfügen können.

Die Person soll nicht nur das im Datenschutzgesetz verankerte Recht auf Einsicht auf die Person betreffende Daten haben, sondern sie soll über die Speicherung und weitere Verwendung dieser Daten auf Basis einer Kopie selbst verfügen können (informationelle Selbstbestimmung). Die Zweitnutzung von Personendaten hat einen hohen wirtschaftlichen Wert, dessen erfolgreiche Nutzung die grossen Internetkonzerne eindrücklich vor Augen führen. Allerdings bleibt den meisten Personen die Wiederverwendung dieser Daten verborgen und äussert sich nur indirekt, z.B. in personalisierten Produktangeboten. Die ideelle und wirtschaftliche Wertschöpfung von Daten entsteht durch die Verknüpfung unterschiedlichster, die Person betreffende Daten. Aufgrund des Datenschutzgesetzes kann eine maximale Verknüpfung kann nur durch die Person selbst durchgeführt werden. Jede Person hat das grundsätzliche Anrecht, über die Wiederverwendung der Daten, welche sich auf sie beziehen, zu bestimmen und an der damit verbundenen Wertschöpfung zu partizipieren.[9]

4. Personendaten sind vor übermässigem staatlichem Zugriff zu schützen

Eine prosperierende Datenwirtschaft kann nur funktionieren, wenn die Bevölkerung das Vertrauen hat, dass der Staat als Inhaber des Gewaltmonopols aktuell und zukünftig die Zugänglichkeit zu Personendaten im gesetzlich vereinbarten Sinn respektiert.

Einerseits muss die Gewissheit bestehen, dass der regulatorische Rahmen nicht verändert werden kann, ohne dass besonders hohe Hürden eingebaut sind. Andererseits muss eine strenge Überwachung der Behördenpraxis stattfinden. Diese muss institutionell so verankert sein, dass sie grösstmögliche Autonomie von der Verwaltung hat und über ein griffiges Instrumentarium verfügt. Dabei muss die Regelung auch vorsehen, wie damit umgegangen wird, wenn offen (Rechtshilfe) oder verdeckt (Geheimdienst) ausländische oder supranationale Staaten oder Organisationen Zugriff verlangen bzw. erzwingen wollen.

---

[9] Formulierungsvorschlag für einen Verfassungsartikel zum Recht auf Kopie von Prof. Dr. iur. Thomas Gächter, Universität Zürich:
„Art. 107a BV Nutzung persönlicher digitaler Daten
1 Der Bund erlässt Vorschriften über die Nutzung persönlicher Daten, die sich aus dem Umgang Privater mit digitalen Netzwerken gewinnen lassen.
2 Als Nutzung dieser Daten gelten alle Tätigkeiten, bei denen zum Zweck der Schaffung eines wirtschaftlichen, wissenschaftlichen oder ideellen Mehrwerts persönliche Daten gesammelt, gespeichert oder weiterverwendet werden.
3 Er beachtet dabei die folgenden Grundsätze.
a. Wer persönliche Daten nutzt, die sich aus dem Umgang Privater mit digitalen Netzwerken gewinnen lassen, hat den Personen, auf die sich die Daten beziehen, auf ihr Verlangen eine Kopie dieser Daten auf ein persönliches Datenkonto zu übertragen. Der Bund kann Ausnahmen vorsehen.
b. Die Pflicht zur Übertragung der Kopie der persönlichen Daten kann nicht wegbedungen werden. Der Bund kann Ausnahmen vorsehen.
c. Datenbanken, die mit der Verwaltung der persönlichen Datenkonten betraut sind, müssen die Sicherheit der Daten gewährleisten.“

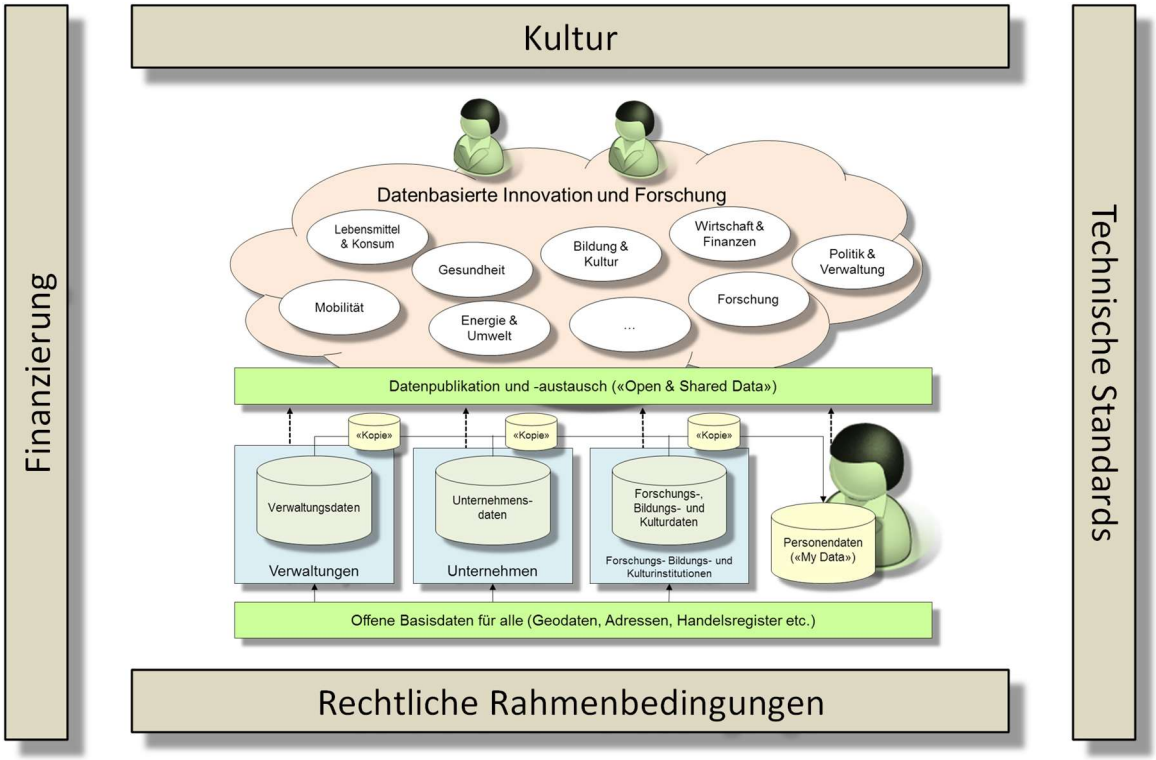
5. Unpersönliche Daten, die im Rahmen von staatlichen Aufgaben anfallen und von der öffentlichen Hand finanziert werden, sollen offen zugänglich sein

Die öffentliche Verwaltung, staatlich kontrollierte Unternehmen sowie private Firmen, welche staatliche Aufgaben wahrnehmen, produzieren grosse Mengen digitaler Daten. Diese Daten werden in der Regel mittels Steuergeldern finanziert und repräsentieren wesentliche Sachverhalte und Entwicklungen in den verschiedensten Bereichen der Wirtschaft und Gesellschaft. Im Kern stellen sie in Form von Geodaten, Gebäude-, Personen- und Firmenregistern sowie Adressen die grundlegenden Gegebenheiten des Landes dar, auf welchen praktisch alle Geschäfts- und Verwaltungsprozesse beruhen. In den verschiedenen Verwaltungsbereichen wie Transport, Energie, Gesundheit oder Erziehung, sind sie die Grundlage für operative und strategische Entscheidungen. Die Daten des öffentlichen Sektors sind als zentraler Teil einer nationalen Dateninfrastruktur zu verstehen, auf deren Nutzung die gesamte Öffentlichkeit und jeder Einwohner, insbesondere auch als Steuerzahler, ein grundlegendes Anrecht hat, sofern diese Datensammlungen durch die öffentliche Hand finanziert wurden und gleichzeitig die Unternehmen und Organisationen nicht auf dem Markt im Wettbewerb mit anderen Marktteilnehmern stehen. Zusätzlich sind jene Daten privater Unternehmen in eine nationale Dateninfrastruktur zu integrieren, welche von allgemeinem Interesse sind, sich nicht auf einzelne Personen beziehen oder Geschäftsgeheimnisse beinhalten, und von den betreffenden Unternehmen auf freiwilliger Basis der Öffentlichkeit zur Verfügung gestellt werden.

3. Zielsetzungen

Die Swiss Data Alliance setzt sich auf Basis ihrer Prinzipien für die folgenden datenpolitischen Ziele ein:

- Die Schweiz entwickelt in den kommenden Jahren rechtliche, finanzielle, technische und kulturelle Rahmenbedingungen, welche es ermöglicht, aus den verfügbaren Daten einen maximalen wirtschaftlichen, wissenschaftlichen, kulturellen und sozialen Mehrwert zu erzielen.
- Zu diesem Zweck stellen die Unternehmen, Verwaltungen sowie Forschungs-, Bildungs- und Kulturinstitutionen der Schweiz ihre Daten von allgemeinem Interesse der Öffentlichkeit („Open Data“) sowie die personenbezogenen Daten den einzelnen Individuen, auf welche sie sich beziehen („My Data“), zur Verfügung.
- Gemeinsame Infrastrukturen und technische Standards ermöglichen die freie, sichere und faire Nutzung der Daten für Innovationen, wirtschaftliches Wachstum, soziales Wohlergehen, politische Entscheidungen und wissenschaftliche Erkenntnisse.
- Die Schweiz wird ab 2021 zu einem führenden Standort in der globalen Datenwirtschaft und gehört sowohl bezüglich Datenbereitstellung als auch Datennutzung sowie den damit verbundenen Dienstleistungen zur internationalen Gruppe der Trend Setters auf diesem Gebiet. Bis dahin werden die dazu notwendigen rechtlichen, finanziellen, technischen und kulturellen Rahmenbedingungen geschaffen.
- Leuchtturm-Projekte für datenbasierte Innovationen in verschiedenen Anwendungsgebieten wie beispielsweise Transport, Umwelt, Ernährung, Gesundheit oder Bildung weisen der Schweizer Datenwirtschaft in den nächsten Jahren den Weg.



4. Handlungsfelder

Die Swiss Data Alliance engagiert sich mit kommunikativen Aktivitäten, politischen Vorstössen und Leuchtturmprojekten in den folgenden Handlungsfeldern:

- **Kommunikation**:
  Förderung des Verständnisses und des Dialoges zum Potenzial, den Prinzipien und den Spielregeln der Datennutzung in der breiten Öffentlichkeit
- **Rechtliche Rahmenbedingungen**:
  Schaffung notwendiger rechtliche Rahmenbedingungen für eine innovative und faire Datennutzung in der Schweiz, insbesondere
  - Verankerung des Rechtes auf Kopie in der Verfassung als Basis für die digitale Selbstbestimmung jeder einzelnen Person
  - Einführung des aktiven Öffentlichkeitsprinzips für die Daten der öffentlichen Verwaltung sowie aller von der öffentlichen Hand finanzierten Unternehmen und Institutionen
  - Schutz der Personendaten, insbesondere auch vor übermässigem staatlichem Zugriff
- **Technische Standards:**
  Förderung der Anwendung technischer Standards, welche die Publikation, den Austausch und die Nutzung der Daten über die Grenzen von Unternehmen, Verwaltungsorganisationen und Forschungsinstitutionen hinweg erleichtern.
- **Öffentliche nationale Dateninfrastruktur**:
  Förderung des Aufbaus einer vernetzten nationalen Dateninfrastruktur, über welche Daten aus Verwaltung, Wirtschaft und Forschung der Öffentlichkeit zur Verfügung gestellt werden können.
- **Persönliche Dateninfrastrukturen:**
  Förderung von Infrastrukturen, welche Services für die Nutzung der persönlichen Daten unter der Kontrolle des Individuums ermöglichen.
- **Datenbasierte Innovation und Forschung:**
  Förderung der Datennutzung für innovative wirtschaftliche, soziale und wissenschaftliche Anwendungen.
- **Bildung («Data Literacy»):**
  Ausbildung aller Bevölkerungskreise im grundsätzlichen Verständnis und in der praktischen Nutzung der offen zugänglichen und der eigenen persönlichen Daten für wirtschaftliche, soziale und kulturelle Zwecke.

5. Organisation

Verein

Die Swiss Data Alliance ist ein Verein im Sinne von Art. 60 ff des Schweizer Zivilgesetzbuches (Gründung im März 2017 geplant). Der Vereinszweck beruht auf den in diesem Grundlagendokument festgehaltenen Prinzipien, Zielsetzungen und Handlungsfeldern.

Mitgliedschaft

Die Swiss Data Alliance ist ein überparteilicher Zusammenschluss von in der Schweiz ansässigen Unternehmen, Wirtschaftsverbänden, zivilgesellschaftlichen Organisationen, Forschungsinstitutionen und Einzelpersonen.[10]

Vorstand und Geschäftsstelle

Die Aktivitäten der Swiss Data Alliance werden von einem Vorstand geleitet, der sich aus gewählten Vereinsmitgliedern zusammensetzt.

Die Swiss Data Alliance unterhält eine Geschäftsstelle, welche für die Kommunikation, die Koordination der einzelnen Projekte sowie weitere vom Vorstand festgelegte Aufgaben zuständig ist.

Expertenausschuss

Der Vorstand der Swiss Data Alliance beruft einen Expertenausschuss für die Erarbeitung und Verabschiedung inhaltlicher Positionen zur Datenpolitik in der Schweiz.

Der Expertenausschuss trifft sich regelmässig zu ausgewählten Themen der Datenpolitik und verabschiedet dazu schriftliche Verlautbarungen (Positionspapiere).

Die Leitung des Expertenausschusses liegt bei einem Mitglied des Vorstandes.

Projekte

Die Swiss Data Alliance führt in den einzelnen Handlungsfeldern Projekte durch, welche ihren Prinzipien und Zielsetzungen entsprechen.

Freigabe, Kontrolle, Lenkung und Abschluss eines Projektes obliegen dem Vorstand.

Patronat

Zur Unterstützung der Aktivitäten der Swiss Data Alliance in der breiten Öffentlichkeit, beruft der Vorstand ein Patronat, zu welchem namhafte Persönlichkeiten aus Politik, Wirtschaft und Wissenschaft eingeladen werden.

Die Mitgliedschaft im Patronat beruht ausschliesslich auf der Unterstützung der Prinzipien und Zielsetzungen der Swiss Data Alliance.

[10] Da sich die Swiss Data Alliance unter anderem als Gesprächspartner für die Verwaltung betreffend Datenwirtschaft und -politik versteht, ist die Mitgliedschaft von Verwaltungsorganisationen nicht vorgesehen.

Swiss Data Alliance gegründet – Orientierung für die Gründerorganisationen

Am 22. März 2017 ist die Swiss Data Alliance gegründet worden. Die Swiss Data Alliance ist ein Verein mit Sitz in Zürich. Gründer sind die folgenden Vereine: der Schweizerische Verband Telekommunikation asut, der Schweizerische Verband der ICT-Anbieter Swico, der Verein Daten und Gesundheit, die Swiss Alliance for Data-Intensive Services und der Verein Opendata.ch.

Die Swiss Data Alliance setzt sich für eine zukunftsorientierte Datenpolitik in der Schweiz ein: Daten sind eine immaterielle Ressource, von welcher alle profitieren können. Damit Daten ihr innovatives Potenzial voll entfalten können, müssen sie möglichst offen zugänglich und frei nutzbar sein. Dabei ist die richtige Balance zwischen den Ansprüchen der Unternehmen nach Schutz ihrer Investitionen und freier Nutzung ihrer Geschäftsdaten, der Individuen nach Schutz ihrer Privatsphäre und Partizipation an der Verwertung ihrer persönlichen Daten, und der Öffentlichkeit nach offenem Zugang zu den von ihr finanzierten Daten der Verwaltung und Forschung zu finden.

Als überparteilicher Zusammenschluss von Unternehmen, Wirtschaftsverbänden, zivilgesellschaftlichen Organisationen sowie Bildungs- und Forschungsinstitutionen engagiert sich die Swiss Data Alliance für:

- das Verständnis und den Dialog zum Potenzial, den Prinzipien und den Spielregeln einer innovativen Datenwirtschaft in der breiten Öffentlichkeit.
- die Schaffung notwendiger rechtlicher, finanzieller, technischer und kultureller Rahmenbedingungen für die innovative und faire Datennutzung in der Schweiz.
- den Aufbau einer nationalen Dateninfrastruktur, über welche Daten aus Verwaltung, Wirtschaft und Forschung der Öffentlichkeit zur Verfügung gestellt werden können.
- den Aufbau von Infrastrukturen für die Nutzung persönlicher Daten unter der Kontrolle der betroffenen Personen.

Auf Basis eines programmatischen Grundlagendokumentes zur Datenpolitik (siehe Beilage) hat die Swiss Data Alliance damit begonnen, sich mit aktuellen datenpolitischen Themen wie die Totalrevision des Datenschutzgesetzes (DSG), das Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) und den Aufbau einer nationalen Dateninfrastruktur auseinanderzusetzen. In den kommenden Wochen und Monaten werden dazu Positionspapiere publiziert, Informationsveranstaltungen durchgeführt und politische Vorstösse vorbereitet.

Rückfragen an:

André Golliez, Präsident Swiss Data Alliance
Telefon: +41 79 669 05 52
Email: golliez@opendataconsulting.ch

Christian Laux, Vizepräsident Swiss Data Alliance
Telefon: +41 79 737 5774
Email: christian.laux@lauxlawyers.ch

Zürich, 26. März 2017

Swiss Cigarette

Kapellenstrasse 14
Postfach
3001 Bern
Tel. +41 58 796 99 18
Fax +41 58 796 99 03
office@swiss-cigarette.ch
www.swiss-cigarette.ch

Per E-Mail an jonas.amstutz@bj.admin

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Bern, 4. April 2017

Vernehmlassungsantwort zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Somaruga
Sehr geehrte Damen und Herren

Im Dezember 2016 haben Sie eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr.

Swiss Cigarette besteht aus den Mitgliedern British American Tobacco Switzerland SA (Boncourt), Japan Tobacco International AG (Dagmersellen) und Philip Morris S.A. (Lausanne). Die Mitglieder von Swiss Cigarette und deren Konzerngesellschaften sind am Standort Schweiz seit Jahrzehnten stark verankert: sie beschäftigen hierzulande 5000 Mitarbeiter und investieren in ihre exportorientierten Produktionsstätten, in Forschungs- und Entwicklungstätigkeiten mit internationaler Ausstrahlung sowie in ihre nationalen, regionalen und weltweiten administrativen Sitze. Sie leisten einen wesentlichen Beitrag zur Prosperität zahlreicher KMUs, beispielsweise in der Werbung, im Handel oder in der IT-Branche, sowie zur Lebendigkeit der kulturellen Landschaft in der Schweiz und unterstützen auch den inländischen Tabakanbau, der in gewissen landwirtschaftlichen Regionen stark verbreitet ist.

Im Hinblick auf die Formulierung des total revidierten Datenschutzgesetzes erlauben wir uns, Ihnen einige für uns wichtige Anliegen darzulegen:

- Im Datenschutzgesetz ist für die Unternehmen ein Maximum an Flexibilität und ein Minimum an Belastung zu wahren. Spielräume im Verhältnis zum internationalen Recht sowie das etablierte System der Selbstregulierung sind so weit als möglich zu nutzen. Die diversen im Vergleich zum EU-Raum überschiessenden Regelungen sind anzupassen. Dabei soll die Totalrevision genutzt werden, auch bestehende Bestimmungen zu hinterfragen und an die technologische Entwicklung anzupassen.

- Es gilt, die übergeordneten Ziele der Strategie «Digitale Schweiz» des Bundesrates im Fokus zu behalten: Zu berücksichtigen ist insbesondere auch der Nutzen der Daten für den digitalen Fortschritt und die Ausschöpfung des wirtschaftlichen Potentials im Interesse der Konsumenten und Unternehmen. Eine einseitige Orientierung lediglich an potentiellen Risiken ist verfehlt. Zentral ist deshalb: Keine Behinderung von Innovation und Entwicklung durch den Datenschutz.

- Unsere Kernanliegen lassen sich in folgende Themenbereiche unterteilen: Profiling, Selbstregulierung, Informations- und Meldepflichten sowie Aufsicht und Sanktionen. Hieraus ergeben sich die folgenden Hauptforderungen:

  - Der Begriff «Profiling» ist auf automatisierte Bewertungen von Personendaten einzuschränken und die Bedingungen dazu sind stark zu reduzieren (Information statt Einwilligung). Wird die generelle Erfordernis der ausdrücklichen Einwilligung für das Profiling Gesetz, verunmöglicht sie faktisch einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung / Marketing und stellt eine Bedrohung für den Standort Schweiz dar;
  - Die Initiative für Empfehlungen der guten Praxis muss stets zwingend von (Branchen)Verbänden ausgehen. Die Selbstregulierung ermöglicht es mittels Bezug zur Praxis, sachgerechte Lösungen zu entwickeln. Der betriebliche Datenschutzbeauftragte ist auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen;
  - Diverse Informations- und Meldepflichten sind überschiessend. Sie bedeuten unverhältnismässigen Aufwand und generieren eine regelrechte «Flut» an Informationen und Meldungen. Abzulehnen sind auch die damit verbundene Offenlegung von Geschäftsgeheimnissen und die Pflicht, sich selbst zu belasten. Gesamthaft wirken sich die vorgeschlagenen Pflichten innovations- und wettbewerbshindernd aus. Sie sind gemäss dem vom Vorentwurf angestrebten risikobasierten Ansatz entsprechend substantiell zu reduzieren. Dies betrifft insbesondere automatisierte Einzelfallentscheide, Datenschutz-Folgenabschätzungen und Meldungen von Datenschutzverstössen. Darüber hinaus braucht es eine Relativierung der Kostenlosigkeit des Auskunftsrechts und weitere, griffige Massnahmen, um dem Missbrauch des Datenschutzrechtes zu datenschutzfremden Zwecken entgegenzuwirken;
  - Ein weiterer umfassender Kritikpunkt ist das vorgeschlagene Sanktionssystem: Private, strafrechtliche Sanktionen sind weder verhältnismässig noch zielführend. Es ist ein tragbares, mit den rechtsstaatlichen Grundsätzen vereinbares Sanktionssystem zu implementieren. Gleichzeitig ist eine zu grosse Machtfülle des EDÖB zu verhindern.

Zusammenfassend:

Der vorliegende Gesetzesentwurf widerspricht den Zielsetzungen des Bundesrates zur Förderung des Wirtschaftsstandortes Schweiz. Er bewirkt vielmehr einen bedenklichen Standortnachteil. Das Datenschutzgesetz ist nur insoweit zu revidieren, als dies die internationalen Vorgaben zwingend erfordern. Jeder darüber hinausgehender „Swiss Finish" wie z.B. beim Profiling lehnen wir ab.

Im Übrigen verweisen wir auf die Vernehmlassungsantworten von economiesuisse und dem Schweizerischen Werbe-Auftraggeberverband, welche wir vollumfänglich unterstützen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für weitere Fragen gerne zur Verfügung.

Mit freundlichen Grüssen

Thomas Meyer

Geschäftsführer

Amstutz Jonas BJ

Von: Noemi Heusler <office@swissfintechinnovations.ch>
Gesendet: Montag, 13. März 2017 08:25
An: Amstutz Jonas BJ
Betreff: Swiss Fintech Innovations VE-DSG Stellungnahme
Anlagen: VE-DSG Stellungnahme SFTI.doc

Sehr geehrter Herr Amstutz

Im Anhang finden Sie die Stellungnahme von Swiss Fintech Innovations zur Totalrevision des Datenschutzgesetzes. Gerne stehen wir Ihnen zur Diskussion, für Fragen und für die weitere Zusammenarbeit zur Verfügung.

Freundliche Grüsse und einen guten Wochenstart
Noemi Heusler
Geschäftsstellenleitung Swiss Fintech Innovations
+41 77 432 76 54

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Swiss Fintech Innovations

Abkürzung der Firma / Organisation : SFTI

Adresse : Universität Zürich, Binzmühlestrasse 14, 8050 Zürich

Kontaktperson : Noemi Heusler, Geschäftsstellenleitung

Telefon : +41 77 432 76 54

E-Mail : office@swissfintechinnovations.ch

Datum : 09.03.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SFTI	Der Verband Swiss Fintech Innovations (SFTI, www.swissfintechinnovations.ch) vertritt die Interessen seiner Mitglieder im Bereich der Digitalisierung und Innovation in der Finanzindustrie. Zu den Mitgliedern des Verbands gehören derzeit: AXA Winterthur, Credit Suisse, CSS, Generali Versicherungen, Helvetia, Hypothekarbank Lenzburg, Lombard Odier, Raiffeisen, Schroders, SIX Group, Swiss Life, Swiss Fintech Innovtion Lab an der Universität Zürich, SYZ Group, Vontobel, Zürcher Kantonalbank und Zuger Kantonalbank. SFTI verfolgt im wesentlichen drei Ziele: (1) die Intensivierung der Zusammenarbeit in sich neu herausbildenden Ökosystemen verschiedener bestehender und neuer Akteure, (2) die Förderung der Zusammenarbeit zwischen Fintech Unternehmen und etablierten Unternehmen in der Finanzindustrie, (3) die kollaborative Bearbeitung und Umsetzung von für unsere Mitglieder relevanten Themen in Arbeitsgruppen. Unsere Arbeitsgruppe „Regulations“ beschäftigt sich mit der Gesetzgebung und reglementarischen Vorschriften rund um Innovation und Digitalisierung in der Finanzindustrie. Dazu gehört insbesondere auch die Gesetzgebung im Bereich von Datenmanagement und Datenschutz, weshalb wir Ihnen zum Vorentwurf des totalrevidierten Datenschutzgesetzes hiermit unsere Stellungnahme zukommen lassen. SFTI nimmt zu den Regelungen des VE-DSG Stellung, welche die Privatwirtschaft, insbesondere in Zusammenhang mit Innovation und Digitalisierung im Finanzbereich, betreffen. Auf eine Stellungnahme zu den übrigen Bestimmungen des VE-DSG und die weiteren Anpassungen in Zusammenhang mit Schengen, wird verzichtet. Demzufolge kann Stillschweigen zu anderen vorgeschlagenen Bestimmungen weder zustimmend noch ablehnend gewertet werden.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SFTI	DSG	2	1		Der Verzicht auf den Schutz von Daten juristischer Personen ist aus Sicht von SFTI sinnvoll. Dieser Schutz ist bereits heute von geringer praktischer Bedeutung, behindert aber oftmals die Bekanntgabe von Daten ins Ausland. Zudem ist auch in der EU-DSGVO sowie im Übereinkommen des Europarats kein Schutz von Daten juristischer Personen vorgesehen. Ein Verzicht darauf führt würde damit nicht zu einem tieferen, nicht-äquivalenten Datenschutzniveau in der Schweiz führen.
SFTI	DSG	3		f	Das DSG regelt ausschliesslich das Bearbeiten von Personendaten (vgl. Art. 3 lit. a VE-DSG). Andere Daten als Personendaten unterstehen dem DSG somit nur bzw. erst, sobald und sofern sie Persönlichkeitsaspekte aufweisen. Ab diesem Zeitpunkt werden Daten ohne Weiteres zu Personendaten. Wir schlagen daher vor, in der Definition nur den Begriff „Personendaten“ zu verwenden und den Begriff „Daten“ zu streichen. Damit nicht die Durchsicht jedes Papierstapels bereits als Profiling zu qualifizieren ist, ist die Definition auf elektronische Aktivitäten zu begrenzen. Dies umso mehr, als auch die EU-DSGVO diese Einschränkung vorsieht und höhere Anforderungen im Rahmen der Schweizer Gesetzgebung mit Blick auf die anzustrebende Äquivalenz zur europäischen Datenschutzgesetzgebung kontraproduktiv wären. Um Rechtsunsicherheit zu vermeiden, schlagen wir zudem vor, den Begriff „wesentliche persönliche“ zu wiederholen, also klar zu stellen, dass nur „wesentliche persönliche Entwicklungen“ gemeint sind. Zusammenfassend schlagen wir folgende Änderungen und Präzisierungen von Art. 3 lit. f VE-DSG vor (Änderungen fett und unterstrichen): «Profiling: jede **elektronische** Auswertung von ~~**Daten oder**~~ Personendaten, um wesentliche persönliche Merkmale zu analysieren oder **wesentliche persönliche** Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;»
SFTI	DSG	3			Wegfall des Begriffs „Datensammlung“: Der Wegfall des Begriffes der Datensammlung (Art. 3 lit. g DSG) ist zu begrüssen. Dieser Begriff ist angesichts der heutigen technologischen Möglichkeiten für die Bearbeitung

					und Nutzung von Daten (mit oder ohne deren Speicherung) nicht mehr zeitgemäss und führt in Rahmen von unterschiedlichen Auslegungsmöglichkeiten oftmals zu Unklarheiten.
SFTI	DSG	4	3		Die Bestimmung des Art. 4 Absatz 3 VE-DSG wurde gegenüber den geltenden Art. 4 Abs. 3 und 4 DSG um das Wort **«klar»** ergänzt. Diese Verschärfung ist unnötig und wird von SFTI klar abgelehnt. Die Unnötigkeit einer solchen Verschärfung zeigt sich insbesondere in der im erläuternden Bericht festgehaltenen Zusicherung, dass mit der neuen Formulierung keine materiellen Änderungen einhergehen. Massgebend muss der unter Berücksichtigung aller Umstände und gemäss Treu und Glauben objektivierbare Grad der Erkennbarkeit des Zwecks sein. Die Ergänzung der erkennbaren Zwecke mit dem Adjektiv „klar“ würde entgegen der gesetzgeberischen Absicht im operativen Alltag mehr Auslegungsfragen als Klärung bewirken.
SFTI	DSG	5			**Datenbekanntgabe ins Ausland:** Das erklärte Ziel der Vereinfachung der Regelung zur Datenbekanntgabe ins Ausland sowie der Anpassung der Regelung an die Konvention des Europarats ist aus Sicht von SFTI zu begrüssen. Die folgenden Punkte sind jedoch aus unserer Sicht präzisierungs- bzw. anpassungsbedürftig, um verschiedene Unklarheiten oder sogar Widersprüche innerhalb des **Art. 5 VE-DSG** auszuräumen:
SFTI	DSG	5	1		Der Absatz 1 von Art. 5 VE-DSG ist verwirrend, da unklar bleibt, inwiefern die darin gemachte Aussage das in den folgenden Absätzen minutiös dargestellte Verfahren beeinflusst. Richtigerweise spielt die Aussage von Abs. 1 keine Rolle, soweit die in den nachfolgenden Absätzen getroffenen Regelungen eingehalten werden. Demzufolge kommt Abs. 1 keine selbständige Bedeutung zu und ist folgerichtig ersatzlos zu streichen.
SFTI	DSG	5	3		Für den Fall, dass (noch) kein Entscheid des Bundesrats hinsichtlich der Angemessenheit des Schutzes in einem Land vorliegt, soll der Verantwortliche diese Angemessenheit prüfen können. Entsprechend müsste Art. 5 Abs. 3 VE-DSG folgendermassen ergänzt werden (Ergänzung fett und unterstrichen): «Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, **wenn der Verantwortliche selbst festgestellt hat, dass ein angemessener Schutz gewährleistet ist oder,** wenn ein geeigneter Schutz gewährleistet ist durch: […]»

SFTI	DSG	5	3/5	c/d	Die in **Art. 5 Abs. 3 lit. c Ziff. 1** und **lit. d** sowie **Abs. 5 VE-DSG** vorgeschlagene **Genehmigungspflicht** wird von SFTI abgelehnt. Die Pflicht zur Genehmigung durch den Beauftragten führt zu einem enormen Mehraufwand, ggf. zu grossen Projektverzögerungen bei Unternehmen und dürfte auch die Behörde überlasten. Letztere könnte im Einzelfall sogar mit Sachverhalten konfrontiert werden, bei welchen sie selbst mit Schadensersatzansprüchen konfrontiert sein könnte, sei es, dass sie eine dringliche und wichtige Anfrage nicht rechtzeitig genehmigt oder dass sie in der Papierflut einen krassen Fall gar nicht erkennt. Gleichzeitig trägt eine Genehmigungspflicht ohnehin kaum etwas zum bessern Datenschutz bei, steht doch das Unternehmen weiterhin selbst in der Verantwortung. Auch die EU-DSGVO sieht eine solche Genehmigungspflicht nicht vor. Die vom VE-DSG vorgesehene Genehmigungspflicht wäre deshalb überschiessender Swiss Finish, welcher den grenzüberschreitenden Datenfluss erheblich und unnötigerweise erschweren würde und dem Äquivalenzprinzip in Bezug auf die europäische Datenschutzgesetzgebung abträglich wäre.
SFTI	DSG	5	6		In **Art. 5 Abs. 6 VE-DSG** wird fälschlicherweise eine **Meldepflicht** angeordnet. Dies ist systemfremd, geht es doch um bereits vorliegende standardisierte Garantien. Weshalb die Verwendung solcher Standards in jedem Verwendungsfall erneut eine Meldepflicht auslösen sollen, ist unerfindlich. Auch solche Regeln widersprechen etabliertem EU-Recht und sind deshalb ein Swiss Finish, welcher der gesetzgeberischen Absicht und dem erklärten Ziel von Äquivalenz mit der europäische Datenschutzgesetzgebung widersprechen (vgl. EuGH-Entscheid Schrems u. gestützt darauf ergangener Entscheid der EU-Kommission vom 16.12.2016, wonach von ihr genehmigte Datenschutz-Standardklauseln nicht erneuter Bewilligung im Einzelfall bedürfen und deshalb ohne Einschränkung verwendet werden dürfen; Art. 45 EU-DSGVO). Zumindest die Meldepflicht oder konsequenterweise der ganze Absatz 6 ist demzufolge zu streichen.
SFTI	DSG	6	a		In **Art. 6 VE-DSG** sind verschiedene Einschränkungen zu streichen, welche das bisherige Recht nicht kannte und die der erklärten Absicht des Gesetzgebers, auch unter neuem Recht keine Verschärfungen zu beabsichtigen, zuwiderlaufen würden. In **lit. a** ist die Einschränkung „im Einzelfall“ weder sinnvoll noch notwendig, da selbst für wiederkehrende Sachverhalte wegen gleichbleibender Erkennbarkeit und unverändertem Erwartungshorizont eine einmalige Einwilligung ausreichen muss. Der Zusatz „im Einzelfall“ widerspricht auch der Gesetzessystematik, wonach nur für die unter lit. c und d genannten Fälle die „Bekanntgabe im Einzelfall“ geregelt werden soll. Der Zusatz „im Einzelfall“ ist deshalb bei lit. a ersatzlos zu

					streichen.
SFTI	DSG	6	b		In **Art. 6 VE-DSG** sind verschiedene Einschränkungen zu streichen, welche das bisherige Recht nicht kannte und die der erklärten Absicht des Gesetzgebers, auch unter neuem Recht keine Verschärfungen zu beabsichtigen, zuwiderlaufen würden. In **lit. b** ist der gewählte Wortlaut zu eng, da es regelmässig um Zusatzverträge geht, welche nicht direkt mit dem Vertragspartner abgeschlossen werden, aber in dessen Interesse liegen, weil z.B. solche Zusatzverträge nötig sind, um den mit dem Vertragspartner geschlossenen Vertrag zu erfüllen. Die Formulierung ist deshalb am Ende wie folgt zu ergänzen (Ergänzungen fett und unterstrichen): „ … des Vertragspartners **oder von Personen, in deren Interesse der Vertrag abgeschlossen werden soll,** handelt.
SFTI	DSG	8			Wir begrüssen insbesondere die in **Art. 8 VE-DSG** definierte Möglichkeit zur Erarbeitung von Empfehlungen der guten Praxis und den aktiven Beizug der interessierten Kreise. Allerdings sollen diese nicht vom Beauftragten, sondern von den jeweiligen Branchen selbst erarbeitet und auch nicht genehmigungspflichtig sein. Es soll an dieser Stelle keine Rechtsetzungskompetenz des Beauftragten eingeführt werden.
SFTI	DSG	13	2		**Informationspflichten:** In **Art. 13 VE-DSG** müssten die Grenzen der Informationspflicht klar abgesteckt werden. Dazu gehört z.B. im Rahmen von **Abs. 2** die Präzisierung, dass die zu erteilenden Informationen nur im erstmaligen Zeitpunkt der Datenbeschaffung richtig und vollständig sein müssen. Spätere Änderungen, insbesondere der Identität des Verantwortlichen, müssen der betroffenen Person nicht mitgeteilt werden. Diesbezüglich sollte insbesondere darauf verzichtet werden, dass der Verantwortliche namentlich genannt werden muss, da die Person des Verantwortlichen wechseln kann. Als Kontaktdaten des Verantwortlichen muss es genügen, dass eine klare und fix definierte Funktionsbeschreibung mitgeteilt wird.
SFTI	DSG	13	4		Problematisch und deshalb zu streichen, ist die Pflicht gemäss **Art. 13 Abs. 4 VE-DSG**, aktiv die *Identität* der Auftragsdatenbearbeiter bekannt zu geben. Die Identität von Auftragsdatenbearbeitern wird regelmässig zum Geschäftsgeheimnis eines Unternehmens gehören und damit wohl ohnehin unter die Ausnahmen von Art. 14 Abs. 3 VE-DSG fallen. Dementsprechend geht auch die EU-DSGVO nicht soweit, weshalb diese

					Regelung einen mit Blick auf die angestrebte Äquivalenz mit der europäischen Datenschutzgesetzgebung kontraproduktiven Swiss Finish darstellen würde. Absatz 4 wird primär im Rahmen von Outsourcing-Verhältnissen zum Tragen kommen, bei welchen die Verantwortung der Datenbearbeitung gegenüber der betroffenen Person beim auslagernden Unternehmen verbleibt, und auch nur dieses auskunftspflichtig sein kann. Es kann nicht sein, dass Dienstleistungserbringer gegenüber Kunden von Dritten auskunftspflichtig sind.
SFTI	DSG	14	3	a	**Art. 14 Abs. 3 lit. a VE-DSG** ist zu eng gefasst. Direkte Einschränkungen ergeben sich nur ganz selten aus einem Gesetz. Häufiger ist der Fall, dass ein Gesetz zwingende Abklärungspflichten, oft verbunden mit damit einhergehenden Geheimhaltungspflichten vorsieht, welche indirekt zu einer Einschränkung von Informationspflichten führen. Dies ist in der Regelung von Art. 14 Abs. 2 lit. a VE-DSG zu präzisieren und zum besseren Verständnis mit der Aufzählung einiger typischer Beispiele zu ergänzen. Zu denken ist etwa an zwingend vorgeschriebene Abklärungen zur Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Korruption.
SFTI	DSG	14	3	B	Unter **Art. 14 Abs. 3 lit. b VE-DSG** ist nicht einsehbar, weshalb nur überwiegende Interessen Dritter massgebend sein sollen. Gleichermassen müssen überwiegende Interessen des Verantwortlichen und überdies der Öffentlichkeit relevant sein. Nur eine umfassende Interessenabwägung kann in zahlreichen Konstellationen zu einer sachgerechten Lösung führen.
SFTI	DSG	15	1		**Automatisierte Einzelentscheidung:** Ein zentraler Punkt der Digitalisierung ist die Automatisierung. Gerade durch Automatisierung lassen sich Effizienzgewinne und damit einhergehend Aufwandreduktionen erzielen, welche im heutigen wirtschaftlichen Umfeld enorm wertvoll wenn nicht gar unabdingbar geworden sind. Um Klarheit zu schaffen, dass nicht jede (rechtliche) Wirkung, wie z.B. ein Geldbezug am Bankomat (Entscheid, ob Geld ausbezahlt wird, erfolgt automatisch) betroffen ist, sollte der Begriff „erhebliche“ wiederholt verwendet werden. Art. 15 Abs. 1 VE-DSG müsste folgendermassen ergänzt werden (Ergänzung fett und unterstrichen): „…und diese **erhebliche** rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffenen Person hat“

SFTI	DSG	15	2		Das in **Art. 15 Abs. 2 VE-DSG** neu vorgeschlagene Recht einer betroffenen Person, sich zu einer automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern („Anhörungspflicht"), stufen wir als wettbewerbs- und auch innovationsbehindernd ein. Darüber hinaus ist dieses Recht aber auch schlicht unnötig, insbesondere angesichts der ebenfalls neu eingeführten Pflicht, die betroffene Person darüber zu informieren, wenn eine automatisierte Einzelentscheidung gefällt wurde (vgl. Abs. 1 von Art. 15 VE-DSG). Die Kunden können selbst entscheiden, ob sie von einem Anbieter Dienstleistungen beziehen möchten, der voll-automatisierten Entscheide trifft oder zu einem Anbieter, der zusätzlich oder vollständig auf die Arbeitskraft natürlicher Personen setzt. Der Kunde wird davon gemäss Art. 15 Abs. 1 VE-DSG bereits ausreichend informiert (z.B. mit einem Piktogramm). Art. 15 Abs. 2 VE-DSG ist ersatzlos zu streichen. (Folgerichtig ist auch der entsprechende thematische Abschnitt in Art. 20 Abs. 3 VE-DSG zu streichen, vgl. unten.)
SFTI	DSG	16			**Datenschutz-Folgenabschätzung** Die vorgeschlagene Bestimmung in **Art. 16 VE-DSG** ist sehr unklar formuliert und soll gemäss dem erläuternden Bericht sehr extensiv ausgelegt werden. So werden als Indiz für ein erhöhtes Risiko fast alle denkbaren Tätigkeiten/Tatbestände im Umgang mit Daten aufgezählt. Trotz der sehr offenen und unklaren Bestimmung soll ein Verstoss gegen die Bestimmung strafrechtlich sanktioniert werden. Dies widerspricht klar dem strafrechtlichen Prinzip von „nulla poena sine lege stricta". Eine Datenbearbeitung braucht für ein Unternehmen, das die Bestimmungen des Datenschutzgesetzes einhalten will, bereits heute eine fachkundige Beurteilung und entsprechende Massnahmenpakete. Dies gesetzlich zu verankern, inklusive einer Benachrichtigungspflicht an den Beauftragten, der innerhalb einer relativ langen Frist Einwände mitteilen kann und später, trotz Nichtäusserung, eine Untersuchung einleiten kann, bringt keinen Mehrwert, sondern verursacht vielmehr erhebliche Rechtsunsicherheit. Schliesslich wird auch der Beauftragte massiv grösseren Aufwand haben, wenn er jede dieser Einschätzungen zu studieren und zu beurteilen hat. Hat der Beauftragte die dafür notwendigen Kapazitäten

					gar nicht, macht die Regel definitiv keinen Sinn, sondern produziert nur unnötigen Aufwand für die Verantwortlichen. Wenn schon müsste die Pflicht zur Datenschutzfolgeabklärung, wie auch gemäss EU-DSGVO, auf Datenbearbeitungen mit hohen Risiken beschränkt werden. Damit sind nach EU-Doktrin solche gemeint, welche auch nach Implementierung geeigneter Massnahmen gleichwohl immer noch hohe Risiken aufweisen. In Art. 16 Abs. 1 VE-DSG wären überdies als Regelungsgrundlage nicht „Persönlichkeit oder Grundrechte“ zu verwenden, sondern entsprechend der Schweizer Gesetzessystematik der Begriff „Persönlichkeitsverletzung“ (vgl. insb. Art. 23 ff. VE-DSG).
SFTI	DSG	16	1		Die Begriffe „voraussichtlich“ und „erhöht“ in Zusammenhang mit dem Risiko sind unklar. In der Schweiz gibt es keine Drittwirkung für Grundrechte, weshalb private Datenbearbeiter ein Risiko für Grundrechte nicht zu prüfen haben. Dies ist klarzustellen. Schliesslich ist es unsinnig, den Auftragsdatenbearbeiter als Dienstleistungserbringenden für den Verantwortlichen ebenfalls zu verpflichten, eine Datenschutz-Folgenabschätzung durchzuführen. Diese Überlegungen führen zu folgenden Änderungsanträgen: „Führt die vorgesehene Datenbearbeitung **mit überwiegender Wahrscheinlichkeit** zu einem hohen Risiko für die Persönlichkeit ~~**oder die Grundrechte**~~ der betroffenen Person, so muss der Verantwortliche ~~**oder der Auftragsdatenbearbeiter**~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen.“
SFTI	DSG	17			**Meldepflicht bei Verletzung des Datenschutzes** Die in **Art. 17 VE-DSG** vorgeschlagene Meldepflicht hat einen klaren rechtsdogmatischen Mangel. Zwar wird auch ein Verstoss gegen die Meldepflicht selbst sanktioniert, wenn die Verletzung entdeckt würde, aber die Meldung gemäss Art. 17 entspricht einer Selbstanzeige, welche mit Sicherheit zu einer Sanktion führt, weil für diesen Fall keine Erleichterungen bei den Sanktionen vorgesehen sind (anders als z.B. im Kartellrecht). Entsprechend wird ein korrekt handelndes Unternehmen auf jeden Fall bestraft, während die wirklich „schwarzen Schafe“, welche nicht im Traum daran denken, eine DSG-Verletzung zu melden, mangels Bekanntwerden des Sachverhaltes i.d.R. straffrei bleiben dürften. Diese Regelung verfolgt den falschen Ansatz, am Worst Case anzuknüpfen und damit letztlich nur die Masse der im Normalfall korrekt Handelnden zu belasten, ohne den Worst Case tatsächlich verhindern zu können. Wir bezweifeln ferner die Sinnhaftigkeit dieser Regel. Bei Datenschutzverstössen steht immer auch die

					Reputation eines Unternehmens auf dem Spiel. Insofern ist es im Eigeninteresse eines jeden seriösen Unternehmens, Kunden korrekt und rechtzeitig zu informieren. Dies hat den auch bisher immer auch ohne gesetzliche Vorschriften funktioniert. Infolge dessen sollte diese Bestimmung ersatzlos gestrichen werden. Soweit sie wider Erwarten nicht gestrichen werden sollte, müsste sie jedenfalls auf wirklich heikle Fälle beschränkt werden. Diese Fälle sind mit qualitativen und quantitativen Kriterien angemessen einzugrenzen. Qualitative Kriterien wären insbesondere ein hoher Verletzungsgrad (analog EU-DSGVO) und die Tatsache, dass durch die Meldung an den Beauftragten ein Mehrwert geschaffen werden kann, z.B. mittels Unterstützung durch den Beauftragten in Fällen, welche vom betroffenen Verantwortlichen nicht mehr allein aus eigener Kraft bereinigt werden kann. Dies kann z.B. dann der Fall sein, wenn - als quantitatives Kriterium durch ein grösseres Sicherheitsleck massenweise Kundendaten gestohlen oder öffentlich werden. Zudem wäre die „unverzügliche“ Meldepflicht gemäss Art. 17 Abs. 4 VE-DSG zu präzisieren. Eine Meldepflicht kann sachlogisch erst ab dem Zeitpunkt bestehen, in welchem der Verantwortliche mit einiger Klarheit weiss, was überhaupt geschehen ist und welche Kunden (-Segmente) betroffen sind. Ohne diese Eingrenzungen wäre die Schweizer Regelung überschiessend und entgegen dem Revisionszweck nicht äquivalent mit der entsprechenden europäischen Gesetzgebung. Zudem wäre die Regelung auch deshalb unsinnig, weil jedes seriöse Unternehmen zwecks Vermeidung strafrechtlicher Vorwürfe jeden noch so kleinen Verstoss melden würde und der Beauftragte aufgrund der Papierflut keine Möglichkeit hätte, in geeigneter Weise zu reagieren. Bei dieser Sachlage würde sich der Beauftragte im Einzelfall höchstens noch mit dem Vorwurf konfrontiert sehen, in einem ganz krassen Fall zu Unrecht nicht in geeigneter Weise reagiert zu haben. Damit verkäme die Meldepflicht zu unnötigem Mehraufwand für die Wirtschaft ohne erkennbaren Sinn und Zweck.
SFTI	DSG	19		a	**Art. 19 lit. a VE-DSG** ist zum Zweck der Schaffung von Rechtssicherheit zu präzisieren. Eine blosse Dokumentationspflicht belässt extrem weiten Spielraum mit Bezug auf Form und Inhalt. Wir schlagen deshalb vor, die Dokumentationspflicht durch das Erfordernis eines Verzeichnisses zu ersetzen. Damit wird auch Gleichlauf mit der EU-DSGVO hergestellt.
SFTI	DSG	19		b	**Art. 19 lit. b VE-DSG** ist eine massive Verschärfung der heutigen Rechtslage und würde zu komplizierten Abläufen und grossen (finanziellen) Aufwänden führen. SFTI setzt sich aus folgenden Gründen für eine

					Streichung dieser Bestimmung ein: • Der aktuelle Vorschlag würde dazu führen, dass Finanzinstitute in die Rolle eines (öffentlichen) Registers gedrängt würden und für die ständige Aktualisierung der Daten auch bei Dritten sorgen müssten. Solche Pflichten sind überschiessend und sprengen den Rahmen einer vernünftigen Datenschutzgesetzgebung. • Der Nutzen dieser Bestimmung im Hinblick auf nicht besonders schützenswerte Daten ist besonders fragwürdig. Schliesslich sind viele nicht besonders schützenswerte Daten sogar öffentlich zugänglich (z.B. über Internetrecherche). • Es kommt dazu, dass betroffene Personen ihre Rechte in diesem Bereich bereits unter Art. 25 VE-DSG geltend machen können. Materiell identische Pflichten an verschiedenen Stellen desselben Gesetzes mit unterschiedlichem Wortlaut zu formulieren, ist der Klarheit und Rechtssicherheit abträglich. Nach alledem fordern wir die ersatzlose Streichung von lit b des Art. 19 VE-DSG.
SFTI	DSG	20/21			**Auskunftsrecht:** Die Information darüber, wie bestimmte Entscheide zustande kommen, gehört zum Geschäftsgeheimnis eines Finanzinstitutes und ist demnach, insbesondere in der aktuell vorgesehen, detaillierten Form gemäss Art. 20 Abs. 3 VE-DSG, klar unverhältnismässig. So ist zum Beispiel das Vorgehen im Rahmen der Einschätzung von Ausfallrisiken bei der Kreditvergabe ein wichtiges, differenzierendes Know-How eines Finanzdienstleisters. Die Auskunft über die für diese Einschätzung genutzten Daten und deren Gewichtung führt zu einer Replizierbarkeit dieser Einschätzung und damit zur Aufgabe dieses Geschäftsgeheimnisses. Die Einschränkungsbestimmung des Art. 21 Abs. 1 VE-DSG dürfte daher mehr die Regel als die Ausnahme bilden. Schliesslich ist die Befürchtung nicht von der Hand zu weisen, dass die Einführung einer „Pflicht zur Anhörung“ zu einer Begründungspflicht führt und letztlich die Vertragsfreiheit eines Finanzdienstleisters erheblich einschränkt. SFTI setzt sich vehement für eine Streichung der Anhörungspflicht von Art. 15 Abs. 2 VE-DSG ein (vgl. oben). Folgerichtig ist auch der entsprechende thematische Abschnitt in Art. 20 Abs. 3 VE-DSG zu

					streichen. Sollte dem Antrag auf Streichung wider Erwarten nicht gefolgt werden, müsste jedenfalls Art. 20 Abs. 3 VE-DSG als dort - unter dem allgemeinen Auskunftsrecht - sachfremde Regelung gestrichen und mit Art. 15 VE-DSG zu einer in sich stimmigen Gesamtlösung verbunden werden. Dabei wäre die Regelung (entsprechend dem richtigen Ansatz der EU-DSGVO, mit welchem der VE-DSG äquivalent sein will) auf schwere Fälle zu begrenzen. Sodann wäre klarzustellen, dass eine einmal in angemessener Art und Weise erfolgte Information im Sinne der Gesetzessystematik ausreichend ist.
SFTI	DSG	50 ff.			**Sanktionen** Mit Bezug auf die vorgeschlagenen Sanktionen bzw. das vorgeschlagene Sanktionsmodell verweist SFTI auf die diesbezügliche Stellungnahme von economiesuisse („Vorschlag der Wirtschaft“), welche vollumfänglich unterstützt wird.

Aus diesen Gründen bitten wir Sie um Berücksichtigung unserer Anliegen. Gerne stehen wir Ihnen zur Diskussion und für die weitere Zusammenarbeit jederzeit zur Verfügung.

Für die Arbeitsgruppe Regulation von SFTI:
Cornelia Stengel, Werner Wyss, Noemi Heusler

Amstutz Jonas BJ

Von: Christian Amgwerd, Swiss Infosec AG <christian.amgwerd@infosec.ch>
Gesendet: Montag, 3. April 2017 10:53
An: Amstutz Jonas BJ
Cc: Reto Zbinden, Swiss Infosec AG
Betreff: Stellungnahme Vernehmlassung VE-DSG
Anlagen: Stellungnahme_Vernehmlassung_VE-DSG_SwissInfosecAG.doc
Signiert von: christian.amgwerd@infosec.ch

Sehr geehrter Herr Amstutz

Gerne nimmt die Swiss Infosec AG unter Einhaltung der Vernehmlassungsfrist mit angehängtem Schreiben Stellung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz.

Sollten dazu Fragen bestehen können Sie mich gerne kontaktieren.

Freundliche Grüsse

Christian Amgwerd
MLaw

E-Mail christian.amgwerd@infosec.ch
Direkt +41 79 231 95 11

Swiss Infosec AG | Beratung, Ausbildung, Services, Tools
Centralstrasse 8A, 6210 Sursee, +41 41 984 12 12
www.infosec.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Swiss Infosec AG

Abkürzung der Firma / Organisation :

Adresse : Centralstrasse 8A, 6210 Sursee

Kontaktperson : Reto Zbinden, CEO, Rechtsanwalt

Telefon : +41 79 446 83 00

E-Mail : reto.zbinden@infosec.ch

Datum : 30. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
	Verzicht auf den bDSB schwächt den Datenschutz **1 Einleitung** Der vorliegende Vorentwurf zum DSG (im Folgenden VE-DSG) enthält keine Verpflichtung von privaten Personen zur Ernennung einer spezifischen Funktion im Bereich Datenschutz. Daher kann in der vorliegenden Stellungnahme nicht auf einen entsprechenden Artikel Bezug genommen werden und die Ausführungen sowie Anträge erfolgen unter «Allgemeine Bemerkungen». Der Verzicht auf die im aktuellen Gesetz festgehaltene Funktion «Betrieblicher Datenschutzverantwortlicher», geregelt in Art. 11a DSG (*https://www.admin.ch/opc/de/classified-compilation/19920153/index.html#)* und konkretisiert in Art. 12a und Art. 12b VDSG (*https://www.admin.ch/opc/de/classified-compilation/19930159/index.html*), wird im erläuternden Bericht zum VE-DSG ohne weitere Begründungen nicht erwähnt und nicht erklärt. Obwohl auf europäischer Ebene eine Pflicht zur Einsetzung eines bDSB gilt, wird im VE-DSG ohne weitere Begründung auf eine solche verzichtet und gleichzeitig die Rechtsgrundlage für die über 1000 beim EDÖB gemeldeten bDSB entzogen. **Die Bezeichnung eines Betrieblichen Datenschutzbeauftragten (bDSB) stellt in der Praxis eine unabdingbare Grundvoraussetzung für die Umsetzung des Datenschutzes dar. Zudem kann und soll die Benennung eines bDSB die Verantwortlichen und Auftragsbearbeiter von verschiedenen Meldepflichten an den Beauftragten entlasten, aber auch den Beauftragten (EDÖB) von der Entgegennahme, Prüfung und Genehmigung dieser Informationen. Aufgaben des Beauftragten (EDÖB) werden so in die Unternehmen verlegt, die für den Datenschutz heikle Bearbeitungen durchführen. Wo immer möglich soll nicht der Staat für die Umsetzung von Rechtsvorschriften sorgen, sondern die dem Gesetz unterstellten Unternehmen durch interne organisatorische Regelungen. Administrative Leerläufe sind unbedingt zu verhindern. Mit der Beibehaltung und qualitativen und quantitativen Stärkung der Rolle des bDSB kann der Datenschutz gestärkt werden. Die Einsetzung von Datenschutzbeauftragten sollte seitens des Gesetzgebers und des EDÖB aktiv gefördert werden** **Zudem muss berücksichtigt werden, dass mit dem Verzicht auf die gesetzliche Verankerung die Rechtsgrundlage für die heute bereits eingesetzten Datenschutzbeauftragten - dringend notwendige Ressourcen für die Umsetzung der technischen und organisatorischen Massnahmen zum Schutz der elektronisch bearbeiteten Personendaten - entzogen würde, was auch zu einer Schwächung der gesamten Informationssicherheit führt.** Mit dem Verzicht auf die gesetzliche Verankerung eines bDSB würden in der Praxis wichtige Ressourcen für die Umsetzung des Datenschutzes verloren gehen (Art. 12b Abs. 2 lit. b DSG) welche sich auch mit der rasanten Entwicklung der Technik

	datenschutzrechtlich auseinanderzusetzen hatten (vgl. Ziele der Revision Ziff. 1.3 Bericht-VE). **Die vorliegende Stellungnahme verwendet absichtlich den Begriff «Betrieblicher Datenschutzbeauftragter» zur Abgrenzung von den für die Einhaltung des Datenschutzes verantwortlichen Organe. Die aktuelle gesetzliche Bezeichnung als «Datenschutzverantwortlicher» ist diesbezüglich unbefriedigend und zu korrigieren.** Die Notwendigkeit zur Einsetzung eines Datenschutzbeauftragten wurde auch von der **Europäischen Union** erkannt. Sie hat die Einsetzung eines Datenschutzbeauftragten in Art. 37 der Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 (im Folgenden **DSGVO**, *http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679*) aufgenommen. Der Verzicht auf die gesetzliche Verankerung eines bDSB im VE-DSG entspricht somit auch nicht der Stossrichtung der bereits in Kraft getretenen DSGVO, die nun bis zum 25. Mai 2018 durch alle Unternehmen in der EU umgesetzt werden muss und gemäss Geltungsbereich des Art. 3 DSGVO auch für bestimmte Schweizer Unternehmen Anwendung finden wird. Analog ist die Funktion des Datenschutzbeauftragten in Randziffer 63 Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 (im Folgenden Schengen-RL, *https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/eu-richtlinie-d.pdf*) ebenfalls ausdrücklich erwähnt. Es stellt sich die **Frage, inwieweit es sinnvoll ist, auf einen bDSB zu verzichten, obwohl dessen Funktion ausdrücklich in der DSGVO wie auch Schengen-RL vorgesehen ist und das Ziel der Revision u.a. darin liegt, sich der europäischen Entwicklung anzugleichen (Art. 1.3 Bericht-VE).** **2 Historische Entwicklung** Der «Betriebliche Datenschutzverantwortliche» ist seit der Revision des DSG im Jahr 2008 gesetzlich vorgesehen. In den Erläuterungen zu den Änderungen vom 17. Dezember 2004 und vom 24. März 2006 des Bundesgesetzes über den Datenschutz (*https://www.edoeb.admin.ch/datenschutz/00628/00784/index.html?lang=de&download=NHzLp-Zeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdXx4hGym162epYbg2c_JjKbNoKSn6A--*) äusserte sich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) zu den Gründen, die die Berufung eines bDSB empfehlenswert machen. Die Institution des «Datenschutzverantwortlichen» innerhalb eines Unternehmens oder einer öffentlichen Verwaltung existiere bereits in verschiedenen Ländern (namentlich Deutschland, Frankreich, den Niederlanden und Schweden) und werde nicht nur von den Datenschutzbehörden, sondern auch von den Unternehmen und den Verwaltungen, die sie eingeführt haben, positiv bewertet. Basierend auf der revidierten Fassung des DSG haben bis 27. Januar 2017 über 1000 Unternehmen ihren Betrieblichen Datenschutzverantwortlichen dem EDÖB formell gemeldet.

	3 Internationaler Vergleich **EU:** Die DSGVO sieht in Art. 37 klare Kriterien für die Notwendigkeit einer Ernennung eines Datenschutzbeauftragen vor. Insbesondere ist dies dann der Fall, wenn personenbezogene Daten, welche gemäss Schweizer Rechtsordnung in den Geltungsbereich der besonders schützenswerten Personendaten fallen, bearbeitet werden (Art. 3 lit. c VE-DSG und Art. 37 i.V.m. Art. 9 DSGVO). Die Wichtigkeit des Themas zeigt sich auch darin, dass die erste überhaupt publizierte Good Practice zur DSGVO gerade die Rolle und die Funktion dieser Datenschutzbeauftragten betraf (*http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf*). **Deutschland** wird gemäss Entwurf des Gesetzes zur Anpassung des Datenschutzrechts an die DSGVO sowie Schengen-RL (im Folgenden VE-DSAnpUG-EU, *http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/entwurf-datenschutz-grundverordnung.html*) voraussichtlich die Anforderungen und die Verpflichtung zur Ernennung eines Datenschutzbeauftragten zusätzlich in seinen nationalen Gesetzen verschärfen. Gemäss Paragraph 38 des VE-DSAnpUG-EU **muss** der Verantwortliche und der Auftragsverarbeiter **eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benennen**, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO unterliegen oder verarbeiten sie personenbezogene Daten geschäftsmässig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie **unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen**. Weiter sollte gemäss Randziffer 63 der **Schengen-RL** der Verantwortliche eine Person benennen, die ihn dabei unterstützt, die interne Einhaltung der nach dieser Richtlinie erlassenen Vorschriften zu überwachen, es sei denn, ein Mitgliedstaat beschliesst eine Ausnahmeregelung für Gerichte und andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit. Mehrere Verantwortliche können dabei unter Berücksichtigung ihrer Organisationsstruktur und ihrer Grösse gemeinsam einen Datenschutzbeauftragten bestellen. Sodann ist zu berücksichtigen, dass im Kommentar zur **Revision der Europaratskonvention SEV 108** (*https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2*) gemäss Art. 8bis RZ 84 ausdrücklich auf die Einsatzmöglichkeit eines bDSB hingewiesen wird. Ein solcher betrieblicher Datenschutzbeauftragter könnte sowohl intern wie auch extern eingesetzt werden und sollte der Behörde gemeldet werden (*«A possible measure that could be taken by the controller to facilitate such a verification and demonstration of compliance would be the designation of a 'data protection officer' entrusted with the means necessary to fulfil his or her mandate. Such a data protection officer, whose designation should be notified to the supervisory authority, could be internal or external to the controller.»).*

	4 Erkenntnisse der eingesetzten Begleitgruppe Gemäss Ziff. 4.9.4 des Normkonzepts zur Revision des Datenschutzgesetzes vom 29. Oktober 2014 (*https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf*) kam die eingesetzte Begleitgruppe zum Schluss, dass die Eigenverantwortung der öffentlichen Datenbearbeitenden für die Einhaltung der datenschutzrechtlichen Vorschriften gestärkt und gefördert werden soll. Bei den Bundesorganen soll dabei (anstelle des heutigen «Beraters für den Datenschutz» gemäss Art. 23 VDSG) immer ein «Datenschutzverantwortlicher» im Sinne von Art. 12a und 12b VDSG, eingesetzt werden müssen (Ziff. 4.3.2). Für die Umsetzung in Unternehmen schlägt ein Teil der Begleitgruppe vor, ab einer bestimmten Grösse die Verpflichtung für den Einsatz eines «Datenschutzverantwortlichen» vorzusehen (Ziff. 4.3.2). Der Bundesrat könnte diese Verpflichtung auf kleinere Unternehmen ausweiten, bei denen ein erhöhtes Risiko besteht. Der Begriff «erhöhtes Risiko» wäre in der Botschaft, in der Verordnung oder in den Regeln der Guten Praxis bzw. in verbindliche Detailregeln (vgl. Ziff. 4.1.2 lit. b) zu präzisieren. Ein anderer Teil der Begleitgruppe ist der Meinung, dass die Verpflichtung zur Einsetzung eines bDSB nicht im Gesetz festgehalten werden solle. Stattdessen könne es den Regeln der Guten Praxis (vgl. Ziff. 4.1.2 lit. b) überlassen werden, je nach Unternehmen angemessene Mittel vorzusehen, um eine Datenbearbeitung zu gewährleisten, mit welcher den Rechten der betroffenen Personen Rechnung getragen wird (z.B. durch die Bestimmung eines Datenschutzverantwortlichen). Gemäss Ausführungen dieser Begleitgruppe bestehen jedoch keine Zweifel, dass bei den Bundesorganen ein «Datenschutzverantwortlicher» eingesetzt werden muss. Im VE-DSG fehlt ein solcher «Datenschutzverantwortlicher» bei den Bundesorganen wie auch für private Personen nun gänzlich. Den Anforderungen der Begleitgruppe wird in diesem Punkt somit nicht entsprochen. Bezgl. den unterschiedlichen Meinungen zum Einsatz eines Datenschutzverantwortlicher» in Unternehmen ist anzumerken, dass im Rahmen einer Verordnung keine Verschärfung des Gesetzes statthaft ist, insbesondere auch nicht in Regeln der Guten Praxis. Eine gesetzliche Verpflichtung zum Einsatz eines Datenschutzbeauftragten mit entsprechenden Erleichterungen bzw. Ausnahmen seitens Bundesrat/Verordnung ist hingegen zu empfehlen. **5 Notwendigkeit eines DSB in der Praxis** Aus Sicht der Praxis ist festzuhalten, dass die Verpflichtung zur formellen Bezeichnung einer für den Datenschutz zuständigen Stelle innerhalb eines Unternehmens die Umsetzung und die Güte der Datenschutzaktivitäten eindeutig positiv beeinflusst. Bereits mit dem Einsatz eines «betrieblichen Datenschutzverantwortlichen» gemäss Art. 11a Abs. 5 lit. e DSG wurde der Datenschutz gestärkt.

	Die Bezeichnung eines bDSB verbessert die Umsetzung der gesetzlich verankerten Grundsätze, die Berücksichtigung der Datenschutzanforderungen im Rahmen von Projekten und ermöglicht erst die Beantwortung offener Fragen zur Anwendung und Umsetzung des Datenschutzes. **Die Konzeption und Umsetzung der technischen und organisatorischen Massnahmen zum Schutz der elektronisch bearbeiteten Personendaten ist auch ein Teil der Aufgaben der mit der Informationssicherheit und der Datensicherheit beauftragten Stellen eines Unternehmens. In den meisten Fällen kann sich aber ausschliesslich der bDSB auf eine gesetzliche Grundlage und Notwendigkeit stützen. Innerhalb einer IT-Organisation und eines Unternehmens bestehen neben dem bDSB als Unterstützungs- und Überwachungsinstanz im gesamten Bereich der Informationssicherheit keine weiteren gesetzlich vorgesehenen Funktionen, ausser in speziell regulierten Bereichen. Die Tätigkeit eines bDSB fördert also die Güte und Qualität der Umsetzung der technischen und organisatorischen Massnahmen nicht nur bei der digitalen Bearbeitung von Personendaten, sondern darüber hinaus generell die Umsetzung der Anforderungen in den Bereichen der Informations- und Datensicherheit.** Die im Gesetz festgehaltenen Informationspflichten, Anforderungen an die Auftragsdatenbearbeitung, an die Sicherheit der Bearbeitung von Personendaten, die Informationspflichten, die Datenschutzfolgeabschätzung, die Meldung von Datenschutzverletzungen und die durch die Technik ermöglichten datenschutzfreundlichen Datenschutzeinstellungen können innerhalb eines Unternehmen nur dann wahrgenommen und umgesetzt werden, wenn es über eine entsprechend ausgeprägte Datenschutzorganisation verfügt. In der Praxis verfügen aber fast nur Grossunternehmen über entsprechende Ressourcen. **Ohne die Verpflichtung zur Einsetzung eines bDSB wird ein grosser Teil der Unternehmen auf die entsprechenden Ressourcen verzichten und den Handlungsbedarf im Bereich Datenschutz weder erkennen noch wahrnehmen.** Basierend auf dem geltenden Datenschutzrecht wurde bereits erreicht, dass über 1000 Unternehmen dem EDÖB die Einsetzung eines bDSB gemeldet haben. Diese würden ihren gesetzlichen Auftrag verlieren und der Datenschutz entsprechend geschwächt und nicht wie beabsichtigt gestärkt. **6 Fehlende Begründung** Unter Anbetracht der genannten Gründe erscheint es daher nicht nachvollziehbar, warum auf die gesetzliche Verankerung eines bDSB verzichtet werden soll. Insbesondere hätten die bestehenden Vorteile des geltenden Rechts berücksichtigt und allfällige Abweichungen ausführlich begründet werden müssen, was aber nicht erfolgt ist. Vergleicht man den VE-DSG mit dem VE-SEV 108, werden im VE-DSG u.a. Regelungen aufgenommen, welche vom VE-SEV 108 nicht gefordert werden (Daten Verstorbener [Art. 12 VE-DSG], kein datenschutzrechtliches Thema bei VE-SEV 108; zwingende Meldepflicht [Art. 6 Abs. 2 VE-DSG], jedoch ausschliesslich Meldepflicht auf Antrag gemäss Art. 12 Abs. 5 VE-SEV 108). Weiter werden Instrumente wie die Datenschutz-

	Folgeabschätzung (Art. 16 VE-DSG), Privacy by Design (Art. 18 Abs. 1 VE-DSG) und Privacy by Default (Art. 18 Abs. 2 VE-DSG) eingeführt, welche vom VE-SEV 108 nicht in dieser ausdrücklichen Art gefordert werden. Viel mehr dürften diese Instrumente direkt der DSGVO entnommen worden sein. Vor diesem Hintergrund ist es nicht ersichtlich, weshalb die gesetzliche Verankerung des bDSB überhaupt ohne weitere Begründung entfernt wurde. Insbesondere muss berücksichtigt werden, dass im Kommentar zur Revision der Europaratskonvention SEV 108 die Möglichkeit des Einsatzes eines bDSB zumindest genannt wird und mit dem Einsatz eines bDSB die Anforderungen nach Art. 8 Abs. 2 Entwurf SEV 108 umgesetzt werden könnten. **7 Anträge** Aufgrund dieser Überlegungen wird der Antrag gestellt, die Funktion des «Betrieblichen Datenschutzbeauftragten» im Datenschutzgesetz wie folgt zu berücksichtigen: **Neuer Artikel 11bis: Bezeichnung eines Betrieblichen Datenschutzbeauftragten** 1 Verantwortliche und Auftragsbearbeiter können einen Datenschutzbeauftragten bezeichnen, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht. 2 Zur Bezeichnung eines Datenschutzbeauftragten sind verpflichtet a. Bundesorgane wenn sie Personendaten bearbeiten b. Auftragsbearbeiter wenn sie als wesentlicher Teil ihrer geschäftlichen Verrichtungen Personendaten für Verantwortliche bearbeiten c. Verantwortliche wenn sie zur Durchführung einer Datenschutz-Folgeabschätzung verpflichtet sind, oder wenn sie mehr als zehn Personen ständig mit der Bearbeitung personenbezogener Daten selbst oder über Dritte beschäftigen, oder wenn sie ohne gesetzliche Pflicht als wesentlicher Teil ihrer geschäftlichen Verrichtungen regelmässig 1 besonders schützenswerte Personendaten Dritter bearbeiten oder personenbezogenes Profiling betreiben;

	2 Personendaten nicht bei der betroffenen Person beschaffen; 3 Personendaten an Dritte bekanntgeben; 4 Personendaten ins Ausland bekanntgeben; 5 Entscheidungen über Personen treffen, die ausschliesslich auf einer automatisierten Datenbearbeitung beruhen. 3 Der Datenschutzbeauftragte kann Arbeitnehmer des Verantwortlichen oder des Auftragsbearbeiters sein oder seine Aufgaben im Auftragsverhältnis erfüllen. 4 Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und dem Beauftragten mitzuteilen. 5 Der Bundesrat regelt Ausnahmen von der Pflicht zur Bestimmung eines Datenschutzbeauftragten, die Stellung und Aufgaben des betrieblichen Datenschutzbeauftragten sowie die Auswirkung seiner Bezeichnung auf die Einhaltung der Datenschutzschutzvorschriften. **Ergänzung in Art. 6 Abs. 2 Bekanntgabe ins Ausland in Ausnahmefällen (roter Text):** Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten oder dem Betrieblichen Datenschutzbeauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt. **Neuformulierung Art. 16 Abs. 3 Datenschutz-Folgeabschätzung (roter Text):** [3] Die Datenschutz-Folgeabschätzung und die vorgesehenen Massnahmen sind dem Beauftragten mitzuteilen oder in Zusammenarbeit mit dem Betrieblichen Datenschutzbeauftragten zu erarbeiten und dem Beauftragten im Rahmen einer Untersuchung oder auf dessen Aufforderung hin vorzulegen. Der Betriebliche Datenschutzbeauftragte kann dem Beauftragten die Datenschutz-Folgeabschätzung und die vorgesehenen Massnahmen zur Beurteilung unterbreiten. **Neuer Art. 17 Abs. 5 Meldung von Verletzungen des Datenschutzes (roter Text):** Verantwortliche und Auftragsbearbeiter treffen organisatorische und technische Massnahmen zur Feststellung der Ursache der Verletzung des Datenschutzes, zur Verhinderung künftiger Verletzungen bzw. zur Milderung ihrer möglichen nachteiligen Auswirkungen. Sie haben bei der Erfüllung ihrer Pflichten bei Verletzungen des Datenschutzes den Betrieblichen Datenschutzbeauftragten beizuziehen und dokumentieren alle Verletzungen

	des Schutzes personenbezogener Daten, deren Umstände und die ergriffenen Massnahmen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung

Amstutz Jonas BJ

Von: Liliane Sieber <liliane.sieber@swisstextiles.ch>
Gesendet: Dienstag, 4. April 2017 10:09
An: Amstutz Jonas BJ
Cc: Peter Flückiger
Betreff: Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes
Anlagen: SwissTextiles_VE_DSG.docx

Sehr geehrte Damen und Herren
Fristgerecht stellen wir Ihnen unsere Stellungnahme zum eingangs erwähnten Vorentwurf zu und bedanken uns im Voraus für die Berücksichtigung unserer Anmerkungen.

Freundliche Grüsse
Liliane Sieber

Dr. iur. Liliane Sieber
Leitung Arbeitgeber- und Sozialpolitik und Geistiges Eigentum

Swiss Textiles
Textilverband Schweiz, Fédération textile Suisse, Swiss textile federation
Beethovenstrasse 20, Postfach, CH-8022 Zürich
T +41 44 289 79 35, F +41 44 289 79 80
liliane.sieber@swisstextiles.ch, www.swisstextiles.ch

Stellungnahme von

Name / Firma / Organisation : Swiss Textiles Textilverband Schweiz

Abkürzung der Firma / Organisation : Swiss Textiles

Adresse : Beethovenstrasse 20

Kontaktperson : Liliane Sieber

Telefon : 044 289 79 35

E-Mail : liliane.sieber@swisstextiles.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Allgemeine Bemerkungen	
Name/Firma	**Bemerkung/Anregung**
	Wir danken für die Möglichkeit, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VEDSG) Stellung nehmen zu können und lassen Ihnen diese nachstehend wie folgt zukommen:
	Allgemeine Bemerkungen Swiss Textiles repräsentiert gut 200 KMU, welche Textilien und Bekleidung in der Schweiz herstellen und/oder damit handeln. Die Branche ist innovativ, exportorientiert, hoch spezialisiert und nachhaltig. Die Unternehmen sind einem starken internationalen Wettbewerb und Kostendruck ausgesetzt. Fast 80% der Produkte unserer Industrie werden exportiert, die Frankenstärke trifft unsere Unternehmen deshalb äusserst hart. Es ist wichtig, dass sich diese jetzt auf ihr Hauptgeschäft konzentrieren können. Im Datenschutzgesetz ist deshalb für die Unternehmen am Standort Schweiz ein Maximum an Flexibilität und ein Minimum an Belastung zu wahren. Vorschriften, welche personelle und finanzielle Ressourcen in den Unternehmen binden, lehnen wir ab. Anlässlich der Inkraftsetzung der neuen EU Datenschutzverordnung (DSGVO) per 1. Januar 2018 soll unser Datenschutzgesetz revidiert werden. Zufolge der extraterritorialen Wirkung werden zahlreiche Schweizer Unternehmen zukünftig in den Geltungsbereich der neuen EU DSGVO fallen. Dies ist zum Beispiel dann der Fall, wenn sie Daten von Personen in der EU bearbeiten, weil sie diesen Produkte oder Dienstleistungen anbieten bzw. liefern. Damit unterstehen diese Unternehmen zugleich auch der Aufsicht der nationalen EU-Datenschutzbehörden und diese sieht abschreckend hohe Bussen bei Verstössen vor. Die Schweiz verfügt heute über ein von der EU als gleichwertig anerkanntes Datenschutzgesetz. Unternehmen können ohne zusätzliche Massnahmen Daten zwischen der Schweiz und EU-Staaten austauschen. Diesen Standortvorteil dürfen wir nicht aufgeben. Dennoch ist die Schweiz verpflichtet, die neue Konvention des Europarates zum Datenschutz umzusetzen. Der vorliegende Vorentwurf lehnt sich stark an die EU-Datenschutz-Grundverordnung. Damit soll sichergestellt werden, dass der Schweiz aus EU-Sicht auch weiterhin ein angemessenes Datenschutzniveau attestiert werden kann. Der Vorentwurf sieht dazu Neuerungen vor für die Verantwortlichen, die Auftragsbearbeiter wie auch die Betroffenen. Diverse Informations- und Meldepflichten sind aus unserer Sicht jedoch überschiessend. Sie bedeuten für unsere Mitglieder einen unverhältnismässigen Aufwand und generieren eine regelrechte «Flut» an Informationen und Meldungen. Speziell zu berücksichtigen gilt der Nutzen von Daten für unsere Industrie. Zentral ist, dass die neuen Bestimmungen für die Unternehmen keine Behinderung in den Bereichen Forschung und Entwicklung darstellen und ihre Innovationtätigkeit somit nicht beeinträchtigt wird. Überschiessende und im Geschäftsalltag nicht praktikable Regulierungen wirken sich innovationshemmend aus. Sie können der Wettbewerbsfähigkeit von unseren Unternehmen auf nationaler Stufe, vor allem aber auch im internationalen Umfeld, lediglich schaden. In Zeiten sich rasch entwickelnder technologischer Innovationen braucht es aus unserer Sicht zur Umsetzung wirksamer Datenschutzvorschriften keinen extensiven Sanktionskatalog, sondern vielmehr die Förderung eines effizienten Dialogs zwischen den staatlichen Institutionen und Datenbearbeitern.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)					
Name/Firma	**Gesetz**	**Art.**	**Abs.**	**Bst.**	**Bemerkung/Anregung**
	VE-DSG	Art. 3	Art. 3		Während im geltenden Gesetz Daten sowohl von natürlichen wie auch von juristischen Personen geschützt werden, sollen neu nur noch die Daten **natürlicher Personen** in den Anwendungsbereich des Datenschutzes fallen. Dadurch würde zwar auf den Schutz von Daten juristischer Personen verzichtet, dafür aber deren Bekanntgabe ins Ausland erleichtert, wo ein solcher Schutz bereits heute mehrheitlich nicht besteht. Mit der Aufgabe des Schweizer Sonderfalls würde der Datenverkehr mit Drittstaaten erleichtert. Gleichzeitig ist jedoch anzufügen, dass sowohl die Bundesverfassung in Art. 13 wie auch Art. 28 ZGB juristischen Personen Persönlichkeitsschutz gewährt. Offenbar liegt hier eine Inkonsequenz vor.
				lit.a	Es fehlt eine Definition der «Bestimmbarkeit». Somit wäre zu konkretisieren was unter «bestimmbaren Personendaten» zu verstehen ist. Zudem ist, wie im geltenden Recht, klarzustellen, dass mit dem Begriff «Daten» stets *Personen*daten gemeint sind.
				lit. c	Die Ausweitung des Begriffs der «besonders schützenswerten Personendaten» auf die entsprechenden Definitionen der genetischen und biometrischen Daten geht aus unserer Sicht zu weit. Der Wortlaut widerspricht den Erläuterungen im Bericht: Angedacht war die Erfassung von Daten, welche zum Zweck bearbeitet wer-den, eine natürliche Person eindeutig zu identifizieren.
				lit. f	Die Definition des Begriffs «Profiling» ist im VE-DSG breit gefasst. Damit geht der VE-DSG deutlich über die entsprechende Regelung der EU hinaus. Erfasst ist namentlich auch das «menschliche», d.h. manuelle Profiling, (z.B. eine schriftliche Mitarbeiterbeurteilung). Diese würde per se als Persönlichkeitsverletzung taxiert, wenn nicht vorgängig eine ausdrückliche Einwilligung eingeholt wird. Hier fordern wir eine Einschränkung der Definition dahingehend, dass Mitarbeiterbeurteilungen in Personaldossiers grundsätzlich nicht erfasst werden.
		4	5		Keine Nachführungspflicht Die permanente Nachführungspflicht geht zu weit und ist speziell für KMU's nicht praktikabel. Der 1. Satz von Art. 4 Abs. 5 VE-DSG ist entsprechend ersatzlos zu streichen
		5	1		Die neu vorgesehene Feststellung durch den Bundesrat, ob Daten im Ausland genügend geschützt sind, bedeutet eine unsachliche und unnötige Einschränkung. Diese Feststellung würde besser durch den Verantwortlichen, gestützt auf eigene Abklärungen und Kenntnisse, erfolgen. Die Bestimmung ist anzupassen.

		7	2		Auftragsdatenbearbeitung: Die vorgesehene Regelung (Versicherungspflicht) geht unseres Erachtens über die Bestimmungen des Obligationenrechts (Auftragsrecht gemäss OR 394ff) hinaus und sollte entsprechend angepasst werden. Die Bestimmung ist zu streichen.
			3		Die Anforderung einer «schriftlichen» Zustimmung ist vor dem Hintergrund der heutigen Geschäftsprozesse, dies insbesondere auch auf Grund der komplexen Dienstleistungsverhältnisse, nicht praxistauglich. Eine dokumentierte Zustimmung reicht aus; Schriftlichkeit i.S.v. Art. 13 OR ist nicht erforderlich. Es ist eine entsprechende Präzisierung vorzunehmen,.
		11			Bei dieser Regelung ist speziell an die KMU's zu denken. Der Bundesrat sollte beim Erlass der Bestimmungen zu den Mindestanforderungen eine praxistaugliche und kostenneutrale Lösung anstreben.
		13			Aus unserer Sicht erfordert die Umsetzung dieser Bestimmung administrativ für KMU's wiederum einen enormen Aufwand und schiesst klar am Ziel der Datensicherheit vorbei. Gerade KMU's, die die Buchhaltung und Personalabteilung oft ausgelagert haben, würden sich mit einem grossen administrativen Mehraufwand konfrontiert sehen.
		16			Das neu eingeführte Instrument der Datenschutz-Folgenabschätzung ist unseres Erachtens klar zu weit gefasst. Die offene und dadurch unklare Formulierung kann dazu führen, dass für praktisch alle Datenbearbeitungen vorgängig aufwändige Abklärungen durchgeführt werden müssten. Besonders problematisch ist die vorgesehene Sanktionierung bei Verstössen. Es ist eine Konkretisierung und Beschränkung auf Fälle vorzunehmen, bei denen ein hohes Risiko für eine Persönlichkeitsverletzung besteht.
		19		lit. a und lit. b	Diese allgemeine Dokumentationspflicht ist bezüglich Inhalt und Umfang unklar formuliert und analog der Verordnung zum DSG auf die Pflicht zur Erstellung «eines Verzeichnisses für regelmässige Datenbearbeitungen» einzuschränken. Die Pflicht, Datenschutzverstösse zu dokumentieren, ist zu weitgehend. Darüber hinaus erachten wir es als zwingend, auch eine Ausnahme der Pflicht für kleinere Unternehmen (z.B. analog der Sozialplanpflicht gemäss OR 335f, die erst ab 250 Mitarbeitenden zum Tragen kommt.) vorzusehen, sofern sie in Bezug auf den Datenschutz keine risikoreiche Tätigkeit ausüben. Aus

					systematischen Gründen sollte diese Bestimmung in Art. 11 VE-DSG (Sicherheit von Personendaten) integriert werden.
		20	1		Das Auskunftsrecht galt bisher nur für Daten in Datensammlungen (DSG 8); neu soll es nach dem Wortlaut für alle Daten, die ein Verantwortlicher bearbeitet, gelten. Dies könnte dazu führen, dass ein Arbeitnehmer in sämtliche Notizen, also auch solche, die nicht zum Personaldossier gehören, gestützt darauf Einsicht verlangen könnte. Deshalb lehnen wir diese Ausdehnung ab.
		50ff			Diese Strafbestimmungen sind unverhältnismässig hoch und sollten klar angepasst werden.
		57ff			Es fehlt eine umfassende Übergangsregelung. Die neuen und revidierten Bestimmungen werden die Prozesse der Unternehmen bedeutend beeinflussen. Es ist deshalb eine allgemeingültige Übergangsbestimmung von 2 Jahren aufzunehmen. Von einer Rückwirkung ist abzusehen.

Jean-Pierre Tappy
Head of External Affairs

Swiss International Air Lines AG
P.O. Box ZRHLX/DS/TAJE
CH-8058 Zürich-Flughafen
Tel. +41 44 564 22 28
Fax +41 44 564 20 21
jean-pierre.tappy@swiss.com

Frau Bundesrätin
Simonetta Sommaruga
Bundesrain 20
3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

Zürich-Flughafen, 3. April 2017

Stellungnahme Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Sehr geehrte Frau Bundesrätin

Wir danken für die Möglichkeit, zum Vorentwurf des Datenschutzgesetzes, nachfolgend VE DSG, sowie zu weiteren datenschutzrechtlichen Erlassen Stellung zu nehmen. Swiss International Air Lines AG nimmt diese Gelegenheit gerne wahr.

Wir erlauben uns, nachfolgend nur einige grundsätzliche Überlegungen und Anliegen aufzuführen. Für konkrete Anträge und Formulierungsvorschläge einzelner Bestimmungen verweisen wir Sie auf die Stellungnahme des Wirtschaftsdachverbands economiesuisse. SWISS war bei der Erarbeitung involviert, unsere Interessen und Anpassungswünsche sind deckungsgleich.

SWISS anerkennt die Bedeutung eines griffigen und effektiven Datenschutzgesetzes. In der heutigen Zeit der sich rasch entwickelnden Digitalisierung und der damit einhergehenden zunehmenden Bedeutung der Nutzung von Daten ist es essentiell, dass die Nutzenden dem Datenschutz vertrauen. Gleichzeitig ist es aber auch die Aufgabe des Gesetzgebers, eine vernünftige Balance zu wahren zwischen Schutz persönlicher Daten vor Missbrauch und der Sicherung von Potentialen zur wirtschaftlichen Nutzung von Daten. Wie in anderen regulatorischen Feldern auch soll der Grundsatz der Verhältnismässigkeit Massstab sein. Die Mittel-Zweck-Relation muss gewahrt bleiben. Überschiessende Regelungen oder Diskrepanzen zu international geltenden Datenschutzordnungen schaden der Wirtschaft und unterminieren damit nicht zuletzt auch die Effektivität des Datenschutzes an sich.

SWISS plädiert dafür, dass die künftigen Datenschutzbestimmungen im Schweizer Recht der Wirtschaft möglichst viel Flexibilität bieten, die Belastungen und administrativen Hürden gleichzeitig auf einem sehr tiefen Niveau gehalten werden. Das Geschäft einer Fluggesellschaft ist von Natur aus stark mit der Erhebung und Bearbeitung von Daten – nicht zuletzt im Auftrag staatlicher Behörden – verbunden. SWISS transportiert pro Jahr mehr als 16 Millionen Passagiere. Fliegen ist ein Massengeschäft in einem sehr internationalen Kontext, entsprechend gross sind die Datenmengen. Die Auflagen des Datenschutzes müssen so ausgestaltet sein, dass diese Datenbearbeitung weiterhin bewältigt werden kann. Überbordende Regulierungen wären äussert schädlich.

Wir lehnen zudem Bestimmungen ab, die im Sinne eines „Swiss Finish" bestehende Bestimmungen im internationalen Umfeld, namentlich im Vergleich zum EU-Recht, überschiessen. Als weltweit in einem Massengeschäft tätige Unternehmung sind Schweizer Spezialregelungen gleichzusetzen mit einer Reduktion der Wettbewerbsfähigkeit. Ist SWISS nicht mehr gewappnet, der starken Konkurrenz im Markt Paroli zu bieten, ist mittel- bis langfristig die Anbindung der Schweiz ans internationale Luftverkehrsnetz in der heutigen Form gefährdet.

Als nicht zielführend erachten wir schliesslich Bestimmungen im neuen Datenschutzgesetz, die der Strategie „Digitale Schweiz" des Bundesrates entgegenwirken und einzelne Entwicklungen gar bedrohen. SWISS würde es begrüssen, wenn die künftigen gesetzlichen Bestimmungen im Datenschutz auf dem Grundsatz aufbauen, dass die Nutzung von Daten an und für sich nicht illegitim, sondern geradezu notwendig für den digitalen Fortschritt ist und die Grundlage bildet, wirtschaftliche Potentiale im Interesse der Konsumierenden und Unternehmen auszuschöpfen. Gerade in der Aviatik ist die Individualisierung des Angebots für den Kunden ein wichtiger Trend. Hierfür werden unter Daten verwendet, die uns die Passagiere übermittelt haben. Das sollte in Zukunft ohne grosse administrative Hürden möglich sein, gerade auch unter Berücksichtigung der grossen Datenvolumina in unserem Geschäftsfeld. Dementsprechend greift die einseitige Fokussierung auf den Missbrauch und die Risiken zu kurz und erscheint als nicht sachgerecht.

Mit Blick auf den vorliegenden Vorentwurf sind es namentlich zwei Themenblöcke, die wir als sehr problematisch erachten:

- Einerseits überschiessen die zahlreich vorgesehenen Informations- und Meldepflichten. Sie verursachen für die Unternehmen unverhältnismässig hohe administrative Aufwände. Nicht zu unterschätzen ist die Informationsflut, die dadurch unnötigerweise generiert wird. Dezidiert lehnen wir die damit verbundene Offenlegung von Geschäftsgeheimnissen sowie die Pflicht, sich selber zu belasten ab. SWISS würde es begrüssen, wenn die entsprechenden Regelungen, die wir in der Summe als schädlich für die Wettbewerbsfähigkeit der Schweizer Wirtschaft erachten, nicht aufgenommen oder zumindest auf ein absolutes Minimum reduziert werden.
- Andererseits ist das vorgesehene Sanktionssystem nicht verhältnismässig. SWISS erachtet es als nicht zielführend, strafrechtliche Sanktionen im vorgeschlagenen Ausmass im Gesetz aufzunehmen. Das Sanktionssystem muss auch im Datenschutz auf rechtsstaatlichen Grundsätzen, namentlich auch der Verhältnismässigkeit fussen.

Wie erwähnt können Sie die konkreten Formulierungen und Änderungsbegehren der Stellungnahme von economiesuisse entnehmen. SWISS bedauert, dass der Vorentwurf in diversen Teilen die oben skizzierten Grundsätze nicht oder nicht ausreichend berücksichtigt.

Wir danken für die wohlwollende Prüfung unserer Anliegen und Ihre Kenntnisnahme.

Freundliche Grüsse
Swiss International Air Lines Ltd.

Jean-Pierre Tappy
Captain, Senior Director
Head of External Affairs

i.V.
Tobias Günzel
Compliance Counsel, Senior Manager
Betrieblicher Datenschutzverantwortlicher

Kopie an:
- Marcel Zuckschwerdt, stellvertretender Direktor, Bundesamt für Zivilluftfahrt BAZL, 3003 Bern

swisscom

Swisscom AG, Group Strategy - Data Governance,
Alte Tiefenaustrasse 6, 3050 Bern

Eidgenössiches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per E-Mail an Herrn Jonas Amstutz: jonas.amstutz@bj.admin.ch

Datum	03.04.2017	**Seite**
Ihr Kontakt	Séverine Knüsli / 058-223 84 39 / severine.knuesli@swisscom.com	1 von 2
Thema	**Vernehmlassung zur Revision DSG**	

Sehr geehrte Frau Bundesrätin Sommaruga

Wir nehmen Bezug auf die Vernehmlassung zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz und bedanken uns für die Gelegenheit zur Stellungnahme:

Swisscom sieht in der Revision des Datenschutzgesetzes im Zeitalter der Digitalisierung die Chance ein praxisnahes griffiges und modernes Datenschutzgesetz für die Schweiz zu schaffen.

Swisscom ist es daher ein Anliegen, dass die Revision des Datenschutzgesetzes in die vom Bundesrat lancierte Dachstrategie *digitale Schweiz* eingebunden wird. Mit dieser Strategie soll die Schweiz mehr und besser von der zunehmenden Digitalisierung profitieren und sich als innovative Volkswirtschaft noch dynamischer entwickeln. Dies bedingt eine kohärente und zukunftsorientierte Datenpolitik.

Mit der aktuellen Revision soll deshalb sowohl die Sicherstellung des Persönlichkeitsschutzes der betroffenen natürlichen Personen als auch die Schaffung und Förderung moderner Rahmenbedingungen für den Wirtschaftsstandort Schweiz im Zeitalter der Digitalisierung vereint werden.

Dies soll vor allem durch die konsequente Verfolgung des risikobasierten Ansatzes erreicht werden, wonach sich umzusetzende Massnahmen nach der Höhe des Risikos zu orientieren haben. Damit kann ein unverhältnismässiger Aufwand auf Seite der Unternehmen und eine undifferenzierte Informationsflut bei den betroffenen Personen vermieden werden.

In dieselbe Richtung geht es im Zusammenhang mit den ausgebauten Dokumentations-, Informations- und Meldepflichten, welche zwingend verhältnismässig sein müssen, damit es nicht zu einer Lähmung der Unternehmenstätigkeit kommt oder zu einem Nachteil des Wirtschaftsstandorts Schweiz führt.

Einer Verschärfung des Sanktionsregimes steht Swisscom kritisch gegenüber, insbesondere der Pönalisierung der Mitarbeitenden.

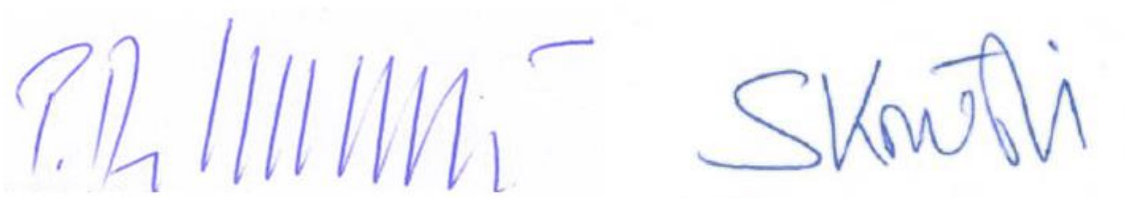
Gleichzeitig ist den regulatorischen Entwicklungen auf Ebene des Europarates und der Europäischen Union (EU) im Datenschutz Rechnung zu tragen. Die Schweiz hat im internationalen Vergleich ein angemessenes Datenschutzniveau zu gewährleisten.

Ein sogenannter "Swiss Finish", welcher über die Vorgaben des Europarates und der EU zielt und zu Lasten der Schweizer Wirtschaft geht, lehnt Swisscom ab.

Für die wohlwollende Prüfung und Berücksichtigung der Anliegen von Swisscom bedanken wir uns im Voraus bestens. Als Beilage finden Sie die Stellungnahme der Swisscom, in welcher wir auf die uns wichtigsten Themenbereiche eingehen. Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüssen

Swisscom (Schweiz) AG
Konzernrechtsdienst & Group Strategy-Data Governance



Patrick Dehmer
General Counsel

Séverine Knüsli
Corporate Legal Counsel

Bailage: Stellungnahme Swisscom

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Swisscom (Schweiz) AG

Abkürzung der Firma / Organisation : Swisscom

Adresse : Alte Tiefenaustrasse 6, 3050 Bern

Kontaktperson : (Frau) Séverine Knüsli

Telefon : 058 223 84 39

E-Mail : severine.knuesli@swisscom.com

Datum : 03.04.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte als Word-Dokument bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen	
Name/Firma	Bemerkung/Anregung
Swisscom	In der Digitalisierung unseres Alltags bilden Daten eine wesentliche Grundlage zur Steigerung des Nutzens eines oder einer jeden sowie zur Entwicklung von innovativen Geschäftsmodellen, Dienstleistungen und Anwendungen. Ihre Bedeutung nimmt mit fortschreitender Digitalisierung stetig zu. Dies hat auch der Bundesrat erkannt und mit der Lancierung seiner Dachstrategie *digitale Schweiz* eine Strategie präsentiert, mit welcher die Schweiz mehr von der zunehmenden Digitalisierung profitieren und sich als innovative Volkswirtschaft noch dynamischer entwickeln soll (Medienmitteilung des Bundesrates vom 20.4.2016: Strategie des Bundesrates für eine digitale Schweiz). Die Wirtschaft soll sich im digitalen Raum möglichst frei entfalten können. Gleichzeitig hält der Bundesrat fest, dass für eine informierte und demokratische Gesellschaft und zur Sicherung der Wohlfahrt, die von der Datenbearbeitung betroffenen Personen die modernen Informations- und Kommunikationstechnologien in ihrem täglichen Leben kompetent und sicher nutzen können sollten. Dies bedingt jedoch eine kohärente und zukunftsorientierte Datenpolitik (Medienmitteilung des Bundesrates vom 22.3.2017: Auf dem Weg zu einer Datenpolitik des Bundes). In diesem Zusammenhang ist daher auch die vorliegende Revision zu sehen, welche sowohl die Sicherstellung des Persönlichkeitsschutzes der betroffenen natürlichen Personen als auch die Schaffung moderner Rahmenbedingungen für den Wirtschaftsstandort Schweiz im Zeitalter der Digitalisierung vereinen muss. Weiter hat sie den regulatorischen Entwicklungen im Datenschutz auf Ebene des Europarates und der Europäischen Union (EU) Rechnung zu tragen. Die Schweiz muss im internationalen Vergleich ein angemessenes Datenschutzniveau gewährleisten können. Gleichzeitig muss die Vorlage die Balance zwischen dem Schutz des Privaten und Massnahmen zur Förderung des Wirtschaftsstandortes Schweiz finden. Ein sogenannter "Swiss Finish" – ein Datenschutz, der über die Forderungen des Europarates und der EU hinausgeht – geht eindeutig zu Lasten der Wirtschaft und ist abzulehnen. Insbesondere dürfen keine Bestimmungen eingeführt werden, welche zusätzliche Hürden vorsehen und die Geschäftstätigkeit unnötig erschweren ohne einen effektiven Nutzen für die betroffenen Personen zu generieren.
Swisscom	Swisscom anerkennt den Revisionsbedarf des Datenschutzgesetzes (VE-DSG) im Zeitalter der Digitalisierung und sieht darin die Chance, ein praxisnahes griffiges und modernes Datenschutzgesetz für die Schweiz zu schaffen. Vor diesem Hintergrund sind folgende Punkte für Swisscom in dieser Vorlage von zentraler Bedeutung: • Brücke schlagen zwischen Sicherstellung Persönlichkeitsschutz der betroffenen Personen und Schaffung moderner Rahmenbedingungen für den Wirtschaftsstandort Schweiz bei der Bearbeitung von Daten: ▪ effektiver Nutzen und Schutz für die betroffenen Personen; ▪ praktikabler und verhältnismässiger Aufwand für die Unternehmen.

	• Ablehnung einer Verschärfung gegenüber den Vorgaben des Europarates und der EU (sog. "Swiss Finish") zu Lasten der Innovation und ohne effektiven Nutzen für die betroffenen Personen. • Konsequente Verfolgung des risikobasierten Ansatzes, wonach umzusetzende Massnahmen sich nach der Höhe des Risikos zu orientieren haben, damit ein unverhältnismässiger Aufwand auf Seite der Unternehmen und eine undifferenzierte Informationsflut bei den betroffenen Personen vermieden wird. • Verhältnismässiger Ausbau der Dokumentations-, Informations- und Meldepflichten, damit es nicht zu einer Lähmung der Unternehmenstätigkeit kommt oder zu einem Nachteil des Wirtschaftsstandorts Schweiz führt. • Sanktionen basierend auf Straftatbeständen mit unklar umschriebenen Begriffen sind abzulehnen. Kritisch zu hinterfragen ist die massive Verschärfung des Sanktionsregimes, welches zu einer Pönalisierung der Mitarbeitenden führt. Dies ist unnötig und nicht zielführend.
Swisscom	Im Rahmen ihrer Stellungnahme führt Swisscom diejenigen Artikel und Bereiche ausführlicher aus, welche für Swisscom aufgrund ihrer Tragweite von Bedeutung sind. Bei Artikeln und Bereichen, welche für Swisscom ebenfalls erwähnenswert, aber von kleinerer Tragweite sind, verweist Swisscom auf die Stellungnahme ausgewählter Verbände.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)					
Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Swisscom	DSG	Allgemeiner Hinweis			Der Vorentwurf verwendet eine Vielzahl verschiedener Begriffe, die ungenügend definiert und / oder ungenügend von anderen Begriffen abgegrenzt oder nicht kohärent verwendet werden (beispielsweise der Begriff der Daten vs. Personendaten, Dritte vs. Empfängerin und Empfänger). Es wäre wünschenswert, wenn dies entsprechend korrigiert wird, um Fehlinterpretationen bei der Anwendung und Auslegung des revidierten Gesetzes zu vermeiden. Verwiesen wird hierzu ergänzend auf die Stellungnahme des VUD zu Art. 3 VE-DSG.
Swisscom	DSG	2			Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	3		f	Swisscom befürwortet eine Angleichung der Formulierung des Begriffs Profiling an die Terminologie der "*Verordnung 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten"* (EU-DSGVO), welche nur die automatisierte Datenverarbeitung von Personendaten erfasst. Es soll nur das personenbezogene Resultat als Profiling qualifiziert werden und nicht jeder Vorgang. Aus dem Wortlaut des VE-DSG geht diese Abgrenzung nicht hervor. Die Auswertung von Personendaten, die nicht der Analyse des Verhaltens einzelner Personen dienen, sondern beispielsweise zur Vorhersage von allgemeinen nicht-personenbezogenen Entwicklungen (z.B. im Bereich von Mobilität), sollte nicht dem strengeren Regime des Profilings unterstellt werden. Das vorgeschlagene Konzept zum "Profiling" stellt einen "Swiss Finish" dar und führt auf Seite der Unternehmen zu einem unverhältnismässigen Aufwand. Zudem hemmt er jegliche Möglichkeit zur Erschliessung neuer innovativer Geschäftsfelder und die Entwicklung von Produkten. ***Aus den genannten Gründen stellt Swisscom den Antrag, Art. 3 Abs. 1 Bst. f VE-DSG wie folgt anzupassen*:**

					Profiling: Automatisierte ~~jede~~ Auswertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale zu analysieren oder personenspezifische Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität und aufgrund dieser Analyse oder Vorhersage eine Person zu bewerten.
Swisscom	DSG	4	5		Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	4	6		Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	5			Gestützt auf den Wortlaut des VE-DSG wird es für ein Unternehmen grundsätzlich nicht schwieriger werden, Daten ins Ausland zu übermitteln. Aufgrund neuer Notifikations- und Genehmigungspflichten gestaltet sich das Verfahren aber wesentlich komplizierter, langwieriger und es drohen zudem neu auch empfindliche Sanktionen bei Verstössen. Neu ist ebenfalls, dass auch der Auftragsbearbeiter der Informations- bzw. Genehmigungspflicht unterworfen ist. Swisscom steht diesen Regelungen kritisch gegenüber:
Swisscom	DSG	5	1		Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	5	3	b-d	Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	5	5		Die unterschiedliche Handhabung der spezifischen resp. standardisierten Garantien ist nicht nachvollziehbar. Eine Information gemäss Abs. 3 lit. b sollte ausreichen. Die Frist zur Genehmigung ist mit einem halben Jahr zu lange angesetzt (bisher musste die Prüfung selbst von BCR innert 30 Tagen durchgeführt sein). Hinzu kommt, dass die tatsächliche Frist sehr viel länger sein kann. Der

					Beauftragte kann sich jederzeit auf den Standpunkt stellen, er habe noch nicht alle erforderlichen Informationen. ***Aus den genannten Gründen stellt Swisscom den Antrag, Art. 5 Abs. 5 VE-DSG zu streichen. Eventualiter sei die Mitteilungsfrist auf 30 Tage zu reduzieren.***
Swisscom	DSG	5	6		Abs. 6 ist zu streichen. Der Beauftragte wurde bereits vorgängig informiert resp. musste die Genehmigung bereits erteilen. Diese zusätzliche administrative Hürde ist unnötig und stellt einen überflüssigen "Swiss Finish" dar.
Swisscom	DSG	5	7		Abs. 7 ist dahingehend zu ergänzen, dass der Bundesrat diese Liste regelmässig aktualisieren muss, da diese neu verbindlichen Charakter für die Unternehmen hat und sich diese darauf verlassen können müssen.
Swisscom	DSG	6	1	b	Abs. 1 lit. b auferlegt der Schweiz strengere Vorschriften als die in der EU-DSGVO genannten. Die EU-DSGVO erlaubt auch die Bekanntgabe, wenn ein Vertrag lediglich im Interesse der betroffenen Person abgeschlossen worden ist und nicht nur, wenn es sich um Daten der Vertragspartner handelt. Diese Regelung muss übernommen werden.
Swisscom	DSG	6	1	c 2	Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	6	2		Diese Pflicht ist neu und bedeutet eine administrative Bürde für alle Unternehmen. Auch wird der Beauftragte mit solchen Informationen überhäuft werden. Zudem ist diese Pflicht dem EU Recht fremd und somit ein "Swiss Finish". Diese Bestimmung zwingt Unternehmen faktisch, dem Beauftragten sensible Geschäftsgeheimnisse wie etwa laufende ausländische Untersuchungen und Gerichtsverfahren offenzulegen, wofür es keinen sachlichen Grund gibt.

					Besonders kritisch sieht Swisscom auch die mögliche Einsicht von Dritten im Rahmen des BGÖ. ***Aus den genannten Gründen stellt Swisscom den Antrag, Art. 5 Abs. 6 VE DSG zu streichen.***
Swisscom	DSG	7	3		Gemäss Art. 7 Abs. 3 VE-DSG soll eine Weiterübertragung der Auftragsbearbeitung ("Sub-Processing") künftig nur noch mit vorgängiger schriftlicher Zustimmung des Verantwortlichen möglich sein. Die schematische Bindung des Sub-Processing an die vorgängige schriftliche Zustimmung des Verantwortlichen wäre in der Praxis hinsichtlich bestehender Auftragsbearbeitungen nur mit grösstem Aufwand umsetzbar. Zudem ist nicht nachvollziehbar, wieso dem Verantwortlichen ein (grundloses) Einspruchsrecht eingeräumt wird. Es handelt sich hier um einen unverhältnismässigen Eingriff in die Vertrags- und Wirtschaftsfreiheit. Es steht den Parteien frei, vertraglich weitergehende Einschränkungen festzulegen. Der Artikel ist weiter auch sonst systemfremd. Die Auftragsbearbeitung als solche ist unter den Voraussetzungen von Art. 7 Abs. 1 und 2 VE-DSG durch die betroffenen Personen ohne weitere Genehmigung zulässig. Warum die Subauftragsbearbeitung einer strengeren Regelung unterstellt werden soll, ist nicht ersichtlich. Richtigerweise sollten Art. 7 Abs. 1 und 2 VE-DSG für weitere Unterauftragsbearbeiter gleichermassen gelten. ***Aus den genannten Gründen stellt Swisscom den Antrag, Art. 7 Abs. 3 VE DSG wie folgt zu formulieren:*** *"Der Auftragsbearbeiter darf die Bearbeitung einem anderen Auftragsbearbeiter übertragen, wenn die obenstehenden Absätze auch in Bezug auf die Unterbeauftragung eingehalten werden. Der Auftragsbearbeiter hat in einem solchen Fall den Verantwortlichen über die Unterauftragsbearbeitung vorgängig zu informieren. Der Verantwortliche hat das Recht, der Unterauftragsbearbeitung zu widersprechen, wenn objektiv*

					begründete Anzeichen bestehen, dass die Einhaltung der obenstehenden Absätze nicht mehr gewährleistet ist." Im Übrigen verweisen wir auf die Stellungnahme der ICT SWITZERLAND zu diesem Artikel.
Swisscom	DSG	8-9			Das Instrument der Empfehlung der guten Praxis wird von Swisscom grundsätzlich begrüsst. Die Umsetzung ist hingegen noch sehr vage und lässt zu viel Spielraum offen, insbesondere in Bezug auf den Rechtsschutz, welche folgende Überlegungen nahelegt: • Befristung der Empfehlungen der guten Praxis; • Überarbeitungsmöglichkeiten; • gerichtliche Überprüfung. Im Weiteren verweist Swisscom hierzu auf die Stellungnahme der asut.
Swisscom	DSG	12			Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	13			Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	13	4		Wir verweisen hierzu auf die Stellungnahme der asut und ICT SWITZERLAND.
Swisscom	DSG	15	1		Wir verweisen hierzu auf die Stellungnahme des VUD
Swisscom	DSG	15	2		Wir verweisen hierzu auf die Stellungnahme des ICT SWITZERLAND.
Swisscom	DSG	16			Swisscom steht der Massnahme in Bezug auf die zeitliche Dimension kritisch gegenüber, da sie die verwaltungsinternen Prozesse für die Wirtschaft erschweren. Für den Erfolg eines neuen Produktes oder Dienstleistung ist eine rasche Lancierung entscheidend. Mit dem vorgesehenen Prozess

					besteht die Gefahr, dass die neue Prüfungskompetenz des Beauftragten die Innovation im Markt hemmt. Besonders kritisch sieht Swisscom auch die mögliche Einsicht von Dritten im Rahmen des BGÖ. Weiter ist Swisscom der Auffassung, dass der Auftragsbearbeiter von dieser Pflicht der Folgeabschätzung auszunehmen ist. Die Nennung des Auftragsbearbeiters ist abzulehnen, da dieser oftmals keine Kontrolle über die Erhebung der Personendaten hat, aber sanktioniert werden kann. Schliesslich ist der Risiko-Begriff zu schärfen. Der VE-DSG sieht vor, dass eine Datenbearbeitung bereits bei einer Erhöhung des Risikos dem Beauftragten zur Genehmigung unterbreitet werden muss. Theoretisch trifft das auf jede Datenbearbeitung zu, ausser man verzichtet gänzlich darauf. Es muss davon ausgegangen werden, dass die Unternehmen zur Vermeidung von Sanktionsrisiken dem Beauftragten jedes Datenschutz-Folgenabschätzungs-Ergebnis zur Genehmigung unterbreitet werden. Dies würde sowohl bei den Unternehmen als auch beim Beauftragten zu einem kaum rechtfertigbaren Aufwand führen. Aus dem Blickwinkel der Verhältnismässigkeit wäre zu begrüssen, wenn eine Mitteilung der Ergebnisse und insbesondere der zu ergreifenden Massnahmen nur bei einem tatsächlich hohen Risiko für die Persönlichkeit der betroffenen Personen erfolgen muss. ***Aus den genannten Gründen stellt Swisscom den Antrag, Art. 16 VE DSG wie folgt anzupassen*:** 1 *Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen ~~erhöhten~~ Risiko für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen.* *2 Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit ~~oder die Grundrechte~~ der*

					betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit ~~oder der Grundrechte~~ der betroffenen Person zu verringern. 3 *streichen*. 4 *streichen.*
Swisscom	DSG	17			Wir verweisen hierzu auf die Stellungnahme des VUD.
Swisscom	DSG	19			Wir verweisen hierzu auf die Stellungnahme der asut und des VUD.
Swisscom	DSG	20	1		Wir verweisen hierzu auf die Stellungnahmen der asut und der ICT SWITZERLAND.
Swisscom	DSG	20	3		Wir verweisen hierzu auf die Stellungnahmen der ICT SWITZERLAND.
Swisscom	DSG	23	2	d	Die generelle Anforderung zur ausdrücklichen Einwilligung für ein Profiling, unabhängig von der Form oder der Art des Profiling und des Zwecks, gehen zu weit. Im Sinne des risikobasierten Ansatzes und damit zu Gunsten eines effektiven und verhältnismässigen Datenschutzes, sollte auch das Profiling einer Interessenabwägung zugänglich sein und nicht generell unter die Voraussetzung einer ausdrücklichen Einwilligung gestellt werden. Die Risiken des Profillings konkretisieren sich nicht bereits schon durch die Auswertung von Daten selbst, sondern durch den Zweck, der damit verfolgt wird. Es ist ein Unterschied, ob eine Bearbeitung von Daten zum Zweck statistischer Vorhersagen erfolgt oder ob sie eine konkrete rechtliche oder diskriminierende Wirkung entfalteten kann. Letzteres ist etwa dann der Fall, wenn Analysen oder Prognosen zu persönlichen Aspekten wie Arbeitsleistung, Gesundheit, Verhalten oder Weltanschauung als Grundlage für Entscheidungen gegen den Einzelnen erfolgen.

					Lit. d ist daher ersatzlos zu streichen. Dieser Einschub stellt ein "Swiss Finish" dar, welcher insbesondere im Hinblick auf den Umfang der damit verstandenen Definition des Begriffs Profiling stossend ist. ***Aus den genannten Gründen stellt Swisscom den Antrag, Art. 23 Abs. 2 lit. d VE DSG zu streichen.***
Swisscom	DSG	23	3		Wir verweisen hierzu auf die Stellungnahmen der asut.
Swisscom	DSG	Allgemeiner Hinweis Kompetenzen Beauftragter			Die Stärkung der Stellung des Beauftragten scheint aus Sicht Swisscom im Hinblick auf die Vorgaben des Europarates grundsätzlich gerechtfertigt. Swisscom befürchtet jedoch, dass durch die Verbindung der ausgebauten Kompetenzen des Beauftragten und der neu eingeführten Meldepflichten, welche mit einer Genehmigungspflicht durch den Beauftragten verbunden sind (zum Teil mit Fristen bis zu 6 Monaten) insbesondere die Umsetzung von Projekten, Transaktionen mit dem Ausland und die Entwicklung von neuen Geschäftsmodellen unverhältnismässig hinausgezögert, wenn nicht verunmöglicht, wird. Dies führt zwangsweise zu einer Lähmung der Unternehmenstätigkeit und zu einem Nachteil des Wirtschaftsstandorts Schweiz. Verschärft wird diese Situation beim Erhalt eines negativen Entscheides (Verfügung), welcher dann vom betroffenen Unternehmen nötigenfalls vor Bundesverwaltungsgericht angefochten und korrigiert werden muss. In diesem Zusammenhang ist ebenfalls auf die bisherige, gut funktionierende Kooperation bei Projekten zwischen den Unternehmen und dem Beauftragten hinzuweisen. Im Rahmen der Gesetzesrevision sollen Anreize geschaffen werden, welche das freiwillige proaktive Verhalten der Unternehmen fördert und honoriert; nicht nur im Rahmen der Datenschutz-Folgenabschätzung, aber auch bei Meldungen von Datenschutzverletzungen.

Swisscom	DSG	41	3		Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	44	3		Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	45			Wir verweisen hierzu auf die Stellungnahme der asut.
Swisscom	DSG	50-55			Eine moderate Erhöhung der Sanktionen erscheint im Hinblick auf die Vorgaben des Entwurfs zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (E-SEV 108) gerechtfertigt und vertretbar. Der vorgeschlagene Strafrahmen und der erweiterte Sanktionskatalog gehen jedoch zu weit. Neu werden faktisch alle Verpflichtungen des Datenbearbeiters mit Sanktionen bewehrt und zwar ebenfalls bei fahrlässiger Missachtung. Dieser Paradigmenwechsel stellt einen unerwünschten "Swiss Finish" dar. E-SEV 108 fordert einzig "geeignete" Sanktionen. Mit einer moderaten Verschärfung des Sanktionssystems wird dieser Anforderung entsprochen, zumal der Beauftragte neu umfassende Untersuchungs- und Verfügungskompetenzen erhält. Art. 50 ff. VE-DSG enthalten Strafbestimmungen gegen natürliche Personen. Dies steht im Gegensatz zu den entsprechenden europäischen Regelungen, die primär Sanktionen gegen Unternehmen vorsehen. Die EU-DSGVO verlangt zudem nur ein der Sache nach gleichwertiges Datenschutzniveau und zwar unabhängig des Sanktionsregimes. Im Bereich der Aufsicht bzw. der Durchsetzung bleibt daher ein nicht unbeträchtlicher Handlungsspielraum, der eine wortwörtliche Übernahme der EU-DSGVO nicht erforderlich macht (vgl. Art. 83 Abs. 9 EU-DSGVO sowie Erwägung 151 EU-DSGV). Weiter gilt zu bedenken, dass in anderen Gesetzen wie dem Bundesgesetz gegen den unlauteren Wettbewerb (UWG, SR 241) oder dem Bundesgesetz über den Schutz von Marken und Herkunftsangaben (MSchG, SR 232.11)

					sowie dem Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen (KG, SR 251) Strafen für natürliche Personen von maximal 100'000 CHF vorgesehen sind. Das im VE-DSG vorgeschlagene Strafmass ist im Verhältnis zur Schwere der Pflichtverletzung im Vergleich ungerechtfertigt. Swisscom erachtet es als kritisch, dass der VE-DSG auf die Pönalisierung natürlicher Personen abzielt, namentlich Mitarbeitende der Unternehmen, welche im Rahmen ihrer alltäglichen Arbeitstätigkeit Daten bearbeiten und nun bei organisatorischen Mängeln des Unternehmens mit hohen Bussen rechnen müssen. Dies wird zu übervorsichtigem Handeln seitens der Mitarbeitenden und somit zu einer Lähmung der Unternehmenstätigkeit führen. Andererseits sieht sich ein Unternehmen mit der Schwierigkeit konfrontiert, dass eine Vielzahl seiner Pflichten zur Einhaltung des Datenschutzes im VE-DSG auf unbestimmten Begriffen basiert. Diese Ausgestaltung des Sanktionsregimes kann sicherlich so nicht gewollt sein. Vor diesem Hintergrund ist die Unbestimmtheit einer Vielzahl der (Straf-)Tatbestände gem. Art. 50 f. VE-DSG äusserst bedenklich. Aus dem Prinzip "Verbot unbestimmter Strafbestimmungen" (nulla poena sine lege certa) wird zudem abgeleitet, dass eine Bestimmung hinreichend klar und bestimmt ausgestaltet sein muss. Hierzu muss die Bestimmung so präzise formuliert sein, dass die betreffende Person ihr Verhalten danach ausrichten und die Folgen eines bestimmten Verhaltens erkennen kann. Viele der Pflichten des VE-DSG und damit auch die daraus abgeleiteten Straftatbestände sind viel zu offen formuliert, so dass es für die private Person schwierig sein wird zu verstehen, was sie genau tun darf und was nicht. Veranschaulicht werden kann dies an der Pflicht zu Privacy by Design (Art. 18 Abs. 1 VE-DSG), welche vorsieht, dass sowohl der Verantwortliche als auch der Auftragsbearbeiter ab dem Zeitpunkt der Planung der Datenverarbeitung Massnahmen zur Verbeugung von Persönlichkeitsverletzungen vorsehen muss. Dasselbe gilt für die

					Dokumentationspflicht, welche in Art. 19 Abs. 1 lit. a VE-DSG nur festhält, dass sowohl der Verantwortliche als auch der Auftragsbearbeiter die Datenbearbeitung zu dokumentieren haben. Auf Grund der entsprechenden Unbestimmtheit (vgl. ebenfalls Art. 16 Abs. 1 VE-DSG: "…vorgesehene Datenbearbeitung [führt] voraussichtlich zu einem *erhöhten* Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person") ist offensichtlich, dass die Anforderungen an die genügende Bestimmtheit sowie der hinreichenden Voraussehbarkeit einer Norm nicht erfüllt sind bzw. eine Strafbarkeit unter diesen Umständen rechtsstaatlich bedenklich wäre. Der Fokus die natürlichen Personen zu pönalisieren, zusammen mit der grossen Unbestimmtheit der Straftatbestände, führt somit zu einer nicht zu rechtfertigenden Bedrohung derjenigen Personen, die mit Personendaten umzugehen haben – und zwar gerade derjenigen Personen, die unternehmensintern die Einhaltung des Datenschutzes sicherstellen müssen und die durch das Datenschutzrecht deshalb zu schützen sind. Dies ist auch deshalb problematisch, weil Datenschutzverstösse viel eher in der unternehmensweiten Komplexität datenschutzrechtlicher Setups begründet sind (z.B. grenzüberschreitende Sachverhalte, zunehmender Trend zu Arbeitsteiligkeit, etc.) und nicht in einem individuellen Verschulden. Einzelne Personen zu bestrafen, wäre daher nicht sachgerecht. Die Sanktionierung fahrlässiger Begehung ist unter diesem Gesichtspunkt strikt abzulehnen. Bezugnehmend auf die vorgenannten Ausführungen betrachtet Swisscom die Ausgestaltung der Strafbestimmungen als einen überschiessenden "Swiss Finish", welche zudem verfassungsrechtlich nicht unbedenklich sind und somit massive Auswirkungen auf den Wirtschaftsstandort Schweiz hätten.
Swisscom	DSG	59			Die Übergangsbestimmungen sind eher rudimentär und würden in dieser Form Raum lassen für unechte Rückwirkungen, welche enorme Aufwände für die Wirtschaft mit sich bringen würden. Bei bisherigen

					Datenbearbeitungen, welche unter neuem Recht fortgesetzt werden, sollen deshalb unechte Rückwirkungen zumindest teilweise explizit eingeschränkt werden. Es gilt daher Folgendes zu beachten: • Wurde für eine Datenbearbeitung die Informationspflicht des bisherigen Rechts erfüllt, ist bei Fortsetzung dieser Datenbearbeitung nach Inkrafttreten des neuen Gesetzes auch dann keine neuerliche Information notwendig, wenn das neue Gesetz strengere Anforderungen an die Informationspflicht stellt • Liegt für eine Datenbearbeitung nach bisherigem Recht eine gültige Einwilligung vor, muss bei Fortsetzung dieser Datenbearbeitung nach Inkrafttreten des neuen Gesetzes auch dann keine neuerliche Einwilligung eingeholt werden, wenn das neuen Gesetz weitergehende Anforderungen an die Einwilligung stellt. • Bei Datenbearbeitungen, welche vor Inkrafttreten des neuen Gesetzes begonnen haben, muss über die in Art. 20 VE-DSG zusätzlich vorgesehenen Datentypen nur soweit Auskunft erteilt werden, als diese Daten beim Auskunftspflichtigen vorhanden sind.

Amstutz Jonas BJ

Von: Swissfundraising | Roger Tinner <roger.tinner@swissfundraising.org>
Gesendet: Montag, 3. April 2017 14:35
An: Amstutz Jonas BJ
Cc: Odilo Noti
Betreff: Vernehmlassung zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz
Anlagen: Vernehmlassung_VE DSG_Swissfundraising_v 1.0_31032017.doc

Sehr geehrter Herr Amstutz

Fristgerecht stellen wir Ihnen hier die Vernehmlassung unseres Verbandes zum genannten Gesetz (Vorentwurf) zu. Swissfundraising ist der Berufsverband der Fundraiserinnen und Fundraiser in Spendenorganisationen und Non-Profit-Organisationen (NPO) der Schweiz und umfasst über 650 Mitglieder. Bitte bestätigen Sie uns den Eingang unserer Eingabe. Wir danken im Voraus für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse
SWISSFUNDRAISING
Dr. Odilo Noti Präsident
Roger Tinner Geschäftsführer

--

swissfundraising

Swissfundraising
Rosenbergstrasse 85, Postfach 20, 9001 St.Gallen
Telefon 071 777 2011, Fax 071 377 2011
roger.tinner@swissfundraising.org

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Swissfundraising

Abkürzung der Firma / Organisation : Swissfundraising

Adresse : Rosenbergstrasse 85, 9001 St. Gallen

Kontaktperson : Roger Tinner, Geschäftsführer

Telefon : +41 71 777 20 11

E-Mail : info@swissfundraising.org

Datum : 31. 03. 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Swissfundraising	Wir begrüssen die angestrebte Modernisierung des Datenschutzrechts. Für die Geschäftsaktivitäten der Mitglieder unseres Verbandes ist zwar der grenzüberschreitende Austausch von Personendaten weniger elementar, wir sehen jedoch, dass diese Frage für die Gesamtwirtschaft von Bedeutung ist. Indirekt ist dieser Austausch auch für unsere Mitglieder bedeutsam, da wir auf Adressdaten aus unterschiedlichen Quellen zugreifen müssen. Wir begrüssen daher, dass mit der Revision des Datenschutzgesetzes dieser grenzüberschreitende Austausch sichergestellt werden kann. Für unsere Mitglieder, bei denen es sich um Fundraiserinnen und Fundraisier in Spendenorganisationen und Non-Profit-Organisationen (NPO) unterschiedlicher Art handelt, ist das Vertrauen der betroffenen Personen in die Datenbearbeitungen von eminenter Bedeutung. Gleichzeitig ist für die Geschäftsaktivität unserer Mitglieder eine hohe Rechtssicherheit im Umgang mit Personendaten entscheidend. Unsere Mitglieder müssen rechtssicher wissen, was von ihnen bei der Bearbeitung von Personendaten verlangt wird und welche Bearbeitungen zulässig oder problematisch sind. Diese Rechtssicherheit wird durch die vorgeschlagenen Bestimmungen leider nicht erwirkt. Wir möchten hiermit betonen, dass Datenbearbeitungen und der Zugang zu möglichst vielen Daten für die Geschäftsmodelle unserer Mitglieder von erheblicher Bedeutung sind. Personendaten und der Zugang zu diesen ist der Sauerstoff für die Tätigkeiten unserer Mitglieder. An den Geschäftsaktivitäten und damit auch Datenbearbeitungen durch unsere Mitglieder besteht ein berechtigtes (öffentliches) Interesse. Unsere Mitglieder nehmen wichtige öffentliche Aufgaben wahr – in der Schweiz und im Ausland. Unverhältnismässige bzw. überschiessende Vorschriften betreffend die Datenbearbeitung können unsere Mitglieder bei deren Aufgabenerfüllung beeinträchtigen. Eine Beeinträchtigung findet nicht nur dann statt, wenn die Datenbeschaffung und -bearbeitung durch die Mitglieder selbst erschwert werden, sondern auch dann, wenn die Datenbeschaffungen und -weitergaben durch die teilweise externen Datenlieferanten eingeschränkt wird. Wird z.B. die Selektion von passenden Adressdaten erschwert, führt dies zu einer weniger effizienten Spendenkampagne. Die zielgerichtete und fokussierte Ansprache von potenziellen Spendern ist sowohl für unsere Mitglieder als auch die potenziellen Spender wichtig. Sie führt zu einem möglichst effizienten Matching zwischen passender Spendenorganisation / NPO und Spender und erhöht damit das Spendenvolumen. Mit Blick auf die vorangehenden Erläuterungen lehnen wir und unsere Mitglieder jeglichen Swiss Finish ab. Wir sind damit einverstanden, dass dort, wo sinnvoll, die Vorgaben der Europarats-Konvention (E-SEV 108) eingehalten werden. Spielräume, welche der E-SEV 108 gewährt, sind dabei auszunutzen. Betreffend die EU-Datenschutzgrundverordnung (EU-DSGVO) genügt das Erreichen einer Angemessenheit. Eine eins-zu-eins Übernahme der EU-Bestimmungen ist hierzu nicht notwendig.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Swissfundraising	DSG	3		a	Wir begrüssen, dass es beim Begriff der „Personendaten“ inhaltlich keine Änderungen geben soll. Die Ausführungen im erläuternden Bericht führen hierbei jedoch im Online-Kontext zu Unklarheiten. Im erläuternden Bericht wird hierzu aus den Erwägungsgründen zur EU-DSGVO zitiert. Die betreffenden Zitatstellen führten in der EU jedoch gerade zu Diskussionen über die Frage, wie die Bestimmbarkeit von Personen im Online-Kontext zu verstehen ist. Die entsprechenden Zitate sind in den Materialien, insbesondere der Botschaft, zu streichen. Es ist vielmehr auf die Praxis und Rechtsprechung zum geltenden DSG zu verweisen. Besonders wichtig ist, dass die Anwendbarkeit der sog. relativen Methode bei der Prüfung der Bestimmbarkeit explizit anerkannt wird.
Swissfundraising	DSG	3		f	**Bei der vorgeschlagenen Regelung des Profiling handelt es sich um einen Swiss Finish. Dieser geht ohne Not über die Regelung in der EU-DSGVO (Art. 4 Ziff. 4) hinaus.** Die vorgeschlagene Bestimmung wird auch vom E-SEV 108 nicht verlangt. In der EU-DSGVO sind für das „normale“ Profiling keine besonderen Datenbearbeitungsregeln aufgestellt. Nur beim automatisierten Profiling, das zu einem Entscheid mit erheblicher Auswirkung auf die betroffene Person führt, werden besondere Massnahmen verlangt. Darüber hinaus ist die Definition des Profiling vollkommen unklar. Aufgrund des vorgeschlagenen Wortlauts und der Ausführungen im erläuternden Bericht könnte eine grosse Vielzahl von Datenbearbeitungen als Profiling qualifiziert werden, ohne dass die betroffenen Personen bei diesen Datenbearbeitungen einen erhöhten Schutz bräuchten. Die Variable Kaufkraft ist z.B. ein wichtiges Kriterium

					für die Selektion von Adressdaten für unsere Mitglieder. Die Variable Kaufkraft kann jedoch auf unterschiedliche Arten gebildet werden. Verfügt ein Unternehmen über Transaktionsdaten über eine längere Zeitperiode, ergibt sich eine ganz andere Art der Kaufkraftbestimmung als wenn die Kaufkraft annäherungsweise mithilfe des Wohnortes, des Berufs usw. bestimmt wird. Nicht jede Analyse oder Auswertung der wirtschaftlichen Lage führt zu einem Risiko für die Persönlichkeit.
Swissfundraising	DSG	4	3		Das Erfordernis der „klaren“ Erkennbarkeit ist zu streichen. Im erläuternden Bericht wird darauf hingewiesen, dass keine inhaltliche Änderung beabsichtigt wird. Dann ist auch auf Änderungen des Wortlautes zu verzichten, falls sich keine zwingende Notwendigkeit ergibt. Vorliegend für die terminologische Änderung ausschliesslich zu Unklarheiten und Rechtsunsicherheit.
Swissfundraising	DSG	4	6		**Aufgrund des Gesetzeswortlautes und der Ausführungen im erläuternden Bericht ist unklar, weshalb hier im Vergleich zum geltenden DSG eine Änderung vorgenommen wurde. Es ist auf die Änderung zu verzichten.** Im erläuternden Bericht wird festgehalten, dass inhaltlich keine Änderung beabsichtigt ist. Dies ist absolut wichtig. Eine Änderung drängt sich aufgrund der Erfahrungen zum bisherigen Recht nicht auf. Die vorgeschlagene Ergänzung des Wortlautes führt damit unnötig zu Unklarheiten. Die strengen Regelungen für die Einwilligung in der EU-DSGVO werden unmittelbar aus dem Wortlaut abgeleitet. Mit der vorgeschlagenen Ergänzung ist daher unklar, ob die Einwilligung nicht doch plötzlich im Sinne der EU-Anforderungen interpretiert wird, obwohl inhaltlich keine Änderung beabsichtigt wird. Sollte der vorgeschlagene Wortlaut beibehalten werden, ist in den Materialien nochmals explizit klarzustellen, dass keine inhaltliche Änderung beabsichtigt ist und insbesondere die Anforderungen an die Einwilligung in der EU-DSGVO in der

					Schweiz nicht gelten. Die Ausführungen zur „ausdrücklichen" Einwilligung sind unklar. Diese Ausführungen sind für die Materialien nochmals zu überarbeiten und zu präzisieren. Klarheit betreffend die ausdrückliche Einwilligung ist für unsere Mitglieder besonders wichtig, wenn für das Profiling eine ausdrückliche Einwilligung vorausgesetzt werden soll.
Swissfundraising	DSG	5 + 6			**Bei den Regelungen zum Datentransfer ins Ausland handelt es sich um einen Swiss Finish.** Unseres Erachtens würde die geltende Regelung weiterhin genügen. Weder die EU-DSGVO noch E-SEV 108 verlangen eine derart komplizierte Lösung. Die vorgeschlagene Lösung führt zu unnötigem administrativem Aufwand und kann, wegen der zahlreichen Informations- und Genehmigungspflichten, Datentransfers zeitlich verzögern.
Swissfundraising	DSG	7			Wir begrüssen, dass die Bestimmungen zur Auftragsdatenbearbeitung im Grundsatz beibehalten werden. Unsere Mitglieder sind auf die Möglichkeit der Auftragsdatenbearbeitung in verschiedener Hinsicht angewiesen. **Bei einzelnen neu vorgeschlagenen Bestimmungen handelt es sich um einen Swiss Finish**. Dieser würde die Auftragsdatenbearbeitung erschweren. Dies betrifft insbesondere die Anforderung, dass ein Auftragsbearbeiter weitere Sub-Unternehmer nur mit schriftlicher Zustimmung des Verantwortlichen beiziehen kann. Diese Anforderung ist nicht notwendig. Für die betroffene Person ist allein entscheidend, dass der Verantwortliche letztverantwortlich bleibt und auch für Fehlverhalten von Auftragsbearbeitern Verantwortung übernehmen muss. Zu streichen ist auch die Kompetenz des Bundesrates zum Erlass weiterer Pflichten. Die Pflichten nach geltendem Recht sind bereits ausreichend klar. Es ist nicht ersichtlich, weshalb es eine Kompetenz zum Erlass weiterer Pflichten

					braucht.
Swissfundraising	DSG	8			Wir begrüssen die Einführung von Empfehlungen der guten Praxis. Diese können zu hilfreichen Präzisierungen führen. Wir sind jedoch der Auffassung, dass die Initiative für den Erlass solcher Empfehlungen alleine von den Industrieorganisationen oder Verbänden ausgehen muss. Der EDÖB soll keine Kompetenz zur Initiierung von Empfehlungen haben. Gegen Entscheide betreffend die Genehmigung oder Nicht-Genehmigung von solchen Empfehlungen muss es ein Rechtsmittel geben. Die Empfehlungen dürften faktisch gesetzesvertretend wirken. Die Details zum Rechtsmittel (z.B. die Frage der Beschwerdelegitimation) sind im Gesetz und den Materialien festzulegen.
Swissfundraising	DSG	12			**Bei dieser Regelung handelt es sich um einen Swiss Finish**. Die Bestimmung ist zu streichen. Entsprechende Regelungen wären ohnehin gesetzessystematisch in anderen Gesetzen, insbesondere im Zivilgesetzbuch, einzubauen.
Swissfundraising	DSG	13			Die Einführung einer aktiven Informationspflicht bei allen Datenbearbeitungen wirkt sich erheblich auf die Geschäftsaktivitäten unserer Mitglieder aus. Indirekt wirkt sich diese Pflicht bereits bei der Datenbeschaffung durch externe Kooperationspartner aus. Je höher die Anforderungen an die Umsetzung der Informationspflicht, je höher der Datenbeschaffungsaufwand, desto kleiner die zur Verfügung stehenden Adressdaten. Es ist fraglich, ob die aktive, ausführliche Informationspflicht die Transparenz seitens der betroffenen Personen effektiv erhöht. Die Informationen sind auf das Wesentliche zu beschränken. Bei der Umsetzung der Informationspflicht sind die vorangehenden Ausführungen

					im Blickfeld zu behalten. Es ist hierbei zu berücksichtigen, dass die modernen Datenschutzgesetze dem sog. risiko-basierten Ansatz folgen. Die Anforderungen an die Datenbearbeitungen sollen jeweils vom Risikograd und dem Schutzbedürfnis der betroffenen Person abhängig sein. Betreffend Umsetzung der Informationspflicht ist klarzustellen, dass die Information mittels standardisierter Datenschutzerklärung auf der Webseite ausreichend ist. Dies ist explizit auch im Explanatory Report zum E-SEV 108 so vorgesehen. Klarzustellen ist auch, dass sich die Informationspflicht auf Daten und Kenntnisse bezieht, welche im Zeitpunkt der Datenbeschaffung vorhanden sind. Eine Nachinformation bei Änderung dieser Daten und Informationen ist gestützt auf die Informationspflicht nicht erforderlich.
Swissfundraising	DSG	13	2		Die Aufzählung mit den Informationsinhalten ist auf das Wesentliche zu kürzen (wer bearbeitet welche Daten oder Datenkategorien für welchen Zweck) und muss abschliessend sein. Gerade weil die Einhaltung dieser Pflicht mit Sanktionen bedroht ist, ist die Rechtssicherheit betreffend zu liefernde Informationen eminent wichtig.
Swissfundraising	DSG	13	4		**Es handelt sich hierbei um einen unnötigen Swiss Finish.** Die Bestimmung ist zu streichen. Die betreffende Bestimmung ist zum Schutz der betroffenen Personen nicht notwendig.
Swissfundraising	DSG	13	5		Die Informationspflicht bei indirekter Datenbeschaffung hat erhebliche Auswirkungen auf die Geschäftstätigkeit unserer Mitglieder. Die zielgerichtete Ansprache von neuen potenziellen Spendern ist ohne indirekte Datenbeschaffungen nicht möglich. Um die Kommunikation möglichst zielgerichtet auszugestalten, müssen zudem bestehende Kontaktdaten veredelt werden. Dies geschieht regelmässig durch Daten aus Drittquellen. Sollte die Pflicht beibehalten werden, sind die vorangehenden Ausführungen bei

					der Umsetzung zu berücksichtigen. Dort ist insbesondere auch der risiko-basierte Ansatz entscheidend. Es ist im Gesetz, wie in der EU-DSGVO, vorzusehen, dass die Information bei der indirekten Datenbeschaffung zeitlich verzögert erfolgen darf, z.B. auch erst bei der ersten Kommunikation mit der betroffenen Person. Dies wird auch durch den E-SEV 108 erlaubt. Zudem muss es auch bei der indirekten Datenbeschaffung erlaubt sein, die Information in standardisierten Datenschutzerklärungen sicherzustellen.
Swissfundraising	DSG	14			**Es handelt sich um einen Swiss Finish.** Die Ausnahmeregelung in der EU-DSGVO ist viel weiter gefasst. Die zusätzlich in der EU-DSGVO enthaltenen Ausnahmen sind in Art. 14 VE-DSG aufzunehmen.
Swissfundraising	DSG	15			**Es handelt sich wiederum um einen Swiss Finish.** Der Anwendungsbereich ist viel weiter gefasst als in der EU-DSGVO. Auch der E-SEV 108 verlangt keine derart extensive Regelung. Wichtig ist insbesondere eine Klarstellung, dass auch die rechtliche Wirkung von erheblicher Bedeutung sein muss. Theoretisch könnte sonst jeder Entscheid zu einer rechtlichen Wirkung führen.
Swissfundraising	DSG	16			**Es handelt sich wiederum um einen Swiss Finish.** Mit der vorgeschlagenen Regelung könnte theoretisch selbst eine einzelne Datenbekanntgabe ins Ausland die Pflicht zur Datenschutz-Folgenabschätzung auslösen. Es ist klarzustellen, dass nur regelmässig durchgeführte Datenbearbeitungsprozesse eine solche Pflicht auslösen. Des Weiteren ist die Schwelle für die Pflichtauslösung anzuheben. Entsprechend der Bestimmung in der EU-DSGVO sollte die Pflicht erst bei einem hohen Risiko

					(oder besser bei einem besonders hohen Risiko) ausgelöst werden. Dies stünde im Einklang mit dem risiko-basierten Ansatz. **Die vorgeschlagene Bestimmung verlangt, dass auch der Auftragsbearbeiter eine Datenschutz-Folgenabschätzung durchführen muss. Hierbei handelt es sich um einen Swiss Finish, der zu streichen ist.** Die EU-DSGVO sieht keine entsprechende Verpflichtung des Auftragsbearbeiters vor. **Um einen Swiss Finish handelt es sich auch bei der Meldepflicht an den EDÖB.** Es ist vorgesehen, dass der EDÖB nach jeder Datenschutz-Folgenabschätzung zu notifizieren ist. Dies führt zu einem unverhältnismässigen Aufwand und zu einer Überlastung des EDÖB. Art. 36 EU-DSGVO hat hier eine viel geeignetere Lösung gefunden. Dort muss nur notifiziert werden, wenn sich aus der Datenschutz-Folgenabschätzung effektiv ein hohes Risiko ergab und wenn der Datenbearbeiter dieses Risiko nicht mit geeigneten Massnahmen reduzieren kann oder will. Diese Lösung ist auch für die Schweiz zu übernehmen.
Swissfundraising	DSG	17	1		**Es handelt sich um einen Swiss Finish.** Es ist die Lösung der EU zu implementieren, bei deren nur bei einer erheblichen Gefährdung der Interessen der betroffenen Person eine Meldung notwendig ist. **Die Lösung der EU orientiert sich hierbei am risiko-basierten Ansatz, der auch für die Schweiz gelten sollte.**
Swissfundraising	DSG	17	2		**Es handelt sich wiederum um einen Swiss Finish.** Die Meldepflicht an die betroffene Person ist zu streichen oder dann auf ganz wenige, besonders kritische Datenpannen zu beschränken.
Swissfundraising	DSG	18			Privacy by Design und by Default entspricht dem risiko-basierten Ansatz und würde sich bei korrekter Interpretation bereits aus dem bestehenden Art. 7 DSG ergeben. Mit der expliziten Nennung dieser Pflichten wird inhaltlich nichts gewonnen.

					Weder im vorgeschlagenen Wortlaut, noch im erläuternden Bericht wird präzisiert, wie die Datenbearbeiter bei diesen Pflichten vorzugehen hat. Es besteht eine vollständige Rechtsunsicherheit. Dies ist besonders bedenklich, weil die Verletzung dieser Pflichten mit Sanktionen bedroht wird.
Swissfundraising	DSG	19		a	**Es handelt sich auch hier um einen Swiss Finish.** Die EU-DSGVO sieht Ausnahmen vor, welche nicht in den Vorentwurf übernommen wurde. Der Umfang der Dokumentationspflicht geht nicht klar aus dem Wortlaut und dem erläuternden Bericht hervor. Es ist klarzustellen, dass es nicht um die Dokumentation einer einzigen Datenbearbeitung gehen kann.
Swissfundraising	DSG	19		b	**Eine solche Mitteilungspflicht ist im E-SEV 108 nicht vorgesehen (Swiss Finish). Sie ist deshalb ersatzlos zu streichen.** Sollte an der Pflicht festgehalten werden, muss ein berechtigtes Interesse der betroffenen Person eine Voraussetzung sein.
Swissfundraising	DSG	20	1		**Es handelt sich um einen Swiss Finish.** Der E-SEV 108 sieht keine allgemeine Kostenlosigkeit vor. Diese Bestimmung ist daher zu streichen.
Swissfundraising	DSG	20	3		**Das Auskunftsrecht bei automatisierten Einzelfallentscheidungen ist viel zu weit gefasst und nach der vorgeschlagenen Regelung geradezu uferlos.** Es handelt sich um einen unnötigen Swiss Finish. Das Auskunftsrecht muss auf Konstellationen beschränkt werden, bei denen eine Informationspflicht und ein Anhörungsrecht bestehen. Zudem ist der Umfang der Auskunft einzuschränken. Der Umfang soll sich an der entsprechenden Regelung in der EU-DSGVO orientieren. Wichtig ist hierbei, dass Geschäftsgeheimnisse geschützt bleiben.
Swissfundraising	DSG	23			**Es handelt sich um einen Swiss Finish, der sich besonders nachteilig auf die Geschäftsaktivitäten unserer Mitglieder auswirkt.** Die ausdrückliche Einwilligung würde die zielgerichtete und fokussierte

					Kommunikation mit bestehenden und potenziellen Spendern stark beeinträchtigen. Unsere Mitglieder wären dadurch gezwungen, die Kommunikation zu Spenden- oder anderen Kampagnen unselektiert oder wenig selektiert an eine viel grössere Anzahl Personen zu verschicken. Dies führt bei unseren Mitgliedern zu unnötigen Kosten und bei den Empfängern dazu, dass sie allenfalls vermehrt Kommunikation erhalten, welche sie nicht interessiert. In der EU-DSGVO ist keine solche Regelung vorgesehen. Normales Profiling wird dort nicht anders geregelt als andere Datenbearbeitungen. Nur wenn das automatisierte Profiling zu Entscheiden mit erheblicher rechtlicher Wirkung führt, sind besondere Schutzmassnahmen vorgesehen. Auch diesbezüglich hat die EU den risiko-basierten Ansatz besser umgesetzt.
Swissfundraising	DSG	23	3		Die Beibehaltung der geltenden Regelung von allgemein zugänglich gemachten Daten ist zu begrüssen und für unsere Mitglieder besonders wichtig.
Swissfundraising	DSG	44	3		**Diese Regelung ist rechtsstaatlich bedenklich.** Vorsorgliche Massnahmen des EDÖB können bei einem Unternehmen erheblich Schäden verursachen. Die Möglichkeit der Überprüfung dieser Massnahmen muss daher gegeben sein. Die Praxis zum bisherigen Recht zeigt, dass das Bundesverwaltungsgericht auf Beschwerde hin doch vereinzelt solche Massnahmen des EDÖB aufgehoben hat.
Swissfundraising	DSG	50 ff.			**Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt**. Dieses vorgesehene Sanktionssystem steht der Digitalen Strategie der Schweiz diametral entgegen. Es führt zu einem ganz erheblichen Standortnachteil der Schweiz. Die vorgeschlagene Sanktionsregelung führt dazu, dass die für Datenbearbeitungen verantwortlichen Personen in den Unternehmen direkt mit Strafrisiken bedroht sind. Die subsidiäre Haftung des Unternehmens dürfte gerade bei kleineren Unternehmen, wo die verantwortliche Person relativ leicht

					eruiert werden kann, nicht zur Anwendung gelangen. Die Strafrisiken für die verantwortlichen Personen würden dazu führen, dass kein Mitarbeiter bereit wäre, die Funktion eines internen Datenschutzbeauftragten zu übernehmen. Dies ist aus Sicht der Datenschutz-Compliance negativ. Zudem würde die Strafbarkeit der Mitarbeiter dazu führen, dass diese – allenfalls vorschnell – Verstösse und vermeintliche Verstösse dem EDÖB melden, um sich selber zu entlasten. Die vorgeschlagene Sanktionslösung führt darüber hinaus bei schweizerischen Unternehmen zu Wettbewerbsnachteilen. Die Vollstreckung allfälliger Sanktionen gegenüber ausländischen Unternehmen wäre stark erschwert, weshalb sich diese allenfalls gar nicht an die Regeln halten würden. Des Weiteren verstösst die vorgeschlagene Regelung gegen gewichtige (rechtsstaatliche) strafprozessuale Prinzipien. Betroffen ist primär das Bestimmtheitsgebot. Tangiert ist aufgrund der verschiedenen Informations-, Melde- und Mitwirkungspflichten im VE-DSG jedoch auch der Grundsatz „nemo tenetur“, d.h. das Selbstbelastungsgebot. Die Pflicht, Datenschutzverstösse zu melden, welche ihrerseits strafbedroht ist, führt faktisch zu einer Selbstanzeigepflicht. **Betreffend die Ausgestaltung eines alternativen Sanktionssystems verweisen wir auf den entsprechenden Vorschlag der economiesuisse**. Im Vordergrund stehen Verwaltungsstrafen gegen das Unternehmen und nicht die natürlichen Personen. Anknüpfungspunkt für die Strafbarkeit der Unternehmen wären Organisationsmängel im Unternehmen, d.h. eine mangelhafte Datenschutz-Compliance. Lediglich subsidiär soll eine Strafbarkeit von Mitarbeitern möglich sein, wenn diese absichtlich bzw. mit Vorsatz gegen interne oder gesetzliche Datenschutzregeln verstossen haben. Aus rechtsstaatlichen Überlegungen darf nicht der EDÖB über die Verwaltungssanktionen entscheiden. Die untersuchende bzw. anklagende Behörde soll nicht gleichzeitig die urteilende Behörde sein. Um dieses Problem zu lösen, ist eine neue Entscheidinstanz zu gründen. Das Verhältnis zwischen

					dieser neuen Behörde und dem EDÖB wäre im DSG zu regeln. Betreffend die Anpassung des Strafkataloges in Art. 50 und 51 VE-DSG wird auf die detaillierten Aufführungen in der Stellungnahme von economiesuisse verwiesen. Wir unterstützen die entsprechenden Vorschläge.
Swissfundraising	DSG	52			**Der vorgeschlagene Ausbau der geltenden Regelung (Art. 35 DSG) ist abzulehnen. Die vorgeschlagene Regelung ist weder durch die EU-DSGVO noch den E-SEV 108 erforderlich.** Sofern die Regelung extensiv interpretiert wird, würde die Konzeption des Schweizerischen Datenschutzrechts auf den Kopf gestellt – zumindest betreffend die Bekanntgabe von Daten an Dritte. Bis anhin durften „normale“ Personendaten grundsätzlich ohne einen Rechtfertigungsgrund an Dritte weitergegeben werden – sofern auch die anderen Datenbearbeitungsgrundsätze eingehalten wurden. Nur für besonders schützenswerte Personendaten und Persönlichkeitsprofile wurde vermutet, dass die Bekanntgabe an Dritte ohne Zustimmung der betroffenen Person eine Persönlichkeitsrechtsverletzung darstellt. Art. 52 VE-DSG würde diesen Mechanismus auf den Kopf stellen. Obwohl eigentlich der materielle Teil des Datenschutzgesetzes für die Bekanntgabe von normalen Personendaten an Dritte keinen Rechtfertigungsgrund verlangt, würde eine solche Pflicht zumindest bei der Bekanntgabe von „geheimen“ Personendaten über den Umweg der strafbewehrten Schweigepflicht eingeführt werden. **Hinzu kommt, dass der Begriff der „geheimen Personendaten“ unklar ist.**

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Swissfundraising	3 lit. a	In den Materialien ist klarzustellen, dass sich an der Interpretation des Begriffs Personendaten inhaltlich nichts ändert. Auf Zitate aus der EU-DSGVO ist zu verzichten. Klarzustellen ist insbesondere auch, dass die sog. relative Methode entscheidend für die Bestimmbarkeit ist.
Swissfundraising	3 lit. f	Das Profiling muss klar auf automatisierte Bearbeitungen beschränkt werden. Zudem muss der Begriff in den Materialien besser präzisiert werden. Es ist auch klarzustellen, dass nicht jede Auswertung zu einem erhöhten Schutzbedürfnis führt.
Swissfundraising	4 Abs. 6	**Auch hier sollte in den Materialien auf allzu viele, unklare Hinweise verzichtet werden.** Klarzustellen ist primär, dass sich inhaltlich an den Anforderungen an die Einwilligung nichts ändert und dass insbesondere die strengen Anforderungen in der EU nicht übernommen werden. Zudem ist der Begriff der ausdrücklichen Einwilligung zu präzisieren.
Swissfundraising	8	**Es muss zwingend klargestellt werden, dass die Initiative für solche Empfehlungen von den Verbänden und Organisationen, nicht jedoch vom EDÖB ausgehen soll.** Zudem muss es gegen Genehmigungsentscheide ein Rechtsmittel geben. Die Voraussetzungen an das Rechtsmittel sind in den Materialien zu präzisieren.
Swissfundraising	13	In den Materialien ist zu präzisieren, wie die Pflichten umgesetzt werden muss. Hierbei muss die Information in einer standardisierten Datenschutzerklärung auf der Webseite ausreichen. Zudem ist klarzustellen, dass keine Nachinformation notwendig ist.
Swissfundraising	15	Hier muss klargestellt werden, dass auch „rechtliche Auswirkungen“ eine gewisse Schwere aufweisen müssen.
Swissfundraising	23 Abs. 3	Die Erwägung im erläuternden Bericht, wonach die Regelung nur zum Tragen komme, wenn die Bearbeitung dieser Daten auch rechtmässig erfolgt (S. 69), ist unzutreffend und daher in der Botschaft klar zu stellen.
Swissfundraising	50 ff	Betreffend Sanktionssystem kann auf die Ausführungen zu den einzelnen Artikeln verwiesen werden.

Swissfundraising	Seite 88	Übergangsbestimmungen Die Übergangsbestimmungen müssen insbesondere für Altdaten ergänzt worden. Es ist ausdrücklich festzuhalten, dass Personendaten, die unter dem alten Recht rechtmässig erhoben und bearbeitet wurden, im entsprechenden Umfang auch unter dem neuen Recht weiterhin bearbeitet werden dürfen. Schlussendlich ist eine angemessene Übergangsfrist von mindestens zwei Jahren für die Umsetzung aller neuen Pflichten unter dem Gesetz vorzusehen um den Unternehmen die Umstellung ihrer Prozesse zu ermöglichen. Eine entsprechende Übergangsfrist hat auch die EU-DSGVO nach ihrem Inkrafttreten vorgesehen.

SwissHoldings
Verband der Industrie- und Dienstleistungskonzerne in der Schweiz
Fédération des groupes industriels et de services en Suisse
Federation of Industrial and Service Groups in Switzerland

4. April 2017

Frau Bundesrätin Simonetta Sommaruga
Vorsteherin EJPD
Bundeshaus West
3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

Stellungnahmen:

1. **Zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)**
2. **Zur vorgesehenen Ratifizierung des Änderungsprotokolls zum Datenschutzübereinkommen des Europarats SEV 108**

Sehr geehrte Frau Bundesrätin

Im Dezember 2016 haben Sie die interessierten Kreise eingeladen, zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. Als Fachverband, der sich für Rahmenbedingungen einsetzt, beachtet SwissHoldings übergeordnete, tendenziell gesamtwirtschaftliche Aspekte und zieht diese in ihre Überlegungen mit ein.

Haltung von SwissHoldings:

1. Der Umgang mit **Daten** ist für die Digitale Wirtschaft zentral. Eine **optimale Datenpolitik** bietet den **Unternehmen Entfaltungsmöglichkeiten** und **sichert das Vertrauen der Nutzer**. Die Regulierung hat sich am **Verhältnismässigkeitsprinzip** zu orientieren. Damit ist in der auf dem Persönlichkeitsschutz basierenden **Datenschutzregulierung** für die Unternehmen ein **Maximum an Flexibilität und ein Minimum an Belastung** zu wahren.
2. Spielräume im Verhältnis zum internationalen Recht sowie das **etablierte System der Selbstregulierung sind zu nutzen**. Zugleich ist aber **sicherzustellen**, dass die **Beibehaltung der Äquivalenz mit dem Datenschutzrecht der EU** nicht gefährdet wird. Die diversen im Vergleich zum EU-Raum **überschiessenden Regelungen sind anzupassen.** Dabei soll die Totalrevision dazu genutzt werden, be-

Nägeligasse 13, Postfach
CH-3001 Bern, Switzerland
www.swissholdings.ch
Phone +41 31 356 68 68
Fax +41 31 352 32 55
sh@swissholdings.ch

stehende Bestimmungen zu hinterfragen und an die technologische Entwicklung anzupassen.

3. Der Begriff **«Profiling»** ist auf automatisierte Bewertungen von Personendaten einzuschränken und die Bedingungen dazu sind stark zu reduzieren (Information statt Einwilligung);
4. Die Initiative für **Empfehlungen der guten Praxis muss stets zwingend von der betroffenen Industrie ausgehen**. Die **Selbstregulierung** ermöglicht es mittels Bezug zur Praxis, sachgerechte Lösungen zu entwickeln. Geben sich Unternehmen einen **betrieblichen Datenschutzbeauftragten**, soll dies auf **strikt freiwilliger Basis** erfolgen und dem Unternehmen daraus **entsprechende Erleichterungen** bereiten.
5. Diverse **Informations- und Meldepflichten sind überschiessend**. Sie bedeuten unverhältnismässigen Aufwand und generieren eine **unübersehbare, unproduktive Flut von Informationen und Meldungen**. Abzulehnen sind auch die damit verbundene Offenlegung von Geschäftsgeheimnissen und die Pflicht, sich selbst zu belasten. Gesamthaft wirken sich die **Vorschläge innovations- und wettbewerbshindernd** aus. Sie sind dem vom Vorentwurf angestrebten **risikobasierten Ansatz entsprechend substantiell zu reduzieren**. Dies betrifft insbesondere automatisierte Einzelfallentscheide, Datenschutz-Folgenabschätzungen und Meldungen von Datenschutzverstössen. Darüber hinaus braucht es eine **Relativierung der Kostenlosigkeit des Auskunftsrechts** und weitere, griffige Massnahmen, um dem Missbrauch des Datenschutzrechtes zu datenschutzfremden Zwecken entgegenzuwirken;
6. Ein weiterer umfassender Kritikpunkt ist das vorgeschlagene **Sanktionssystem**: **Private, strafrechtliche Sanktionen sind weder verhältnismässig noch zielführend**. Es ist ein tragbares, mit den **rechtsstaatlichen Grundsätzen vereinbares Sanktionssystem** zu implementieren. Gleichzeitig ist eine zu **grosse Machtfülle des EDÖB** zu verhindern. Die Wirtschaft skizziert ein eigenes Sanktionsmodell als Grundlage für die **Entwicklung eines alternativen Lösungsansatzes**.
7. Der **Ratifizierung des Änderungsprotokolls** zur von der Schweiz bereits früher ratifizierten "Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" (**Datenschutzkonvention SEV 108**) in der künftigen modernisierten Form ist **aus grundsätzlichen Überlegungen zuzustimmen**.

Unsere Überlegungen im Einzelnen:

A. Grundsätzliche Bemerkungen

SwissHoldings, der Verband der Industrie- und Dienstleistungskonzerne in der Schweiz, umfasst 62 der grössten Konzerne in der Schweiz, die zusammen rund 70 Prozent der gesamten Börsenkapitalisierung der SIX Swiss Exchange ausmachen. Unsere Mitgliedfirmen beschäftigen global rund 1,7 Millionen Personen, rund 200‘000 davon arbeiten in der Schweiz. Über die zahlreichen Dienstleistungs- und Lieferaufträge, die sie an KMU erteilen, beschäftigen die multinationalen Unternehmen der Schweiz – direkt und indirekt – über die Hälfte aller Angestellten in der Schweiz.

Daten als solche sind zu einem wichtigen Wirtschaftsgut geworden. Sie müssen in einer auf hochwertige Forschung ausgerichteten Wissenswirtschaft nicht nur in grossem Umfang erhoben, sondern auch effizient verwaltet und verteilt werden. Neue Möglichkeiten zur Auswertung grosser Datenmengen und daraus resultierende Angebote sowie die hohe Bedeutung von sozialen Medien führen dazu, dass sich deren Sichtbarkeit auch in der Öffentlichkeit erhöht. Der Ausgleich der verschiedenen Interessen führt weltweit zu spezifischen Digitalregulierungen. Schweizerische Unternehmen sind davon in mehrfacher Hinsicht direkt betroffen: Zum Beispiel im Personalbereich bezüglich des Umgangs mit Mitarbeiterdaten, in Marketing und Auftragsabwicklung bezüglich Werbezielgruppen und Kunden sowie je nach Sektor in Forschung und Entwicklung oder bei personalisierten Geschäftsmodellen. Die Qualität der Datenregulierung ist dabei ein wichtiger Faktor im Standortwettbewerb. Die Leitlinien unseres Verbands lauten diesbezüglich:

- Die Digitalisierung ist aus dem Geschäftsalltag der Schweizer Konzerne nicht mehr wegzudenken. Sie ist Teil der Geschäftsmodelle und wird an Bedeutung gewinnen.
- Die für unsere Prosperität entscheidende Forschung und Entwicklung der Zukunft verlangt weitgehend ungehinderte internationale Verbreitung und Verfügbarkeit von Daten.
- Die Datenregulierung der Schweiz muss die Digitalisierung nicht nur im Auge behalten, sondern sie auch fördern.
- Um im internationalen Standortwettbewerb mitzuhalten, braucht es einen Datenregulierungsrahmen, der die richtigen Signale sendet.
- Während bei der laufenden Datenschutzvernehmlassung der Schutz der Persönlichkeit im Fokus steht, muss eine umfassende, kohärente nationale Datenstrategie den Ausgleich mit verschiedenen weiteren wirtschaftlichen und gesellschaftlichen Zielsetzungen (Gesundheit, wirtschaftliches Wohlergehen, Arbeitsplätze etc.) sicherstellen.

Für unseren Verband, als Vertreter der international tätigen Wirtschaft der Schweiz, betrachten wir die Gestaltung der Datenregulierung als eines unserer Kernthemen. In dieser wiederum stellt der rechtliche Schutz der Persönlichkeit, mittels der jetzt zur Vernehmlassung stehenden Datenschutzgesetzgebung, einen wichtigen Pfeiler dar.

Auch gilt es, die übergeordneten Ziele der Strategie «Digitale Schweiz» des Bundesrates im Fokus zu behalten: Zu berücksichtigen ist insbesondere auch der Nutzen der Daten für den digitalen Fortschritt und die Ausschöpfung des wirtschaftlichen Potentials im Interesse der Konsumenten und Unternehmen. Eine einseitige Orientierung lediglich an potentiellen Risiken ist verfehlt; Innovation und Entwicklung dürfen durch den Datenschutz nicht unnötig behindert werden. Der Bundesrat hat diese Zielrichtung auch in seinem Beschluss vom 22. März 2017 zur Datenpolitik des Bundes richtigerweise grundsätzlich bestätigt.

B. Beurteilung des Vorentwurfs zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

1. Einleitende Bemerkungen

Ein angemessenes und wirksames Datenschutzgesetz ist für die Wirtschaft von grosser Bedeutung. Dieses muss Raum für die wirtschaftliche Entwicklung lassen sowie der Rechts- und Investitionssicherheit dienen. Darüber hinaus sind Akzeptanz und Vertrauen der Nutzer in den Datenschutz eine zentrale Voraussetzung für die Fortentwicklung der immer wichtiger werdenden digitalen Wirtschaft und der Nutzung des damit verbundenen wirtschaftlichen Potentials. Überschiessende und im Geschäftsalltag nicht praktikable Regulierungen wirken sich demgegenüber innovationshemmend aus. Sie können der Wettbewerbsfähigkeit von Unternehmen auf nationaler Stufe, vor allem aber auch im internationalen Umfeld schaden. Zu weitgehende Bestimmungen, welche den Individuen ihre Handlungsfähigkeit absprechen, führen zudem zu einer Bevormundung der Bürger.

Angesichts der dynamischen technologischen aber auch der internationalen Entwicklungen im Bereich Datenschutz ist für die Schweiz von Bedeutung, dass sie mit modernen Regelungen den Zugang insbesondere zum EU-Raum nicht unnötig einschränkt. Unternehmen aller Grös-

senstufen und entlang der ganzen Wertschöpfungsketten sind vital darauf angewiesen, Daten nicht nur aus der Schweiz exportieren, sondern namentlich auch aus der EU in die Schweiz importieren zu können. Das einfachste und sicherste Mittel dazu wäre es, wenn die EU-Kommission i.S.v. Erw. 104 DSGVO bzw. Art. 45 DSGVO ((EU) 2016/679) der Schweizer Regulierung weiterhin ein «angemessenes Schutzniveau» attestieren könnte. Damit die Schweizer Regulierung aus Sicht der EU derart als *äquivalent* angesehen werden kann, muss sie grundlegende Garantien bieten, wie sie im vorerwähnten Artikel beispielhaft, aber nicht abschliessend aufgeführt sind. Zugleich hat sich das Schweizer Datenschutzrecht auch verbindlich an der Konvention 108 des Europarates zu orientieren.

Hierbei ist innerhalb der internationalen Vorgaben ein Maximum an Flexibilität für den Schweizer Standort zu erhalten; die Wirtschaft soll nicht durch übertriebene Bestimmungen («Swiss Finish») mit unnötigem administrativen und finanziellen Aufwand belastet werden. Dieser wäre überdies auch aus einer gesamtheitlichen Sicht kontraproduktiv, weil solche Schweizer Besonderheiten einen einheitlichen internationalen Datenraum verhindern und damit auch zulasten der Schweizer Unternehmen wettbewerbsverzerrend wirken würden. Damit ist ausdrücklich gemeint, dass das EU-Niveau überschiessende, aber im geltenden DSG (*de lege lata*) schon enthalte Bestimmungen ebenfalls maximal auf das EU-Niveau zurückzunehmen sind.

2. Zweck

Die Zweckbestimmung ist anzupassen. Gerade auch unter Berücksichtigung der Strategie des Bundesrates für eine «digitale Schweiz» ist der Zweck um «die Förderung des freien Verkehrs der Personendaten» zu ergänzen. Dies entspricht dem Ziel des erläuternden Berichts, dass durch die Datenschutzgesetzrevision «die Wettbewerbsfähigkeit der Schweiz gewährleistet und verbessert werden [soll], namentlich indem die Bekanntgabe von Daten ins Ausland erleichtert wird». Eine entsprechende Zielsetzung kennt auch die europäische Verordnung.

3. Geltungsbereich

Berücksichtigung bereichsspezifischer Datenschutzbestimmungen

Einige Mitglieder haben darauf hingewiesen, dass in verschiedenen Bereichen (z.B. in der Humanforschung) spezielle Bestimmungen zu datenschutzrechtlichen Fragen bestehen. Diese sind teilweise auf Verordnungsebene festgeschrieben. Es ist für die betroffenen Unternehmen zentral, dass sie sich weiterhin auf die entsprechenden Regelungen verlassen können. Es sollte festgehalten werden, dass Spezialbestimmungen im Datenschutzrecht den Regelungen des DSG vorgehen bzw. dass der Grundsatz «lex specialis » umfassend zu verstehen ist.

Kein Schutz für juristische Personen

Die Abschaffung des Datenschutzes für Unternehmen analog der DSGVO und E-SEV 108 wird begrüsst. Dieser hat in der Praxis kaum eine Rolle gespielt. Zudem wird der Persönlichkeitsschutz von ZGB 28 und der Schutz von Geschäftsgeheimnissen dadurch nicht tangiert. Einzelunternehmen und Mitglieder von Personengesellschaften, die im Handelsregister eingetragen sind, sind jedoch weiterhin vom Schutz des DSG umfasst. Es wurde angeregt, dass hier dieselbe Regelung zum Geltungsbereich wie für juristische Personen gelten sollte.

Neues Missbrauchspotential beim Auskunftsrecht

Der VE-DSG sieht neu vor, dass das Datenschutzgesetz auch auf bereits rechtshängige Zivilprozesse und laufende Strafverfahren zur Anwendung gelangen soll. Dieser erweiterte Geltungsbereich birgt erhebliches Missbrauchspotential beim Auskunftsrecht (Beweisbeschaffung über die zivilprozessualen Editionsrechte hinaus). Es braucht griffige Mechanismen, welche dem Rechtsmissbrauch oder der nicht vorgesehenen Anwendung dieser Bestimmung im Zivilprozess oder im Strafverfahren entgegenstehen (vgl. nachfolgend Ziff. 11).

Regelung des räumlichen Anwendungsbereichs / IPR

Im VE-DSG fehlt eine Regelung zum räumlichen Anwendungsbereich des Gesetzes. Von wirtschaftlicher Seite her besteht der Wunsch, den räumlichen Anwendungsbereich nicht übermässig auszudehnen und damit den Status quo beizubehalten. Dies bedarf einer gleichzeitigen Anpassung der entsprechenden Regelung im IPRG, damit der Geltungsbereich des Schweizerischen Datenschutzgesetzes in räumlicher Hinsicht relativiert werden kann.

4. Begriffe

Definition der Personendaten

Art. 3 lit. a VE-DSG sieht keine Definition der Bestimmbarkeit vor. Es ist zu konkretisieren was unter «bestimmbaren Personendaten» zu verstehen ist. Zudem ist wie im geltenden Recht klarzustellen, dass mit dem Begriff «Daten» stets *Personen*daten gemeint sind.

Einschränkung der Definition der besonders schützenswerten Personendaten

Die Ausweitung des Begriffs der «besonders schützenswerten Personendaten» auf die entsprechenden Definitionen der genetischen und biometrischen Daten geht zu weit. Der Wortlaut widerspricht den Erläuterungen im Bericht: Angedacht war die Erfassung von Daten, welche zum Zweck bearbeitet werden, eine natürliche Person eindeutig zu identifizieren. Dies entspricht auch der Stossrichtung der Konvention 108. Nach der im VE-DSG vorgeschlagenen Definition wäre beispielsweise künftig jedes Gesichtsfoto als biometrisches Datum erfasst. Die Definition ist entsprechend einzuschränken.

Einschränkung der Definition des Profiling

Die Definition des Begriffs «Profiling» ist im VE-DSG sehr breit gefasst und geht deutlich über die entsprechende Regelung der EU hinaus. In der DSGVO hängt die Zulässigkeit des Profiling von der Wahrnehmung der betroffenen Interessen ab. Nur in Fällen, in denen das Profiling Teil einer *automatischen Entscheidung* wird und rechtliche Wirkung erzeugt, gelten andere Vorschriften. Der VE-DSG vermischt die beiden Institute: Erfasst ist auch das «menschliche», d.h. manuelle Profiling (z.B. eine schriftliche Mitarbeiterbeurteilung oder die Alterskapitalberechnung einer Versicherung) sowie nicht-personenbezogene Daten. Dies stellt eine unzulässige Ausweitung des Geltungsbereiches dar und steht damit im Widerspruch zu Art. 2 Abs. 1 VE-DSG.

Die Definition des Begriffes ist analog der DSGVO auf die *automatisierte* Auswertung von *Personen*daten zu begrenzen. Zudem ist die Auswertung, bzw. Analyse keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte auswirkt. Die Bestimmung sollte daher anstatt «Auswertung» analog der DSGVO den Begriff «Bewertung» verwenden.

Einführung des betrieblichen Datenschutzbeauftragten

Es besteht klar der Wunsch, eine Regelung zur Bezeichnung eines betrieblichen Datenschutzbeauftragten auf freiwilliger Basis vorzusehen. Dies soll im Gegenzug mit einer entsprechenden Erleichterung bei den Pflichten unter dem DSG verknüpft werden (vgl. nachfolgend, Ziff. 8.2). In diesem Sinne ist auch eine Definition des betrieblichen Datenschutzbeauftragten erforderlich.

5. Grundsätze

Klare Terminologien

Der VE-DSG verschärft den Grundsatz der Erkennbarkeit des Zweckes unnötigerweise mit dem Zusatz der «klaren» Erkennbarkeit. Diese Anpassung an die Terminologie des DSGVO ist in diesem Falle verfehlt, da die Schweizer Regelung einem unterschiedlichen Grundkonzept folgt (Erkennbarkeit im Rahmen einer klaren Zweckbindung). Die Verschärfung ist auslegungsbedürftig und produziert damit auch Rechtsunsicherheit. Der Zusatz ist nicht erforderlich und zu streichen.

Dies gilt auch für den Begriff der «eindeutigen» Einwilligung von Art. 4 Abs. 6 VE-DSG: Damit wird lediglich wiederholt, was bereits heute unter dem risikobasierten Ansatz gilt. Der Zusatz ist ebenfalls wegzulassen. Auch wann eine Einwilligung «ausdrücklich» sein soll, ist nicht klar. Jedenfalls muss auch passives Verhalten als gültige Einwilligung gelten, damit weiterhin die im Massengeschäft unumgänglichen Allgemeinen Geschäftsbedingungen (AGB) verwendet werden können. Das Erfordernis der Einwilligung für das Profiling muss gänzlich gestrichen werden (vgl. Ziff. 13).

Keine Nachführungspflicht

Die permanente Nachführungspflicht geht zu weit und ist nicht praktikabel. Der 1. Satz von Art. 4 Abs. 5 VE-DSG ist entsprechend ersatzlos zu streichen.

6. Auslandtransfer

Unnötige Wiederholung von Grundsätzen

Art. 5 Abs. 1 VE-DSG wiederholt bereits statuierte Grundsätze und ist im Kontext von Art. 5 verwirrend und überflüssig. Der Absatz ist deshalb zu streichen.

Keine zwingende Feststellung durch den Bundesrat

Die neu vorgesehene Feststellung durch den Bundesrat, ob Daten im Ausland genügend geschützt sind, bedeutet eine unsachliche und unnötige Einschränkung. Diese Feststellung würde i.d.R. besser durch den Verantwortlichen, gestützt auf eigene Abklärungen und Kenntnisse, erfolgen. Es erscheint zudem problematisch, wenn sich der Verantwortliche nur auf die Einschätzung des Bundesrates verlässt, selbst, wenn ihm eine schwerwiegende Gefährdung von Persönlichkeitsrechten bekannt ist. Die Bestimmung ist dahingehend anzupassen, dass die Feststellung des Bundesrates keine abschliessende ist und diese nur subsidiär zum Zuge kommt.

6.1. Informations- und Genehmigungspflicht

Unklare und widersprüchliche Kategorisierung der Garantien

Die Unterscheidung in Art. 5 Abs. 3 VE-DSG zwischen «spezifischen» und «standardisierten» Garantien ist unklar und macht aus Sicht der Praxis keinen Sinn. Erschwerend kommt hinzu, dass die standardisierten Garantien einer Genehmigung durch den EDÖB bedürfen.

Auch Binding Corporate Rules (BCR) unterliegen der Genehmigungspflicht, diese stellen aber eine Untergruppe der spezifischen Garantien dar. Für diese wiederum ist jedoch nur eine Informationspflicht vorgeschrieben. Dies ist widersprüchlich. Es sollte lediglich zwischen Standardverträgen und anderen Verträgen/Garantien unterschieden und die Pflichten entsprechend angepasst werden.

Berücksichtigung von Geheimhaltungsinteressen

Spezifische Garantien sind in der Regel in Verträgen enthalten. Es ist praxisfern und insbesondere im Zusammenhang mit dem BGÖ problematisch, wenn diese alle dem EDÖB vorgelegt werden müssen.

Kürzung der Genehmigungsfrist

Für eine Genehmigung ist die vorgesehene Frist des EDÖB von 6 Monaten nicht praktikabel. Im Tagesgeschäft sind entsprechende Bewilligungen kurzfristig erforderlich. Mit derart ausgedehnten Fristen ist eine Verwendung solcher Garantien / BCR kaum noch möglich, da ein Unternehmen nach Vertragsabschluss nicht derart lange warten kann. Die Frist ist auf das heutige Mass von 30 Tagen zu kürzen und von einer unbeschränkt möglichen Verlängerung abzusehen. Der Beauftragte muss also innerhalb dieser Frist reagieren, ansonsten gelten die vorgelegten Garantien / BCR als genehmigt.

Zu berücksichtigen ist ferner, dass in gewissen Branchen auch 30 Tage viel zu lang sein können, da aufgrund der Umstände umgehend reagiert werden muss. Für die entsprechenden Sachverhalte liegen bereits heute Spezialregelungen vor, die der Genehmigungspflicht von Art. 5 VE-DSG weiterhin vorgehen müssen (z.B. von der FINMA, um Finanzinstituten die Einhaltung von Pflichten nach ausländischen Bestimmungen zu ermöglichen).

Alternativ: Keine Genehmigung durch den Beauftragten

Einzelne Mitglieder wünschen, die Genehmigung von standardisierten Garantien oder verbindlichen unternehmensinternen Datenschutzvorschriften (BCR) durch den Beauftragten ganz wegzulassen. Die Genehmigungspflicht würde zu einem erheblichen Mehraufwand für die Unternehmen und gegebenenfalls zu Projektverzögerungen führen. Gleichzeitig trage diese kaum etwas zum besseren Datenschutz bei, da das Unternehmen weiterhin selber in der Verantwortung stehe. Ein grenzüberschreitender Datenfluss würde durch diese Regelung erheblich erschwert. Lediglich die DSGVO (nicht die Konvention 108) sieht eine entsprechende Vorgabe vor. Es wird hier klar Raum für einen sich im Verhältnis zur DSGVO differenzierenden Regelungsansatz gesehen. Für ein «angemessenes Schutzniveau» ist die Genehmigung jedenfalls nicht nötig.

Keine Informationspflicht bei Vorliegen standardisierter Garantien

Die pauschale Informationspflicht von Art. 5 Abs. 6 VE-DSG im Zusammenhang mit standardisierten Garantien bringt keinen Mehrwert. Es geht hier um bereits genehmigte oder aner-

kannte Garantien. Dies ist nicht einmal in der DSGVO vorgesehen[1]. Die Bestimmung ist entsprechend zu streichen.

6.2. Ausnahmen

Keine Einwilligung «im Einzelfall»

Die in Art. 6 Abs. 1 lit. a VE-DSG vorgesehene Ausnahme der «Einwilligung im Einzelfall» ist weder sinnvoll noch notwendig. Nach den allgemeinen Grundregeln reicht für wiederkehrende Sachverhalte bei gleichbleibender Erkennbarkeit und Erwartung eine einmalige Einwilligung. Der Zusatz «im Einzelfall» ist zu streichen. Dies gilt auch für die «Bekanntgabe im Einzelfall» (Art. 6 Abs. 1 lit. d VE-DSG).

Erweiterung der Ausnahme i. Zh. mit Verträgen

Die Ausnahmebestimmung von Art. 6 Abs. 1 lit. b VE-DSG ist mit der DSGVO abzustimmen. Die Ausnahme ist auf diejenigen Fälle auszuweiten, in denen die betroffene Person nicht Vertragspartei ist, der betroffene Vertrag aber in ihrem Interesse ist oder zu ihren Gunsten abgeschlossen wurde.

Streichung Begriffe «Gericht» und «Verwaltungsbehörde»

Die Begriffe «Gericht» und «Verwaltungsbehörde» bei Art. 6 Abs. 1 lit. c VE-DSG sind zu streichen. Die Unterscheidung ist nicht erforderlich und es stellen sich schwierige Abgrenzungsfragen. Massgebend ist, dass die Datenbearbeitung zur «Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen» erfolgt.

Keine Informationspflicht bei Vorliegen eines Ausnahmetatbestandes

Die in Art. 6 Abs. 2 vorgesehene Informationspflicht, dies trotz Vorliegen eines Ausnahmetatbestandes, ist unverhältnismässig und zu streichen. Eine entsprechende Bestimmung ist in der Konvention nicht vorgesehen. Nebst zu erwartender hoher Anzahl an Meldungen wäre auch die Information des EDÖB über heikle Verfahren und (Geschäfts-)geheimnisse problematisch (BGÖ).

7. Auftragsdatenbearbeitung

Keine Vergewisserungspflicht

Die in Art. 7 neu vorgesehene Vergewisserungspflicht führt zu massivem Mehraufwand beim Outsourcing der Datenbearbeitung. Es ist unklar, welche Pflichten dem Auftragsdatenbearbeiter überbunden werden sollen. Die Vergewisserungspflicht widerspricht dem prinzipienbasierten Ansatz des VE-DSG und die Präzisierung ist gerade in Bezug auf projektspezifische Herausforderungen kontraproduktiv. Die Bestimmung ist zu streichen. Dies gilt auch für den letzten Satz von Absatz 3 bezüglich Präzisierung weiterer Pflichten des Auftragsbearbeiters durch den Bundesrat.

[1] Vgl. dazu EuGH-Entscheid Schrems und Entscheid der EU-Kommission vom 16.12.2016 (keine erneute Einwilligung im Einzelfall).

Reduzierte Anforderungen an die Einwilligung

Die Anforderung einer «schriftlichen» Zustimmung ist vor dem Hintergrund der heutigen Geschäftsprozesse, dies insbesondere auch aufgrund der komplexen Dienstleistungsverhältnisse, nicht praxistauglich. Eine dokumentierte Zustimmung reicht aus; Schriftlichkeit i.S.v. Art. 13 OR ist nicht erforderlich. Es ist eine technologieneutrale Präzisierung vorzunehmen, dass, dies auch im Einklang mit der Bestimmung in der EU, eine generelle Einwilligung für den Beizug von Sub-Auftragsdatenbearbeitenden und eine Information im konkreten Fall ausreicht.

8. Selbstregulierung

8.1. Empfehlungen der guten Praxis

Begrüssenswerte Selbstregulierung aber keine Empfehlungen des Beauftragten

Grundsätzlich sind Empfehlungen der guten Praxis in Anlehnung an das bestehende und bewährte Konzept der Selbstregulierung der Branchen zu begrüssen. Der wesentliche Vorteil liegt darin, dass so sehr knappe oder aber sehr komplexe gesetzliche Regelungen praxisnah und operativ umsetzbar präsentiert werden können. Dazu müssen themenspezifische Wünsche der Branche tatsächlich in die Regelung einfliessen. Die im VE-DSG vorgesehene Kompetenz des EDÖB, Empfehlungen der guten Praxis auf eigene Faust auszuarbeiten, widerspricht aber dem Zweck des Instituts. Es fehlen Kontrollen und Rechtsschutzmechanismen. Entsprechend besteht die Gefahr, dass der EDÖB «falsche» oder unverhältnismässige Empfehlungen im Alleingang, ohne institutionelle Kontrolle, verabschiedet. Aufgrund der Fiktion der Rechtmässigkeit von Art. 9 Abs. 1 VE-DSG würde er damit faktisch zum Gesetzgeber.

Dem stünde noch verschärfend entgegen, dass eigene Empfehlungen der interessierten Kreise nur mittels Genehmigung durch den EDÖB festgelegt werden könnten. Unter der DSGVO ist die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen.

Daraus ergibt sich, dass die Bestimmung der VE-DSG dahingehend anzupassen ist, dass die Initiative für Empfehlungen der guten Praxis stets zwingend von (Branchen)Verbänden ausgehen muss. Dies würde der Tradition der Selbstregulierung entsprechen und brächte den Vorteil mit sich, dass solche Richtlinien von Experten mit starkem Bezug zur Praxis verfasst werden. Dies würde es ermöglichen, sachgerechte Lösungen zu entwickeln, bei denen der Beauftragte durch die Genehmigung immer noch das letzte Wort hat. Die genehmigten Empfehlungen der guten Praxis sind vom EDÖB zu publizieren.

Vermutung der Richtigkeit statt Fiktion / Geltung auch für Auftragsdatenbearbeiter

Die Fiktion, welche von der Einhaltung der Empfehlungen auf die Einhaltung der Datenschutzvorschriften schliesst, ist ausserdem nicht zielführend. Es sind Konstellationen denkbar, die von den Empfehlungen nur unvollständig / unzureichend geregelt sind. Die Fiktion ist auf eine Vermutung der Richtigkeit zu reduzieren. Diese muss ebenfalls für den Auftragsdatenbearbeiter gelten.

8.2. Betrieblicher Datenschutzbeauftragter

Einführung auf freiwilliger Basis gekoppelt mit Freistellung von Meldepflichten

Der VE-DSG verlangt richtigerweise nicht die breite Einführung eines betrieblichen Datenschutzbeauftragten. Das Institut eines betrieblichen Datenschutzbeauftragten sollte aber wei-

terhin vorgesehen werden. Dies als Option für die Unternehmen kombiniert mit der Freistellung von allfälligen Meldepflichten gegenüber dem EDÖB (z.B. bei der Datenschutz-Folgenabschätzung). Ein betrieblicher Datenschutzbeauftragter könnte als zentrale Stelle die Pflichten für die Unternehmen oder ganze Unternehmensgruppen wahrnehmen. Damit liessen sich Doppelspurigkeiten vermeiden. Auch würde dadurch eine Anlaufstelle für Auskunftsbegehren geschaffen. Dies würde eine Flexibilisierung und gerade für grössere Unternehmen Erleichterungen mit sich bringen, ohne dass KMU belastet würden. Letztlich würde auch die Zugänglichkeit des Datenschutzes für die betroffene Person verbessert.

Die betrieblichen Datenschutzbeauftragen sind auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen (z.B. bei Art. 15, 16 und 17 VE-DSG). Die entsprechende Person darf jedoch im Rahmen von Sanktionen nicht übermässig exponiert werden (siehe hierzu unten, Ziff. 14.3).

9. Daten einer verstorbenen Person

Keine Regelung im DSG

Art. 12 VE-DSG erscheint im VE-DSG als Fremdkörper. Die Regelung könnte zu Rechtsunsicherheiten führen. Der Nachweis der persönlichen Beziehungen im Zusammenhang mit dem schutzwürdigen Interesse ist in der Praxis kaum zu erbringen. Für Geschäftsdaten bestehen gemäss spezialgesetzlichen Regelungen weitreichende legitime Dokumentations- und Archivierungspflichten, weshalb die pauschale Formulierung des Löschungsrechts nicht zielführend ist. Erben sind bereits durch die erbrechtliche Universalsukzession ausreichend legitimiert, geeignete, interessenwahrende Massnahmen vorzukehren. Die Bestimmung ist deshalb im VE-DSG zu streichen. Eine Regelung wäre an geeigneter Stelle (z.B. im ZGB) vorzusehen, dies aber zu einem späteren Zeitpunkt im Rahmen einer umfassenden Regelung in Bezug auf die Verfügung über Daten und nicht ausschliesslich aus einer datenschutzrechtlichen Sicht.

10. Pflichten

Keine pauschale Anwendung

Die pauschale Anwendung der vorgesehenen Pflichten auf alle Geschäftsmodelle und Branchen ist nicht sachgerecht und wäre mit enormem Aufwand verbunden. Es gilt, ein gestuftes Modell vorzusehen: Strengere Bestimmungen wären dabei für Geschäftsmodelle vorzusehen, welche besonders sensible Datenbearbeitungen umfassen, wie dies typischerweise bei spezifischen Marketing-Dienstleistern und Data-Minern der Fall ist. Auch bei den Pflichten ist ein risikobasierter Ansatz vorzukehren. Zudem können branchenspezifische Regelungen weitergehende Pflichten vorsehen.

Erleichterungen für Unternehmensgruppen

Gleich strenge Regelungen für die interne Weitergabe von Daten in Konzernverhältnissen sind nicht verhältnismässig. Analog Art. 47 DSGVO ist eine Bestimmung zu internen Datenschutzvorschriften für die erleichterte gruppeninterne Datenweitergabe in das DSG aufzunehmen. Dabei ist auch der Einsatz eines allfälligen internen Datenschutzbeauftragten (vgl. oben) zu berücksichtigen.

10.1. Informationspflichten

Risikobasierte Transparenzpflicht als Leitlinie

Die erweiterten Informationspflichten auf alle Personendaten bringen Mehraufwand und führen aufgrund des öffentlich-rechtlichen Charakters der Bestimmungen und den daraus fliessenden Sanktionsfolgen zu Problemen in der Praxis. Die vorgesehene massive Ausdehnung der Informationsmenge führt zu einer Überinformation der betroffenen Personen und würde sich damit kontraproduktiv auf die Transparenz auswirken. Die Regel muss grundsätzlich im Sinne einer risikobasierten Transparenzpflicht überarbeitet werden. Es sollte zudem explizit die Möglichkeit von standardisierten Informationen (z.B. mittels AGB oder Erklärungen auf Websites) eingeführt werden. Dies auch deshalb, weil oft nicht klar ist, worüber genau informiert werden muss.

Konkret ist die Informationspflicht auf besonders schützenswerte Daten und überdies auf Datenbearbeitungen ausserhalb des (objektiven) Erkennbarkeitshorizonts i.S.v. Art. 4 DSG der betroffenen Person zu beschränken. Ausserdem ist klarzustellen, dass sich die Information (und damit auch die Richtigkeit und Vollständigkeit der Daten) auf den Zeitpunkt der Datenbeschaffung bezieht und nicht auf nachträgliche Änderungen. Dies schliesst auch eine Pflicht zur Nachinformation klar aus. Als Kontaktdaten des Verantwortlichen muss eine klare und definierte Funktionsbeschreibung ausreichen, da die natürliche Person innerhalb einer Funktion wechseln kann.

Präzise und einheitliche Terminologien

Unklar ist die Differenzierung zwischen «Beschaffung» und «Bearbeitung» und die in Abs. 3 verwendeten Begriffe «Dritte» sowie «Empfängerinnen und Empfänger». Es sollten präzisere und einheitliche Terminologien verwendet werden. Es ist auch fraglich, warum der Vorentwurf den Begriff «Beschaffung» statt wie in der DSGVO vorgesehen «Erhebung» verwendet. Dadurch können sich (nachteilige) Abweichungen im Informationszeitpunkt ergeben.

Keine Mitteilung von Identität und Kontaktdaten der Auftragsdatenbearbeiter

Die Pflicht zur Mitteilung der Identität und der Kontaktdaten sämtlicher Auftragsdatenbearbeiter ist gegenüber dem EU-Recht klar überschiessend. Sie ist weder sinnvoll noch erforderlich. Die Offenlegung der oft für untergeordnete Tätigkeiten mandatierten Auftragsdatenbearbeiter ist nur mit unverhältnismässigem Aufwand zu bewerkstelligen und greift zudem in berechtigte eigene Datenschutzinteressen sowie Geschäftsgeheimnisse der Unternehmen ein. Schliesslich ist unklar, wann genau über was informiert werden muss. Die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben ist bereits Gegenstand von Art. 7 VE-DSG. Diese Zusatzanforderung ist zu streichen.

Keine Mitteilung bei indirekter Datenbeschaffung

Die vorgesehene Informationspflicht bei der indirekten Datenbeschaffung geht zu weit und verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Dem Verantwortlichen werden die relevanten Eckwerte, insbesondere die erstmalige Speicherung, oftmals gar nicht bekannt sein. Das Aufwand-Ertragsverhältnis ist damit unverhältnismässig. Darüber hinaus sind solche direkten Informationspflichten nicht erforderlich; eine allgemeine vorgängige Information des Kunden reicht aus. Die Bestimmung ist zu streichen.

Erweiterung und Präzisierung der Ausnahmen

Die Ausnahmebestimmung von Art. 14 Abs. 3 lit. a VE-DSG ist zu eng gefasst. Direkte Einschränkungen ergeben sich nur selten aus einem Gesetz. Häufiger sieht ein Gesetz zwingende Abklärungspflichten vor, welche mit Geheimhaltungspflichten verbunden sind und welche damit mit einer Einschränkung der Informationspflicht einhergehen. Die Bestimmung ist zu präzisieren und mit typischen Beispielen zu ergänzen (z.B. Abklärungen im Zusammenhang mit Geldwäscherei, Terrorismusbekämpfung und Korruption). Ausserdem können sich Verpflichtungen auch aus einem Vertrag ergeben. Eine weitere Ausnahme ergibt sich bei Datenbearbeitungen, die für eine Rechtsdurchsetzung erforderlich sind. Auch dies ist zu ergänzen.

Für die Einschränkung der Berufung auf überwiegende private Interessen, d.h. auf Fälle, in denen die Personendaten nicht Dritten bekannt gegeben werden, gibt es keine sachlichen Gründe. Besonders bei Konzernverhältnissen würde daraus ein enormer administrativer Mehraufwand resultieren. Sollte die betroffene Person durch die Bekanntgabe beeinträchtigt sein, so wäre dies im Rahmen der allgemeinen Interessensabwägung von Art. 24 VE-DSG zu berücksichtigen. Die Einschränkung ist damit zu streichen.

Die Bestimmung von Art. 14 Abs. 5 VE-DSG ist nicht praktikabel und zu streichen; diese würde dazu führen, dass ständig einzelne Interessensabwägungen überprüft werden müssten. In grossen, komplexen Organisationen ist dies nicht zu bewerkstelligen.

10.2. Automatisierte Einzelfallentscheide

Begrenzung des Anwendungsbereichs und der Pflichten; insb. keine Anhörungspflicht

Die Reichweite der neu eingeführten Informations- und Anhörungspflicht sowie Auskunftsrechte bei automatisierten Einzelfallentscheiden ist zu weitgehend. Zwar kennen die Konvention 108 und die EU eine entsprechende Regelung. Der Anwendungsbereich von Art. 15 VE-DSG ist jedoch viel breiter: Der VE-DSG unterscheidet stärker zwischen Profiling und automatisieren Einfallentscheiden und sieht auch keine Ausnahmen vor. Dies hat Folgen, welche so wohl nicht beabsichtigt waren: So wären beispielsweise Spam- und Virenscanner, Zugangskontrollen via Badge und sehr viele andere Routineentscheide erfasst, die aus Gründen der Effizienz dem Computer übertragen werden. Die Automatisierung ist ein zentraler Punkt der Digitalisierung und im heutigen wirtschaftlichen Umfeld von grundsätzlicher Bedeutung. Davon profitieren auch die Kunden, z.B. durch Objektivität der Entscheidung, schnellere Prozesse und damit besserer Nutzererfahrung sowie einer attraktiven Preisgestaltung.

Insbesondere das vorgesehene Äusserungsrecht der betroffenen Person bringt keinen Mehrwert; es ist angesichts der neu vorgesehen Informationspflicht auch schlicht unnötig und für die Unternehmen wettbewerbs- und innovationsbehindernd. In der Praxis würde es wohl regelmässig zu einer Begründungspflicht führen und damit die Vertragsfreiheit der Unternehmen über Gebühr einschränken. Die Offenlegung, wie bestimmte Entscheide zustande gekommen sind, betrifft zudem oft auch Geschäftsgeheimnisse.

Die Bestimmung ist entsprechend auf schwere Fälle, bzw. solche, die erhebliche Auswirkungen auf die Rechtstellung der betroffenen Person haben, zu begrenzen. Der Wortlaut ist an die entsprechende Bestimmung in der DSGVO anzupassen (insbesondere «Beeinträchtigung» statt «Wirkung» und «erhebliche» in Bezug auf beide Alternativen). Auch dann sind sinnvolle Ausnahmen notwendig, welche zumindest auf dem Verordnungsweg vorzusehen sind. Eine einmalige angemessene Information ohne ausdrückliche Einwilligung i.S.d. Gesetzessystematik ist ausreichend. Das Äusserungsrecht und der damit zusammenhängende Art.

20 Abs. 3 (Auskunftsrecht) sind zu streichen. Dies ist aufgrund des Derogationsrechts der Mitgliedstaaten der EU für die Äquivalenz nicht abträglich (vgl. Art. 22 Abs. 2 lit. c DSGVO).

10.3. Datenschutz-Folgenabschätzung

Beschränkung und Präzisierung / keine Pflicht des Auftragsdatenbearbeiters

Das in Art. 16 neu eingeführte Instrument der Datenschutz-Folgenabschätzung (Privacy Impact Assessment) ist zu weit gefasst. Die offene und dadurch unklare Formulierung führt dazu, dass für praktisch alle Datenbearbeitungen vorgängig aufwändige Abklärungen durchgeführt werden müssten. Besonders problematisch ist die vorgesehene Sanktionierung bei Verstoss. Analog der DSGVO ist eine Konkretisierung sowie Beschränkung auf Fälle vorzunehmen, bei denen ein *«hohes Risiko*» besteht bzw. ein solches nach vorgenommenen Massnahmen zur Risikominimierung *verbleibt*. Darüber hinaus ist zu präzisieren, dass ein Risiko für eine Persönlichkeitsverletzung bestehen muss. Der Begriff «oder die Grundrechte» ist sodann zu streichen: Das Schweizer Recht kennt, anders als das europäische Recht, keine direkte Drittwirkung der Grundrechte. Schliesslich ist der Auftragsdatenbearbeiter von der Pflicht auszunehmen. Dieser verfügt regelmässig nicht über die notwendigen Angaben, sondern unterliegt den Entscheidungen des Verantwortlichen.

Meldung nur bei *Rest*risiko und Verkürzung der Frist / Streichung der Meldepflicht

Die anschliessenden umfangreichen Meldepflichten sind ein klares «Swiss Finish»; sie sind unverhältnismässig und greifen in die Geheimsphäre der Unternehmen ein. Die zu erwartende «Meldeflut» ist für eine angemessene Reaktion des EDÖB kontraproduktiv. Problematisch ist auch die lange Frist, innert welcher der EDÖB Einwände mitteilen oder später eine Untersuchung einleiten kann. Damit werden falsche Anreize gesetzt. In der Gesamtheit bringt die Bestimmung keinen Mehrwert, führt jedoch zu erheblichen Rechtsunsicherheiten und innovationshemmenden Verzögerungen. Die Forderung der Konvention 108, bei geplanten Datenbearbeitungen Risiken einzuschätzen, wurde bereits durch Art. 11 VE-DSG (Datensicherheit) erfüllt. Schliesslich bestehen weitere Spezialregeln, welche bestimmte Datenflüsse bereits einer anderweitigen Überwachung unterstellen (z.B. im Bankengesetz). Doppelte Überwachungen sind aus Effizienzgründen zu vermeiden.

Eine Meldung an den EDÖB sollte nur dann erfolgen müssen, wenn *nach* ergriffenen Schutzmassnahmen ein grosses *Rest*risiko verbleibt. Es ist klar zu regeln, welche Informationen weitergeleitet werden müssen und wie damit bei Informationszugangsgesuchen nach dem Öffentlichkeitsgesetz umgegangen wird. Weiter ist die vorgesehene Reaktionszeit des EDÖB von drei Monaten, welche zudem laufend verlängert werden kann, auf einen Monat zu reduzieren.

Einige Mitglieder sprechen sich für die gänzliche Streichung der Meldepflicht und folglich auch von Art. 16 Abs. 4 VE-DESG aus. Eine Meldung solle erst erfolgen, wenn eine Verletzung des Datenschutzes passiert ist, nicht bereits aufgrund von Risiken. Auch die E-SEV 108 verlange nicht, die Behörden von der Datenschutz-Folgenabschätzung zu informieren. Eine Ausnahme der Meldepflicht sollte zumindest für Unternehmen mit einem betrieblichen Datenschutzbeauftragten vorgesehen werden.

10.4. Meldepflichten

Beschränkung auf Verstösse mit gravierenden Folgen

Die vorgesehene unverzügliche Meldepflicht im Falle sämtlicher Datenschutzverstösse (inkl. Datenverluste) an den EDÖB (*Data Breach Notification*) ist stark einzuschränken. Sie erfasst weit mehr Fälle als die DSGVO, welche diese Pflicht nur für Verletzungen von Sicherheitsmassnahmen vorsieht, die zusätzlich zu einem Bruch oder Verlust des Gewahrsams an den Daten führen. Zudem kann die vorgesehene Ausnahme sachlogisch nie angerufen werden, da eine «falsche» Datenbearbeitung per Definition immer eine Verletzung von Persönlichkeitsrechten ist.

Eine Pflicht ohne Eingrenzung in qualitativer und quantitativer Weise würde uferlos; jeder noch so geringe Verstoss müsste gemeldet werden, um den Sanktionsfolgen zu entgehen. Der Beauftragte sähe sich mit einer weiteren Meldungsflut konfrontiert und wäre ausser Stande, allfällig wichtige Meldungen zeitgerecht zu erkennen und geeignete Massnahmen einzuleiten. Die Meldepflicht führt auch zu einem Konflikt mit dem strafrechtlichen Grundprinzip von «*nemo tenetur*»[2]. Schliesslich wäre eine «unverzügliche» Meldung auch in zeitlicher Hinsicht nicht umsetzbar, da zuerst hinreichende Informationen gesammelt werden müssen. Zudem besteht die Gefahr, durch vorschnelles Handeln Geschäfts- oder Berufsgeheimnisse zu verletzen. So sieht die DSGVO eine Frist von bis zu 72 Stunden vor.

Der Begriff des «Data Breach» sollte analog E-SEV und DSGVO formuliert werden. Die Pflicht wäre damit auf Verstösse mit gravierenden Folgen zu beschränken, bei welchen ein Kontrollverlust an den Daten vorliegt. Als weiteres qualitatives Kriterium müsste die Tatsache ergänzt werden, dass durch die Meldung an den Beauftragten ein Mehrwert geschaffen werden kann. Dies z.B. mittels Unterstützung in Fällen, welche von den Verantwortlichen nicht mehr aus eigener Kraft bereinigt werden können. Weiter ist die Bestimmung durch ein quantitatives Element zu konkretisieren, z.B. auf Fälle, in welchen Daten von mindestens 100'000 Personen betroffen sind. Eine Meldung beim EDÖB muss den Schutz vor Sanktionen zur Folge haben (vgl. nachfolgend Ziff. 14.3).

10.5. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Anpassung der Reichweite und Überführung zu den Sicherheitsbestimmungen

Die Formulierung von Art. 18 VE-DSG geht ebenfalls über jene der DSGVO hinaus. Zudem gehört diese systematisch zu Art. 11 VE-DSG (Sicherheit von Personendaten). Diese Bestimmung deckt die Anforderungen von «privacy by design» bereits. Art. 18 VE-DSG ist zu streichen, resp. in Art. 11 zu integrieren. Die Reichweite ist an das EU-Recht anzupassen.

10.6. Weitere Pflichten

Verzeichnis statt allgemeine Dokumentationspflicht / Ausnahme für kleinere Unternehmen

Die allgemeine Dokumentationspflicht von Art. 19 lit. a VE-DSG ist bezüglich Inhalt und Umfang unklar und geht über die vergleichbare Bestimmung der EU hinaus. Die Pflicht ist analog der DSGVO auf die Pflicht zur Erstellung «eines Verzeichnisses für regelmässige Datenbearbeitungen» einzuschränken. Die Pflicht, Datenschutzverstösse zu dokumentieren, ist zu weitgehend. Darüber hinaus ist auch eine Ausnahme der Pflicht für kleinere Unternehmen (z.B. analog EU mit weniger als 250 Mitarbeitenden oder am Umsatz gemessen) vorzusehen, so-

[2] Vgl. mehr dazu unter „Aufsicht und Sanktionen“.

fern sie in Bezug auf den Datenschutz keine risikoreiche Tätigkeit ausüben. Aus systematischen Gründen sollte auch diese Bestimmung in Art. 11 VE-DSG integriert werden.

Beschränkung der Informationspflicht an Dritte

Die Reichweite der neu vorgesehenen Pflicht, Dritten die Berichtigung, Löschung oder Vernichtung von Daten zu melden, geht sehr weit und ist in der Praxis nicht umsetzbar. Eine solche Meldepflicht ist von E-SEV 108 nicht und von der DSGVO nicht in dieser Form vorgesehen. Die DSGVO kennt eine entsprechende Meldepflicht nur unter gewissen Voraussetzungen im Zusammenhang mit dem «Recht auf Vergessen». Der VE-DSG erfasst demgegenüber auch unbedeutende Vorgänge; im täglichen Arbeitsprozess werden ständig Daten berichtigt, gelöscht oder vernichtet (z.B., weil ein Kunde bezahlt hat oder die Daten schlicht keine Relevanz mehr haben). Die Auswirkungen dieser Meldepflicht wurden offenbar unterschätzt. Zu deren Bewältigung müsste eine neue Infrastruktur aufgebaut werden, welche sämtliche Empfänger über Jahrzehnte hinweg verwaltet. Eine betroffene Person ist besser in der Lage zu beurteilen, welche Daten für welche Empfänger (noch) von Interesse sind. Gerade solche Informationsansprüche der betroffenen Person sind aber bereits unter Art. 25 VE-DSG vorgesehen. Die Informationspflicht an Dritte ist analog der DSGVO auf Fälle zu beschränken, in welchen die betroffene Person die Nachinformation aus berechtigten Gründen verlangt hat.

11. Auskunftsrecht

Massnahmen gegen missbräuchliche Auskunftsbegehren

Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen und hängige Verfahren bringt grosse Aufwendungen mit sich. Umso mehr, weil ein Auskunftsbegehren im Datenschutzsystem der Schweiz nie unverhältnismässig sein kann, da auch untergeordnete Datenschutzinteressen für einen Anspruch ausreichen. Gerade auch die vorgesehene umfassende Kostenlosigkeit des Auskunftsrechts führt zu Fehlanreizen: Es sind keine Massnahmen vorgesehen, welche es den Unternehmen erlauben würden, dem Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken Einhalt zu gebieten (vgl. Ziff. 3).

Es sind griffige Massnahmen gegen den Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken vorzusehen: Die Kostenlosigkeit ist wie in Art. 2 VDSG zu relativieren, so z.B. bei unverhältnismässigem Aufwand und bei Ersuchen zu nicht ausschliesslich datenschutzrechtlichen Zwecken. Zudem sind weitere Mechanismen zur Verhinderung des Auskunftsrechts bei offensichtlich nicht datenschutzrechtlichen Zwecken vorzusehen (z.B. bei Art. 21 VE-DSG).

Deutliche Einschränkung der Informationspflicht bei automatisierten Einzelfallentscheiden

Eine «Rechenschaftspflicht» in Bezug auf automatisierte Entscheide in der vorgesehenen detaillierten Form ist unverhältnismässig: Informationen darüber, wie bestimmte Entscheide zustande kommen, gehören zum Geschäftsgeheimnis. Durch die gewählte Formulierung wäre jedes Ergebnis, d.h. jeder Entscheid erfasst. Dies würde zu einem zusätzlichen Administrativaufwand führen, ohne dass damit mehr Transparenz geschaffen würde. Im Gegenteil: Kunden würden Informationen erhalten, mit denen sie gar nichts anzufangen wissen (z.B. warum sie eine Werbeanzeige nicht erhalten haben).

Die geforderte Information über Vorliegen einer automatisierten Einzelfallentscheidung (Art. 20 Abs. 2 lit. e VE-DSG) sollte in allgemeiner Weise erfolgen. Die Bestimmung von Art. 20 Abs. 3 VE-DSG sollte in Art. 15 VE-DSG integriert werden. Dessen Grundsätze («erhebliche

Auswirkung») wären dabei einzuhalten. Es muss klargestellt werden, dass das Auskunftsrecht nur von der jeweils tatsächlich betroffenen Person ausgeübt werden kann. Zudem ist ein Verweis auf die Einschränkungen des Auskunftsrechts bzw. der Informationspflichten (Art. 21 i.V.m. 14 VE-DSG) anzubringen.

12. Ausnahmetatbestände

Ausweitung der Ausnahmen

Die vorgesehenen Ausnahmetatbestände gemäss Art. 14 VE-DSG sind zu eng formuliert und nicht konsistent. Die Informationspflicht sollte immer entfallen, wenn die Information nicht möglich oder unzumutbar ist. Eine Beschränkung auf Fälle der indirekten Beschaffung oder in denen keine Weitergabe an Dritte erfolgte ist nicht nachvollziehbar. Die Bestimmung ist entsprechend anzupassen.

Es sind Ausnahmen, auch in Hinblick auf die rechtsmissbräuchliche Geltendmachung des Auskunftsrechts, für folgende bearbeiteten Daten vorzusehen:

- Daten, welche die betroffene Person bereits erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen;
- Aufgrund einer gesetzlichen Pflicht bearbeitete Daten, z.B. zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption;
- Daten, welche vom Auskunftspflichtigen als Geschäftsgeheimnisse qualifiziert werden;
- Rein intern bearbeitete Daten;
- Daten über Drittpersonen;
- Unter rechtsmissbräuchlichen Umständen herausverlangte Daten, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder mit häufiger, sachlich nicht nachvollziehbarer Wiederholung.

Übergabe der Informationen an Dritte bei Missbrauchsverdacht

Um Missbräuche zu verhindern, ist zudem vorzusehen, dass bei begründetem Verdacht auf Missbrauch die herauszugebenden Personendaten einem Dritten (bspw. dem EDÖB) übergeben werden können. Dieser würde anstelle des Gesuchstellers die Einhaltung bzw. Verletzung des Datenschutzes prüfen. Eine Möglichkeit bestünde darin, dass der EDÖB den Entscheid über Herausgabe in Form einer anfechtbaren Verfügung vorlegt (vgl. analoge Regelung in Art. 8 Abs. 2 BPI).

13. Besondere Bestimmungen für die Datenbearbeitung durch private Personen

Keine ausdrückliche Einwilligung beim Profiling

Gemäss Art. 23 Abs. 2 lit. d VE-DSG gälte Profiling automatisch als Persönlichkeitsverletzung, wenn nicht vorgängig eine ausdrückliche Einwilligung eingeholt wird. Diese gesetzliche Vermutung stellt einen unbegründeten partiellen Paradigmenwechsel im Schweizer Datenschutzrecht dar (von grundsätzlicher Erlaubnis der Datenbearbeitung unter Einhaltung bestimmter Voraussetzungen zum Verbot mit Erlaubnisvorbehalt). Das Erfordernis der ausdrücklichen Einwilligung beim Profiling ist entsprechend zu streichen. Durch eine entsprechende Information kann genug Transparenz geschaffen werden. Eine Regelung hat unter Art. 15 VE-DSG zu erfolgen.

Klare und erweiterte Rechtfertigungsgründe

Der Ausdruck «möglicherweise» in Art. 24 Abs. 2 VE-DSG schafft Rechtsunsicherheit. Die aktuelle Bestimmung (Art. 13 Abs. 2 DSG) wurde unnötigerweise geändert und sollte beibehalten werden.

Art. 24 Abs. 2 lit. a VE-DSG sollte analog Art. 6 Abs. 1 lit. b VE-DSG Verträge berücksichtigen, die zu Gunsten oder im Interesse der betroffenen Person geschlossen werden.

14. Aufsicht und Sanktionen

Das vorgeschlagene Sanktionsmodell wurde in unserer internen Vernehmlassung breit kritisiert. Angesichts dieser Kritik und der Bedeutung der Thematik für die Schweizer Wirtschaft wird zum Thema Aufsicht und Sanktionen in detaillierterer Form Stellung genommen. Zudem präsentieren wir im Folgenden eine Grobskizze für einen alternativen Vorschlag für ein im Datenschutzgesetz zu integrierendes Sanktionsmodell.

Verschiedene Fachspezialisten aus der Wirtschaft sind gerne bereit, den Lösungsansatz zusammen mit weiteren interessierten Kreisen, beispielsweise im Rahmen einer vom Bundesamt für Justiz angelegten Arbeitsgruppe, zu vertiefen und eine ausgearbeitete Lösung zu entwickeln.

14.1. Ausgangslage

Anders als der VE-DSG setzen die Konvention 108 und die EU-Verordnung in erster Linie auf Verwaltungssanktionen gegen Unternehmen. Bei der Regelung der Sanktionierung von Datenschutzverletzungen besteht gemäss den europäischen Bestimmungen ein erheblicher Spielraum: Die Konvention verlangt im Wesentlichen *geeignete gerichtliche und nicht-gerichtliche Sanktionen und Rechtsmittel* (Art. 10 E-SEV 108). Die DSGVO (und auch die Richtlinie) sprechen von *wirksamen, verhältnismässigen und abschreckenden Sanktionen.* Es ist dabei den Mitgliedsstaaten überlassen zu entscheiden, ob Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind (Erw. 149 und 152).

14.2. Kritik am Vorentwurf und weitere Überlegungen

Die Wirtschaft ist bei der Abwägung verschiedener Sanktionsmodelle zum Schluss gekommen, dass die im VE-DSG vorgesehenen Sanktionen und insbesondere der Weg über das Strafrecht nicht zielführend sind:

Persönliche Strafbarkeit der Mitarbeitenden

Die Mitarbeitenden eines Unternehmens geraten durch die persönliche Strafbarkeit zu stark in den Fokus der Sanktionen. Verschärft wird dies durch die Höhe der Bussen und die vorgesehene Möglichkeit, sogar fahrlässiges Handeln zu bestrafen. Damit wird der risikobasierte Ansatz, der mit der Revision verfolgt wird, untergraben.

Strafrechtliche Sanktionen führen dazu, dass Mitarbeitende in Zukunft selbständig jeden (möglichen) Verstoss bei den Behörden melden müssen. Dies birgt das Risiko, dass sie sich gegenseitig anzeigen, um nicht selbst ins Visier der Strafbehörde zu geraten. Der VE-DSG bietet zudem Dritten viele Anknüpfungspunkte (sobald eine Datenerhebung stattgefunden hat), um Anzeige zu erstatten. Dies kann zum Unterlaufen der intern definierten Datenschutz-Governance und zu Unruhen innerhalb der Unternehmen führen sowie entsprechende Reputationsschäden nach sich ziehen. Entsprechende Meldungen bergen ausserdem die Gefahr, selbst wiederum zu Verletzungen des Datenschutzes zu führen.

Verurteilte Mitarbeitende wären sowohl intern als auch extern stark exponiert. Es dürfte daher mittelfristig schwierig werden, qualifiziertes Personal zu finden, das bereit ist, die Verantwortung mit den einhergehenden Risiken zu tragen. Die Folge wäre ein sukzessives Abfallen der Qualität im Bereich der Datenbearbeitung.

Die persönliche Strafbarkeit der Mitarbeitenden entspricht auch nicht der von anderen Schweizer Gesetzen vorgesehen Linie (vgl. KG, UWG, FMG, BEHG), bei welchen der Fokus klar auf der Sanktionierung der Unternehmen liegt.

Die strafrechtliche Sanktionierung würde schliesslich insbesondere die KMU stark belasten. Bei übersichtlichen Verhältnissen ist die Identifikation fehlbarer Mitarbeitenden relativ einfach; entsprechend bestünde ein Anreiz für die Strafverfolgungsbehörden, gerade bei solchen Unternehmen unverhältnismässig streng vorzugehen.

Verstoss gegen strafrechtliche Grundprinzipien

Problematisch sind die im VE-DSG vorgesehenen Mitwirkungspflichten angesichts des im Strafrecht vorherrschenden Grundsatzes des «*nemo tenetur*» bzw. des Selbstbelastungsverbotes. Die Pflicht, Datenschutzverstösse zu melden, käme faktisch einer Pflicht zur Selbstanzeige gleich. Der VE-DSG geht von einer verschuldensunabhängigen Sanktionierung aus und steht damit im Widerspruch zum Verschuldensprinzip: Bei Vorliegen des objektiven Tatbestandes wird direkt darauf geschlossen, dass auch der subjektive Tatbestand erfüllt ist. Viele der Pflichten des VE-DSG und damit auch die daraus abgeleiteten Straftatbestände sind offen formuliert (vgl. Art. 16 Abs. 1 VE-DSG: *"…vorgesehene Datenbearbeitung [führt] voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person*"). Dies ist mit dem strafrechtlichen Bestimmtheitsgebot bzw. einer hinreichenden Voraussehbarkeit einer Strafbarkeit nicht vereinbar.

Umfang von potentiellen Verstössen und Meldungen

Datenbearbeitungen stellen innerhalb der Unternehmen eine alltägliche Aktivität dar. Unternehmen können im Zeitalter der Digitalisierung nicht mehr wählen, ob eine entsprechende Handlung vorzunehmen ist oder nicht. Damit unterscheidet sich das Datenschutzrecht beispielsweise vom Kartellrecht. Im VE-DSG sind kaum Erheblichkeitsschwellen vorgesehen. Folglich würde jede geringfügige Unregelmässigkeit in alltäglichen Datenbearbeitungsvorgängen eine Datenschutzverletzung darstellen. Die daraus resultierende Mitteilungsmenge an den Beauftragten sowie die drastischen Sanktionsfolgen wären höchst problematisch.

Strafkatalog

Im Kern entspricht der Strafkatalog grundsätzlich den europäischen Bestimmungen. Hingegen werden die Berufspflichten erheblich verschärft und es wird sogar eine Freiheitsstrafe als Sanktion vorgesehen. Diese Ausweitung des Berufsgeheimnisses ist als überschiessende Bestimmung klar abzulehnen; es können in dieser Hinsicht nicht alle Berufe mit jenen von Art. 321 StGB gleichgesetzt werden.

Fazit

Die strafrechtlichen Sanktionen des VE-DSG, die gegen Mitarbeiter eines Unternehmens ausgesprochen werden können, sind weder verhältnismässig noch zielführend. Diese stehen im Widerspruch zu einer Vielzahl von schweizerischen strafprozessualen Prinzipen. Die auf Risikoausgleich ausgerichteten Möglichkeiten des VE-DSG werden damit ausgehöhlt und der Interessensausgleich wird unnötig eingeschränkt. Gesamthaft geht das vorgeschlagene straf-

rechtliche Sanktionsmodell damit deutlich über die im europäischen Raum vorgesehenen Sanktionen, die in erster Linie verwaltungsrechtlicher Natur sind, hinaus.

14.3. Vorschlag der Wirtschaft für ein mögliches Sanktionsmodell im DSG (Grundlage)

Aufgrund der vorangehenden Überlegungen sprechen wir uns für ein alternatives Sanktionsmodell aus. Nicht strafrechtliche Sanktionen gegen Individuen, sondern Verwaltungsstrafen gegen Unternehmen sollen dabei im Vordergrund stehen (vgl. Anhang).

Auch bei Verwaltungsstrafen ergeben sich verschiedene Problemfelder, gerade auch aus rechtsstaatlicher Sicht. Das nachfolgend skizzierte Modell berücksichtigt diese und schlägt ein auf die spezielle Konstellation des Datenschutzes angepasstes, verwaltungsrechtliches Sanktionsmodell vor. Dieses soll effizient ausgestaltet sein, die richtigen Anreize setzen und den Anforderungen an ein faires Verfahren entsprechen.

Die einzelnen Regeln dieses Verwaltungsverfahrens müssen den besonderen Verhältnissen bei Verletzungen des Datenschutzgesetzes entsprechend ausgestaltet werden und dürfen wegen den unterschiedlichen in Frage stehenden Rechtsgütern nicht einfach analog aus dem Kartellgesetz übernommen werden (insbesondere bezüglich der Sanktionen).

<u>Grundsatz: verwaltungsrechtliche Sanktionen gegen Unternehmen</u>

Das DSG soll bei Verstössen gegen die Datenschutzbestimmungen eine Sanktionierung der Unternehmen vorsehen. Anknüpfungspunkt sind dabei Organisationsmängel im Unternehmen. Lediglich subsidiär soll eine strafrechtliche Verfolgung von Mitarbeitenden möglich sein. Anzeigen sollen in der Regel durch die Unternehmen selbst erstattet werden. Im Ergebnis würde eine Anpassung des Sanktionsziels die Situation für die Datenbearbeitenden im Sinne einer Verbesserung des Datenschutzes im Unternehmen massgeblich entschärfen.

Weiter soll eine Sanktionierung der Mitarbeitenden nur bei direkt vorsätzlichem Handeln, das sich gegen die Interessen des Unternehmens und/oder der betroffenen Person richtet, in Frage kommen. In diesem Zusammenhang ist eine Abstimmung mit den bereits im BT StGB vorgesehenen Strafbestimmungen erforderlich. Diese dürften für die Bestrafung der natürlichen Person meist schon ausreichen (z.B. Verletzung des Geschäftsgeheimnisses und unbefugte Datenbeschaffung). Der Kreis der potentiell strafrechtlich verantwortlichen Mitarbeitenden müsste zum Vornherein eingeschränkt werden (entsprechend Art. 29 StGB).

<u>Angepasste Rolle des EDÖB und verbesserte Gewaltentrennung durch eine neu zu bildende Spruchbehörde</u>

Eine Behörde, die gleichzeitig über Untersuchungs- und Spruchkompetenzen verfügt (wie bei Sanktionen mit verwaltungsrechtlichem Charakter üblich), hat die Tendenz, eine mit dem Prinzip der Gewaltenteilung nur schwer vereinbare Machtfülle zu erlangen. Die Verwaltungssanktionen sollten daher nicht von der Untersuchungsbehörde verhängt werden.

Die Ausstattung des EDÖB mit Spruchkompetenzen, sogar die im VE-DSG bereits vorgesehene Ausstattung mit Verfügungskompetenzen, kann dazu führen, dass der EDÖB zu mächtig wird. Zusätzlich besteht die Gefahr, dass eine vertrauensvolle Zusammenarbeit mit den Unternehmen im Bereich der wichtigen Beratung beeinträchtigt wird. Ein auf Vertrauen basierender Austausch mit den Unternehmen ist für die Tätigkeit des Beauftragten jedoch von grundsätzlicher Bedeutung, dies umso mehr, als ihm gemäss VE-DSG die Aufgabe zukommt, Empfehlungen der guten Praxis zu erlassen.

Die Verfügungskompetenzen sowie die Sanktionskompetenz könnten entsprechend in einer neu zu bildenden «Datenschutz-Kommission» gebündelt werden. Diese könnte beispielsweise dem EDI oder EJPD angehängt sein. Ausschliesslich dieser kämen nebst der Sanktionskompetenz auch die Verfügungskompetenzen zu, dies gerade auch im Bereich vorsorglicher Massnahmen. Das Verhältnis zwischen «Datenschutz-Kommission» und EDÖB müsste präzisiert werden, insbesondere in Bezug auf die Überwachungs- und Untersuchungskompetenzen des Beauftragten i.S.v. Art. 40 f. VE-DSG. Als Alternative könnte auch der Weg über ein Gericht, z.B. am Sitz des EDÖB, geprüft werden (vgl. Verfahren in Kartellfragen in Deutschland).

In dieser Struktur würde der EDÖB seine bisherigen Aufgaben wahrnehmen und eine Vorselektion der ihm zugetragenen Fälle machen. Sollte sich in einem Fall eine mögliche Strafbarkeit abzeichnen, würde er die Angelegenheit der «Datenschutz-Kommission» weiterleiten. Bei Verfahren auf dieser zweiten Stufe würde die verwaltungsrechtliche Mitwirkungspflicht des Beauftragten wegfallen. Gegen Entscheide dieser Spruchbehörde stünde den Betroffenen der Weg zum Bundesverwaltungsgericht als Rechtsmittelinstanz offen.

Strafkatalog

Der Strafkatalog ist mit jenem der DSGVO abzugleichen, soll jedoch nicht darüber hinausgehen. Folgende Anpassungen sind erforderlich:

- Konkretisierung / Streichung der zu offen formulierten Tatbestände;
- Beschränkungen und Anpassungen bei den Pflichten der Verantwortlichen und Auftragsbearbeiter sind beim Strafkatalog zu berücksichtigen;
- Fokus auf wesentliche Bedrohung für die Privatsphäre der betroffenen Person;
- Einführung einer Erheblichkeitsschwelle, welche sich z.B. an der Schwere der Persönlichkeitsverletzung (in quantitativer oder qualitativer Hinsicht) oder an der Höhe des entstandenen Schadens in Bezug auf die betroffene Person orientiert. Zu einem schweren Verstoss gegen das Datenschutzgesetz gehört auch, dass die unbefugte Datenbearbeitung vorsätzlich vorgenommen wurde;
- Verzicht auf die Pönalisierung von reinen Fahrlässigkeitsdelikten;
- Streichung der Strafandrohung bei verweigerter Mitwirkung / Kooperation ab 2. Stufe des Verfahrens (siehe unten);
- Beschränkung der beruflichen Schweigepflicht auf Fälle, in denen die betroffene Person eine berechtigte Erwartung der Geheimhaltung hat (z.B. aufgrund eines Vertrages). Angeregt wurde auch, den heutigen Art. 35 DSG beizubehalten oder diese Bestimmung ins StGB zu übertragen.

Mitwirkungspflichten und Rechtfertigungs- und Strafmilderungsgründe

Neben der im Vorentwurf vorgesehenen Pflicht, Datenschutzverstösse bei den Behörden zu melden, besteht für die Unternehmen im verwaltungsrechtlichen Verfahren generell eine Mitwirkungspflicht. Wie oben kritisiert, läuft die Idee der anschliessenden Bestrafung im Rahmen eines Strafverfahrens diesem Konzept entgegen und verstösst zusätzlich gegen das Selbstbelastungsverbot. Ein kooperatives Verhalten, das letztlich einer raschen Schadensminderung dienen soll, muss gefördert werden. Unternehmen, die den Beauftragten über eine Verletzung der Datenschutzbestimmungen informieren, mit den Behörden kooperieren, Fehler aktiv korrigieren und grössere Risiken zu verhindern suchen, sollen mit einer Reduktion der Sanktion oder gar dem Absehen von einer Sanktion rechnen können (vgl. auch Art. 49a Abs. 2 KG). Dieser auf Schadensminderung ausgerichtete Ansatz entspricht den modernen Grundsätzen der Corporate Governance und fördert gleichzeitig das Ziel, ein hohes Datenschutzniveau zu erreichen. Gründe, die rechtfertigend oder zumindest strafmildernd wirken sollten, wären:

- Compliance-Defense: Implementierung eines tauglichen Compliance-Programmes;
- Einhaltung der Corporate Governance: Einhalten sämtlicher unternehmensinternen Richtlinien, Ausschöpfen der betriebsinternen Eskalationsleiter und Interventionsmöglichkeiten, Meldung eines möglichen Verstosses sowie kooperatives Verhalten gegenüber den Behörden;
- Handeln nach Treu & Glauben durch vernünftigen Umgang mit komplexen Regeln: Angemessene Umsetzung komplexer Verhältnisse (z.B. viele Beteiligte und grenzüberschreitende Verhältnisse) unter Berücksichtigung des «state of the art»;
- Wahrung berechtigter Interessen: Güterabwägung im Fall von Pflichtenkollision mit anderen zwingenden Rechtsregeln (z.B. unter Zeitdruck angewendete etablierte Notfallszenarien (BCM) im öffentlichen Interesse zur Abwendung eines Unternehmenskonkurses; vgl. Notstand, Art. 17 StGB);
- Rechts- und Sachverhaltsirrtum (vgl. Art. 13 und 21 StGB);
- Strafrechtliche Verfolgung eines Mitarbeitenden. Eine Anzeige gegen einen direktvorsätzlich handelnden Mitarbeitenden durch das Unternehmen muss im Rahmen der Bestrafung des Unternehmens, insbesondere im Hinblick auf das Schuldprinzip, berücksichtigt werden;
- Aktive Schadensverminderung und Zusammenarbeit mit den Behörden.

Sanktionen

Datenbearbeitungen gehören zur täglichen Arbeit der Unternehmen. Datenschutzverletzungen können dementsprechend im Rahmen des Tagesgeschäftes geschehen. Dies muss bei der Festlegung der Sanktionshöhe einen Einfluss haben. Keinesfalls dürfen umsatzorientierte Ansätze zur Anwendung kommen. Dies wäre nicht sachgerecht, da Verletzungen des Datenschutzgesetzes kaum je in der Absicht erfolgen, den Umsatz oder Gewinn des Unternehmens zu erhöhen (anders als z.B. bei Kartellabsprachen). Deshalb ist eine maximale Obergrenze von CHF 500’000 für Bussen zu setzen. Zudem sind bei der Festlegung der Bussenhöhe die gesamten Umstände des Einzelfalles zu berücksichtigen, so z.B. die Schwere und die Auswirkungen des Verstosses sowie die oben genannten Rechtfertigungs- und Strafmilderungsgründe. Ebenso muss, in Anlehnung an die DSGVO, eine Konkurrenzklausel eingefügt werden: Bei gleichen oder miteinander verbundenen Datenbearbeitungsvorgängen, durch die vorsätzlich mehrere Bestimmungen des VE-DSG verletzt wurden, darf der Gesamtbetrag der Busse nicht denjenigen Betrag übersteigen, der für die schwerwiegendste Verletzung vorgesehen ist.

15. Übergangsfristen

Im VE-DSG fehlt eine umfassende Übergangsregelung. Die neuen und revidierten Bestimmungen werden die Prozesse der Unternehmen bedeutend beeinflussen. Es ist deshalb eine allgemeingültige Übergangsbestimmung von 2 Jahren aufzunehmen. Von einer Rückwirkung ist abzusehen.

C. Beurteilung der vorgesehenen Ratifizierung des Änderungsprotokolls zum Datenschutzübereinkommen des Europarats SEV 108

Europa nimmt beim Datenschutz traditionell eine Vorreiterrolle ein. Bereits 1981 verabschiedete der Europarat mit dem Übereinkommen vom 28. Januar 198128 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten («Übereinkommen SEV 108») den ersten völkerrechtlichen Vertrag im Bereich des Datenschutzes. Als die Schweiz in der ersten Hälfte der neunziger Jahre sein erstes Datenschutzgesetz entwickelte, diente das Übereinkommen SEV 108 als wichtigstes Referenzwerk und unser Land kam dadurch auch in die Lage, dem Übereinkommen 1997 formell beizutreten.

Die digitale Transformation hat nun weltweit den Bedarf gezeigt, die noch aus den Anfängen der Computerzeit stammenden Konzepte zum Schutz des Individuums vor übermässiger Datenbearbeitung zu hinterfragen. So überarbeitet der Europarat die auch von der Schweiz ratifizierte "Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" (Datenschutzkonvention Nr. 108) grundlegend. Im Jahr 2011 leitete der Europarat dazu ein Verfahren zur Revision des Übereinkommens SEV 108 und seines Zusatzprotokolls ein. Damit sollen die Herausforderungen für den Schutz der Privatsphäre und der Grundrechte der betroffenen Personen, welche die Globalisierung, die technologischen Entwicklungen und die Zunahme des grenzüberschreitenden Datenverkehrs mit sich bringen, besser bewältigt werden können. Daraus resultiert nun ein Modernisierungsentwurf, der nach unserer Kenntnis zwar zum aktuellen Zeitpunkt formell noch nicht verabschiedet und deshalb auch einer Ratifizierung durch die Schweiz ebenfalls formell noch nicht zugänglich ist. In inhaltlicher Hinsicht bildet der Modernisierungsentwurf im jetzigen Status aber einen europäischen Konsens über die derzeit angemessenen Datenschutzprinzipien so vollständig ab, dass er als Fundament einer ebenfalls zu modernisierenden schweizerischen Datenschutzgesetzgebung nicht zu umgehen ist.

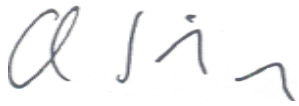
Auch im Hinblick auf die anzustrebende Äquivalenz mit der EU-Regulierung ist eine künftige Ratifizierung angezeigt, wird diese doch nicht nur als fast unabdingbares Kriterium bei der Prüfung der Äquivalenz seitens der EU ausdrücklich erwähnt (vgl. Erw. 105 DSGVO), sondern ermöglicht es auch der Schweiz im Rahmen des Begleitkommitees zum Übereinkommen direkt die gesamteuropäische Rechtsentwicklung im Datenschutzbereich mitzubeeinflussen.

Der Ratifikation der von der Schweiz bereits bisher ratifizierten "Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" (Datenschutzkonvention SEV 108) in der aktuell bekannten modernisierten Form ist deshalb grundsätzlich zuzustimmen.

Wir danken Ihnen, sehr geehrte Frau Bundesrätin, für die wohlwollende Prüfung unserer Anliegen.

Mit freundlichen Grüssen

SwissHoldings
Geschäftsstelle

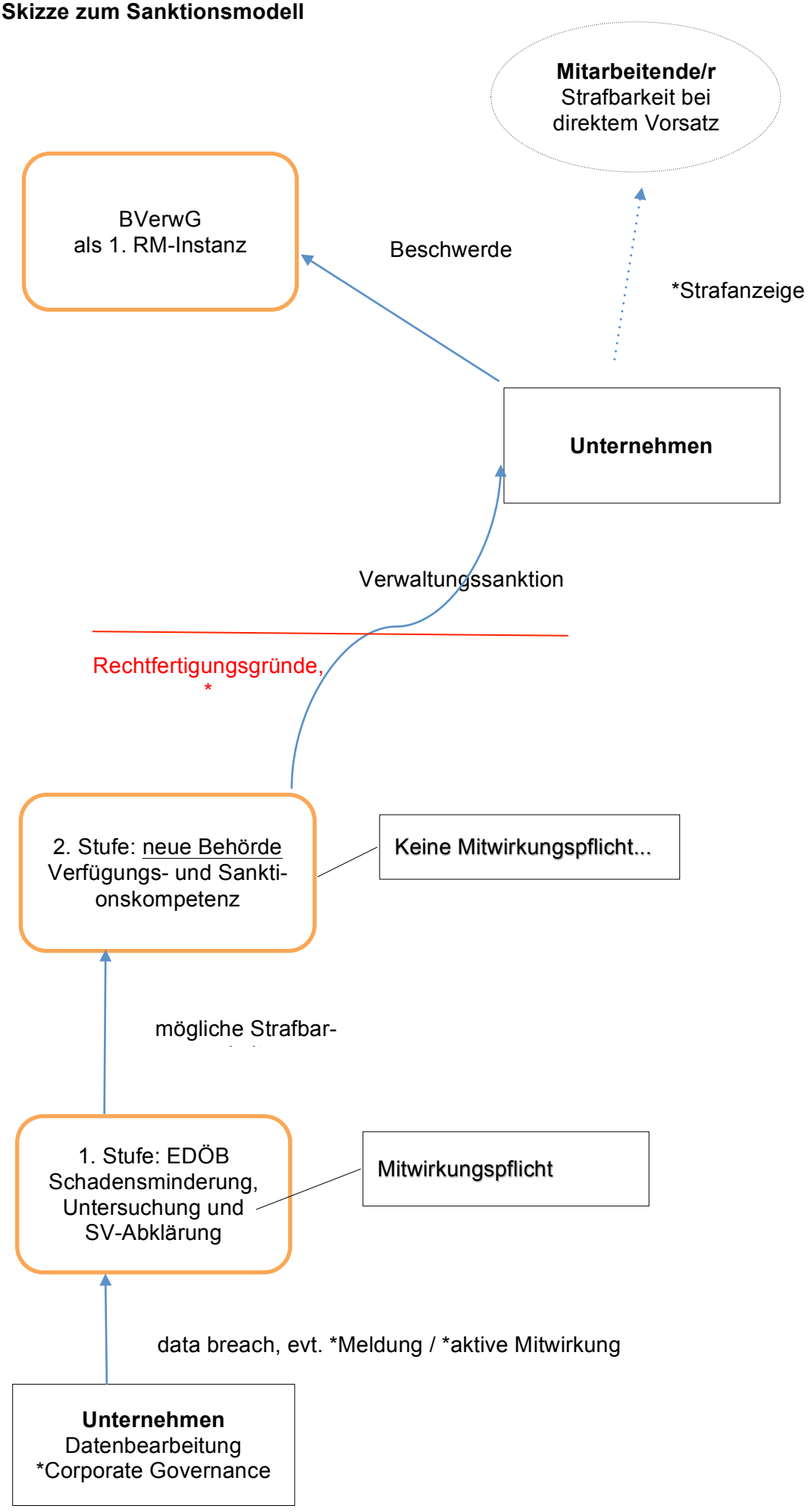


Christian Stiefel
Vorsitzender der Geschäftsleitung

Jacques Beglinger
Mitglied der Geschäftsleitung

cc – SH-Vorstand

Anhang: Skizze zum Sanktionsmodell



Amstutz Jonas BJ

Von:	Simon Zaugg <Simon.Zaugg@swissict.ch>
Gesendet:	Dienstag, 4. April 2017 16:11
An:	Amstutz Jonas BJ
Cc:	delacruz@delacruzberanek.com; Thomas Flatt
Betreff:	swissICT Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)
Anlagen:	170330 Vernehmlassung swissICT.docx

Sehr geehrter Herr Amstutz,

Ich nehme Bezug auf die offene Vernehmlassung zum **Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz** unter https://www.admin.ch/ch/d/gg/pc/pendent.html

swissICT reicht hierzu die angehängte Stellungnahme ein.

Ich danke Ihnen für die Kenntnisnahme.

Freundliche Grüsse,
Simon Zaugg

Kommunikation & Marketing

Direkt +41 43 336 40 28
simon.zaugg@swissict.ch

swissICT: Für die Informatik. Für Informatiker. Für Sie.

Schweizerischer Verband der Informations- und Kommunikationstechnologie

http://www.swissict.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : swissICT, Schweizerischer Verband der Informations- und Kommunikationstechnologie

Abkürzung der Firma / Organisation : swissICT

Adresse : Vulkanstrasse 120, 8048 Zürich

Kontaktperson : Thomas Flatt

Telefon : +41 43 336 40 24

E-Mail : thomas.flatt@swissict.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
swissICT	DSG				**Vorbemerkung:** Die Totalrevision des DSG sollte vor allem • eine Brücke schlagen zwischen Sicherstellung Persönlichkeitsschutz der betroffenen Personen und Schaffung moderner Rahmenbedingungen für einen innovativen Wirtschaftsstandort Schweiz im Zeitalter der Digitalisierung; und • eine unnötige Verschärfung gegenüber den Vorgaben des Europarates und der EU (sog. "Swiss Finish") zu Lasten der Innovation und ohne effektiven Nutzen oder Schutz vermeiden, welche die wirtschaftliche Entwicklung hindert. Mit der Lancierung der Strategie für eine digitale Schweiz präsentiert der Bundesrat eine Dachstrategie (Medienmitteilung des Bundesrates vom 20.4.2016: Strategie des Bundesrates für eine digitale Schweiz), mit welcher die Schweiz mehr von der zunehmenden Digitalisierung profitieren und sich als innovative Volkswirtschaft noch dynamischer entwickelt soll. Die Wirtschaft soll sich im digitalen Raum möglichst frei entfalten können. Gleichzeitig hält der Bundesrat fest, dass für eine informierte und demokratische Gesellschaft und zur Sicherung der Wohlfahrt, die von der Datenbearbeitung betroffenen Personen die modernen Informations- und Kommunikationstechnologien in ihrem täglichen Leben kompetent und sicher nutzen können sollten. Dies bedingt jedoch eine kohärente und zukunftsorientierte Datenpolitik zu entwickeln. Weiter führt der Bundesrat aus, dass sich das Potenzial der vermehrten Sammlung und Bearbeitung von Daten zum Vorteil der Schweiz realisieren muss, ohne die Kontrolle über diese Daten zu verlieren. In diesem Kontext ist daher auch die Revision des Datenschutzgesetzes zu sehen und entsprechend einzuordnen, welche absolut zentral ist für die Weiterentwicklung des Wirtschaftsstandortes Schweiz im Zeitalter der Digitalisierung.

					Aus diesem Grund wird eine Verschärfung gegenüber den Vorgaben des Europarates und der EU (sog. "Swiss Finish") zu Lasten der Innovation und ohne effektiven Nutzen oder Schutz, welche die wirtschaftliche Entwicklung hindert, von swissICT abgelehnt. Die europäische Datenschutz-Grundverordnung (DSGVO) verlangt keine pauschale Übernahme ihrer Bestimmungen. Für die Angemessenheitserklärung genügt es vielmehr, grundlegende Garantien einzuhalten, beispielsweise die Rechtsstaatlichkeit oder die Existenz unabhängiger Aufsichtsbehörden. Die DSGVO hält denn auch ausdrücklich fest, dass die Umsetzung der ERK 108 bei der Angemessenheitsbeurteilung ein wesentlicher Faktor ist. Vor diesem Hintergrund sollte sich das künftige DSG primär an der ERK 108 orientieren. Darüber hinausgehende Regelungen können nur insofern sinnvoll sein, als sie helfen, einen einheitlichen Standard nach Massgabe der DSGVO zu fördern. **Eine Verschärfung des DSG gegenüber der ERK 108 und der DSGVO wäre deshalb konzeptionell falsch, nicht notwendig, zulasten schweizerischer Unternehmen wettbewerbsverzerrend und innovationsfeindlich. Ein sog. „Swiss Finish“ kommt daher nur infrage, wenn er eine Erleichterung mit sich bringt** und zur Attraktivität des Wirtschaftsstandortes der Schweiz und zur Förderung der Innovation und Digitalisierung beiträgt**.**
swissICT	DSG	2	3		**Kernanliegen: Keine Streichung der Regel von Art. 2 Abs. 2 lit. c DSG** Zur Eindämmung des Missbrauchs und um die verfahrensrechtlichen Regeln gemäss den einschlägigen Verfahrensordnungen wie z.B. der ZPO nicht zu verwässern, fordern wir, Art. 2 Abs. 2 lit. c DSG (Nichtanwendbarkeit des DSG auf hängige Zivilprozesse und anderer Verfahren mit Bezug auf sämtliche Verfahren insbesondere auch auf kantonaler Stufe) nicht zu streichen. Es ist ferner nicht einsehbar, weshalb die wichtige und richtige Regel von Art. 2 Abs. 3 VE-DSG nur für bundesrechtliche Verfahren gelten soll. In hängigen Verfahren müssen insbesondere auch kantonale (Vor-) Instanzen gleichermassen rechtlich geschützt sein. Auch der geltende Art. 2 Abs. 2 lit. c DSG bezieht sich auf Verfahren vor allen Instanzen. Vgl. im Einzelnen hinten zu Art. 20 Abs. 1 VE-DSG.

swissICT	DSG	3		f	**Kernanliegen: Streichung des im Vergleich zur DSGVO überschiessenden „Swiss Finish“ und Beschränkung auf Personendaten sowie eine automatisierte Bearbeitung.** Die Definition von „Profiling“ ist zu breit und geht massiv weiter als die Definition von „Profiling“ in der DSGVO: Bereits eine „von Hand“ bearbeitete Mitarbeiterbeurteilung würde als “Profiling“ nach Art. 23 Abs. 2 Bst. d VE-DSG und damit per se als Persönlichkeitsverletzung gelten. Konsequenterweise müsste ein Bearbeiter vor jeder Bearbeitung einen Rechtfertigungsgrund ausweisen können, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden wäre. Dies stellt für das Profiling einen Paradigmenwechsel im schweizerischen Datenschutzrecht dar, für den es keinen Grund gibt. Zudem umfasst „Profiling“ dem Wortlaut des Vorentwurfs nach auch das Bearbeiten von nicht-personenbezogenen Daten, was eine unzulässige Ausweitung des Geltungsbereichs des DSG darstellen und im Widerspruch zu Art. 2 Abs. 1 VE-DSG stehen würde. Schliesslich ist eine Analyse bzw. Auswertung keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte der betroffenen Personen auswirkt. Richtigerweise wäre der Begriff „Auswertung“ durch „Bewertung“ zu ersetzen – erst diese stellt einen datenschutzrechtlich relevanten Eingriff in die Persönlichkeitsrechte der betroffenen Personen dar. „Bewertung“ umfasst eine Entscheidung, die sich auf eine Analyse bzw. Auswertung stützt. Die Anknüpfung an die Auswertung greift demnach zu weit.
swissICT	DSG	5			**Kernanliegen: Die Informations- und Genehmigungspflichten setzten komplizierte sowie ressourcenintensive, interne Prozesse voraus. Die Fristen für die Überprüfungen durch den EDÖB sollten auf höchstens vier Wochen reduziert werden.**
swissICT	DSG	5	2 und 3		Art. 5 Abs. 2 und 3 VE-DSG sehen vor, dass der Bundesrat eine Liste von Staaten mit angemessenem Schutz führt. Aus Abs. 3 ergibt sich, dass die Übermittlung in einen Staat, der nicht auf dieser Liste figuriert, grundsätzlich unzulässig ist, vorbehaltlich der Garantien nach art. 5 und der Ausnahmesituationen nach Art. 6 VE-DSG. Die Liste des Bundesrats fingiert also, dass nicht aufgeführte Staaten keinen angemessenen Schutz gewährleisten. Das ist abzulehnen, weil die Anpassung der Liste auf dem Verordnungsweg relevante Rechtsänderungen nicht sofort nachvollziehen kann. Es

					ist zudem denkbar, dass ein Datenbearbeiter über Informationen verfügt, aus denen sich ergibt, dass ein bestimmter Empfängerstaat über ein angemessenes Schutzniveau verfügt, obwohl er nicht auf der Liste des Bundesrats aufgeführt ist. In solchen Fällen führt eine Übermittlung ins Ausland nicht zu einer Gefährdung der betroffenen Personen und damit auch nicht zu einer Verletzung von Art. 5 Abs. 1 VE-DSG. Die Liste des Bundessrats muss daher für aufgeführte Staaten eine Positivliste darstellen, auf die sich Datenbearbeiter verlassen dürfen. Das deckt die Masse der Auslandsübermittlungen ab. Die Liste darf umgekehrt aber keine Negativliste im Sinne einer Fiktion sein. Sie darf höchstens die Vermutung begründen, dass im betreffenden Staat ein angemessener Schutz fehlt. Dem Datenexporteur muss der Beweis des Gegenteils dabei offengelassen werden.
swissICT	DSG	5	3	b	Gemäss lit. b muss der Beauftragte informiert werden, bei lit. d braucht es eine Genehmigung des Beauftragten. Diese unterschiedliche Handhabung ist nicht nachvollziehbar. Worin der Unterschied zwischen Garantien nach lit. b und d besteht, bedarf daher einer Klärung, Der Aufwand für ein Unternehmen sollte verhältnismässig sein und wenn möglich sollte der VE-DSG einheitliche Instrumente/Abläufe vorsehen, was ebenfalls dem EDÖB bei der internen Beurteilung zugute kommt.
swissICT	DSG	5	3	d	Art. 5 Abs. 3 VE-DSG regelt das Vorgehen, wenn der Bundesrat keinen angemessenen Schutz festgestellt hat. In lit. d Ziff. 2 wird als Ausnahme die Genehmigung einer ausländischen Behörde zu einer verbindlichen unternehmensinternen Datenschutzvorschrift erwähnt, sofern diese in einem Staat liegt, welche einen angemessenen Schutz gewährleistet. Unklar ist hierbei, wer beurteilt, dass diese ausländische Behörde einem Staat angehört, die einen angemessenen Schutz gewährleistet.
swissICT	DSG	5	3	d	Die Regelung, wonach die Genehmigung von Binding Corporate Rules (BCR) durch den EDÖB bis zu sechs Monate dauern kann, ist weder sachgerecht noch praktikabel (Art. 5 Abs. 3 lit. d und Abs. 5 VE-DSG). Zudem stellen die BCR eine „Unterkategorie“ der „spezifischen Garantien“ i.S.v. Art. 5 Abs. 3 lit. b VE-DSG dar – und für diese ist lediglich eine Informationspflicht vorgesehen (eine Genehmigung durch den EDÖB ist nicht erforderlich). Dasselbe gilt für die Möglichkeit des EDÖB, Informationen nachzuverlangen (Abs. 5), was die sechsmonatige Frist verlängern würde. Bei einer solchen Regelung würden BCR im Ergebnis nicht mehr verwendet, was dem Regelungsziel von Art. 5 VE-DSG zuwiderläuft.

swissICT	DSG	5	4		Die Frist von 30 Tagen kann bei laufenden Vertragsverhandlungen zu lang sein. Eine kürzere Prüffrist der spezifischen Garantien (Vertrag) von 10 Tagen wäre daher zu begrüssen, um eine Lähmung der Unternehmenstätigkeit zu verhindern.
swissICT	DSG	5	5		Die unterschiedliche Handhabung der spezifischen resp. standardisierten Garantien ist nicht nachvollziehbar. Eine Information gemäss Abs. 3 lit. b sollte ausreichen. Die Frist zur Genehmigung ist mit einem halben Jahr zu lange angesetzt (bisher musste die Prüfung selbst von BCR innert 30 Tagen durchgeführt sein). Hinzu kommt, dass die tatsächliche Frist wiederum sehr viel länger sein kann, da der EDÖB sich jederzeit auf den Standpunkt stellen kann, er habe noch nicht alle erforderlichen Informationen. Erschwerend tritt hinzu, dass bei einem negativen Entscheid ein Unternehmen aufgrund der neuen Verfügungsmacht des EDÖB den Entscheid vor dem Bundesverwaltungsgericht anfechten muss, was zu einer weiteren Verzögerung, bei gleichzeitiger Lähmung der Unternehmenstätigkeit, führt.
swissICT	DSG	5	6		Art. 5 Abs. 6 ist ersatzlos zu streichen. Die pauschale Informationspflicht bietet weder der betroffenen Person noch dem EDÖB einen Mehrwert; die DSGVO kennt eine entsprechende Informationspflicht auch nicht (Art. 5 Abs. 6).
swissICT	DSG	5	7		Abs. 7 dahingehend zu ergänzen, dass der Bundesrat diese Liste aktuell halten muss, da diese neu verbindlichen Charakter für die Unternehmen hat und sich diese darauf verlassen müssen.
swissICT	DSG	6			**Kernanliegen: Berücksichtigung der Bedürfnisse der Praxis bei der Festlegung der Ausnahmetatbestände.**
swissICT	DSG	6	1	a	Im Text des Vorentwurfs ist wie im heutigen Text von einer Einwilligung „im Einzelfall“ die Rede. Diese Begrenzung findet sich nicht in Art. 49 Abs. 1 lit. a DSGVO. Es wäre wichtig, im Text des VE-

					DSG – oder zumindest im Erläuternden Bericht – festzuhalten, dass der „Einzelfall" jeweils die Gesamtheit ähnlich gelagerter Bekanntgaben ins Ausland umfasst. Die Einwilligung muss daher jeweils für alle vergleichbaren Bekanntgaben gelten, wie dies in der heutigen Lehre anerkannt ist.
swissICT	DSG	6	1	b	Art. 6 Abs. 1 lit. b VE-DSG sollte mit der Regelung der DSGVO in Übereinstimmung gebracht werden. Danach sollte eine Bekanntgabe im Sinne eines Ausnahmefalls auch dann zulässig sein, wenn die betroffene Person nicht Vertragspartei ist, aber der fragliche Vertrag in ihrem Interesse oder zu ihren Gunsten abgeschlossen wurde. Art. 6 Abs. 1 lit. b ist daher wie folgt anzupassen: *die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt <u>oder einer Person, zu deren Gunsten oder in deren Interesse der Vertrag abgeschlossen wird</u>;*
swissICT	DSG	6	1	c	Um schwierige Abgrenzungsfragen im Voraus auszuschliessen, sollten in Art. 6 Abs. 1 lit. c Ziff. 2 VE-DSG die Begriffe „Gericht" sowie „Verwaltungsbehörde" ersatzlos gestrichen werden. Massgebend ist, dass die Datenbearbeitung zur „Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen" erfolgt. Die hierfür zuständigen ausländischen Behörden können aus historischen Gründen unterschiedlich organisiert sein sowie verschiedene Bezeichnungen tragen und sich nicht in eine der beiden Kategorien zuordnen lassen. Art. 6 Abs. 1 lit. c Ziff. 2 ist daher wie folgt anzupassen: *die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen ~~vor einem Gericht oder einer Verwaltungsbehörde~~;*
swissICT	DSG	6	2		Art. 6 Abs. 2 VE-DSG sollte ersatzlos gestrichen werden. Erstens ist eine Pflicht, den EDÖB trotz Ausnahmetatbestand zu informieren, unverhältnismässig. Zweitens wird diese breite (für Verantwortliche <u>und</u> Auftragsdatenbearbeiter) geltende Pflicht zu einer „*Meldeflut*" führen, welche der EDÖB gar nicht wird bewältigen können. Ferner würde der EDÖB dadurch über heikle Verfahren und (Geschäfts-)Geheimnisse informiert, ohne sachlichen Grund und ohne Mehrwert für betroffene

					Personen. Das greift massiv in die unternehmerische Freiheit und in die durch das ZGB und andere Erlasse weiterhin geschützte Geheimsphäre der Unternehmen ein. Zudem ist diese Pflicht der DSGVO und der Konvention 108 fremd und stellt damit einen abzulehnenden Swiss Finish dar.
swissICT	DSG	7	3		**Auftragsdatenbearbeitung / Sub-Processing** Gemäss Art. 7 Abs. 3 VE-DSG soll eine Weiterübertragung der Auftragsbearbeitung ("Sub-Processing") künftig nur noch mit vorgängiger schriftlicher Zustimmung des Verantwortlichen möglich sein. Im erläuternden Bericht wird darauf verwiesen, die DSGVO sehe "etwa Ähnliches" vor. Dem kann nicht gefolgt werden; die DSGVO enthält keine vergleichbare Bestimmung, womit der VE-DSG hier weiter geht als notwendig. Die strengen Zulässigkeitsvoraussetzungen sind auch in der Sache nicht begründet. Bei der Übertragung der Auftragsbearbeitung an einen Sub-Processor in einem Staat ohne angemessenes Datenschutzniveau finden die Bestimmungen zur Datenbekanntgabe ins Ausland gemäss Art. 5/6 VE-DSG Anwendung und sorgen bereits für hinreichenden Schutz. Die schematische Bindung des Sub-Processing an die vorgängige schriftliche Zustimmung des Verantwortlichen wäre in der Praxis hinsichtlich bestehender Auftragsbearbeitungen nur mit grösstem Aufwand umsetzbar. Zudem ist nicht nachvollziehbar, wieso dem Verantwortlichen ein (grundloses) Einspruchsrecht eingeräumt wird. Es handelt sich hier um einen unverhältnismässigen Eingriff in die Vertrags- und Wirtschaftsfreiheit. Nehmen wir als Beispiel ein Marketing-Unternehmen, das für seine Geschäftskunden Mailings zuhanden derer Kunden erstellt/versendet, also als Auftragsbearbeiter tätig ist. Möchte dieses Marketing-Unternehmen seine IT-Infrastruktur an einen Dritten auslagern, könnte dies von Gesetzes wegen am Einspruch eines einzigen seiner Geschäftskunden scheitern. Dies ist in einer digitalisierten und hochspezialisierten Welt praxisfremd. Vorstellbar wäre allenfalls eine Regelung, wonach der Auftragsbearbeiter auf Verlangen des Verantwortlichen eine Liste mit seinen (Sub-)Auftragsbearbeitern zur Verfügung stellt (was im Lichte der Dokumentationspflicht ohnehin angebracht erscheint). Es steht den Parteien frei, vertraglich weitergehende Einschränkungen festzulegen. Der Artikel ist weiter auch sonst systemfremd. Die Auftragsbearbeitung als solche ist unter den Voraussetzungen

					von Art. 7 Abs. 1 und 2 VE-DSG ohne weitere Genehmigung durch die betroffenen Personen zulässig. Warum die Subauftragsbearbeitung einer strengeren Regelung unterstellt werden soll, ist nicht ersichtlich. Richtigerweise sollten Art. 7 Abs. 1 und 2 VE-DSG für weitere Unterauftragsbearbeiter einfach analog gelten. Falls also der Verantwortliche seine Zustimmung verweigern würde, müssten bestehende Auftragsbearbeitungen vorzeitig beendigt werden, was zu erheblichen Mehrkosten der Leistungserbringung führen kann. Auch für künftige Auftragsbearbeitungen bringt diese Norm unnötigen Overhead bei den Auftragsbearbeitern und damit letztlich Mehrkosten bei den Verantwortlichen. Art. 7 Abs. 3 VE-DSG ist deshalb ersatzlos zu streichen.
swissICT	DSG	Div.	Div.		**Auftragsdatenbearbeitung / Erweiterte Pflichten des Auftragsbearbeiters** Die Pflichten des Auftragsbearbeiters werden im VE-DSG gegenüber dem Status Quo erheblich ausgeweitet. Dabei wird der Auftragsbearbeiter teils alleine und teils kumulativ, alternativ oder subsidiär zum Verantwortlichen in die Pflicht genommen. Hierbei ist nicht völlig klar, ob die sprachliche Unterscheidung jeweils bewusst getroffen wurde (z.B. alternative Pflicht bei der Datenschutz-Folgenabschätzung in Art. 16 VE-DSG, kumulative Pflicht hinsichtlich Privacy by Design und Privacy by Default in Art. 18 VE-DSG). Während die kumulative Verpflichtung des Auftragsbearbeiters im Rahmen von Art. 11 Abs. 1 VE-DSG (Datensicherheit) und Art. 19 Bst. a VE-DSG (Dokumentation) sachgerecht erscheint, ist sie bei Art. 18 VE-DSG zumindest in Bezug auf Privacy by Default abzulehnen, handelt es sich hierbei doch um eine inhärente Pflicht des Verantwortlichen, die der Auftragsbearbeiter gar nicht wahrnehmen kann. Auch die kumulativen Pflichten des Auftragsbearbeiters gemäss Art. 19 Bst. b VE-DSG gehen zu weit; hinsichtlich der Information über Verletzungen des Datenschutzes besteht gar ein Widerspruch zu Art. 17 Abs. 4 VE-DSG, wonach der Auftragsbearbeiter (nur) den Verantwortlichen über eine unbefugte Datenbearbeitung zu informieren hat.

					Auch die alternative Verpflichtung ergibt bei einzelnen Bestimmungen keinen Sinn: So kann die Mitteilung einer Datenbekanntgabe ins Ausland in Ausnahmefällen gemäss Art. 6 Abs. 2 VE-DSG konsequenterweise nur durch den Verantwortlichen erfolgen, weil nur jener sich auf die entsprechenden Ausnahmetatbestände gemäss Art. 6 Abs.1 VE-DSG berufen kann. Die überschiessende Ausweitung der Pflichten des Auftragsbearbeiters ist auch deshalb als problematisch einzustufen, weil bei einem Verstoss gegen diese Pflichten auch der Auftragsbearbeiter unter die Sanktionsnorm gemäss Art. 51 VE-DSG fällt. Die dem Auftragsbearbeiter unter dem VE-DSG obliegenden Pflichten sollten deshalb auf das absolut Notwendige beschränkt werden und nur dort Anwendung finden, wo der Auftragsbearbeiter auch über die entsprechende Kompetenz und Möglichkeit in der Sache verfügt, um die Pflichten einzuhalten.
swissICT	DSG	8 und 9			Selbstregulierung ist besonders bei technikneutralen, aber dennoch techniknahen Regulierungen wichtig. Art. 8 und 9 VE-DSG werden deshalb ausdrücklich begrüsst. Dabei ist es zentral, dass die Wirtschaft einbezogen wird, wenn der EDÖB von sich aus Regelungen der guten Praxis ausarbeitet, wie das in Art. 8 Abs. 1 VE-DSG vorgesehen ist.
swissICT	DSG	12			**Kernanliegen: Ersatzlose Streichung des ganzen Artikels** Die Regelung von Art. 12 VE-DSG ist schwer verständlich und erscheint im VE-DSG als Fremdkörper. Soweit es sich bei Personendaten auch um Geschäftsdaten handelt, was die Regel ist, bestehen gemäss diversen andern einschlägigen Gesetzen (wie z.B. Buchführungsrecht gemäss OR, Steuerrecht, spezialgesetzliche Regelungen wie z.B. im Finanzmarktrecht zur Sicherstellung von Anlegerschutz, etc.) weitreichende legitime Dokumentations- und Archivierungspflichten, welche dem Kerngehalt von Art. 12 VE-DSG zuwiderlaufen. Nur schon deshalb bringt Art. 12 VE-DSG in dieser pauschalen Formulierung mit Wirkung für sämtliche Branchen und Konstellationen nichts und ist demzufolge ersatzlos zu streichen. Bei genauerem Betrachten fokussiert die Regelung wohl auf Daten einer verstorbenen Person auf **Social Media-Plattformen**. Dann sollte dies aber wenn schon in der Regelung auch explizit so eingeschränkt werden. Allerdings bringt die Regelung auch im Bereich Social Media keinen erkennbaren Mehrwert.

					Effektiv gehen beim Tod einer Person dessen Rechte qua **erbrechtlicher Universalsukzession** ohne Weiteres auf die Erben über (Art. 560 Abs. 1 ZGB). Gestützt auf diesen erbrechtlichen Übergang sämtlicher Rechte von Gesetzes wegen sind die Erben bereits ausreichend legitimiert, geeignete Massnahmen vorzukehren und z.B. die Löschung von Daten des Erblassers auf einer Social Media-Plattform zu verlangen. Die Regelung von Art. 12 VE-DSG ist somit weder nötig noch sinnvoll. Umgekehrt können die Erben per definitionem auch nicht mehr Rechte haben, als der Erblasser sie hatte. Art. 12 VE-DSG ist sogar kontraproduktiv, weil er eine Regelung aufstellt, welche zumindest nicht deckungsgleich ist mit etabliertem Erbrecht. Gleiches gilt mit Bezug auf Regelungen von Amts- und Berufsgeheimnissen in bereits bestehenden gesetzlichen Regelungen, für Banken z.B. nach Art. 47 BankG. Die pauschale Regelung, dass unter Art. 12 Abs. 3 VE-DSG Amts- und Berufsgeheimnisse generell nicht geltend gemacht werden können, kann so jedenfalls nicht stimmen. Tritt z.B. gemäss Vereinbarung der Erbengemeinschaft nur ein einzelner Erbe in die Rechtsstellung des Erblassers z.B. einer bestimmten Bank gegenüber ein, stehen nur diesem Erben sämtliche Rechte des Erblassers zu, während gegenüber allen andern Erben das Bankkundengeheimnis uneingeschränkt gilt. Nach alledem ist Art. 12 VE-DSG jedenfalls geeignet, statt der– heute nach Erbrecht bestehenden – Rechtssicherheit eher **Widersprüche zu bestehenden gesetzlichen Regelungen** zu produzieren. Aufgrund all dieser Argumente fordern wir die **ersatzlose Streichung von Art. 12 VE-DSG**. Stattdessen ist soweit sinnvoll zu überlegen, inwieweit gezielte spezialgesetzliche Regelungen z.B. in Ergänzung von Art. 28 ff. ZGB sinnvoll erscheinen. Nach dem Gesagten eher nicht.
swissICT	DSG	13			Die aktive Informationspflicht wird auf alle Personendaten ausgeweitet, was zu erheblichem Mehraufwand für die Unternehmen führen würde. Das ist abzulehnen. Die Informationspflicht sollte nur für besonders schützenswerte Personendaten und im Fall der Profilierung gelten. Wichtig ist ferner, dass die aktive Informationspflicht ausschliesslich bei der Beschaffung gilt, nicht bei jeder weiteren Bearbeitung und auch nicht bei weiteren Bekanntgaben an Dritte. So ist Art. 13 VE-DSG auch zu verstehen, wie sich aus Abs. 1 ergibt. Daran kann Abs. 3 VE-DSG nichts ändern. Sollte Abs. 3 VE-DSG dagegen so zu lesen sein, dass bei *jeder* Drittbekanntgabe erneut zu informieren ist, wäre eine solche Regel nicht praktikabel unbedingt abzulehnen.

					In den Erläuterungen sollte präzisiert werden, dass bei allfälligen Änderungen keine Nachinformation erfolgen muss.
swissICT	DSG	13	3		Vgl. zu Art. 13 oben.
swissICT	DSG	13	4		Art. 13 Abs. 4 VE-DSG ist konzeptionell falsch und muss gestrichen werden. Die Auftragsdatenbearbeitung basiert auf dem Konzept einer Privilegierung (Auftragsdatenbearbeiter ist der „lange Arm" des Verantwortlichen; alles was der Verantwortliche darf, kann er auch durch einen Auftragsdatenbearbeiter ausführen lassen). Art. 7 VE-DSG geht dementsprechend davon aus, dass eine Auftragsdatenbearbeitung nur dann vorliegt, wenn eben die dort genannten Voraussetzungen (Vertrag, Sicherheitsbestimmungen, Weisungsgebundenheit, namentlich Verwertungsverbot zu eigenen Zwecken) erfüllt sind. Wenn sie erfüllt sind, liegt die privilegierte Situation „Auftragsdatenbearbeitung" vor. Sind sie nicht erfüllt, greift auch die Privilegierung nicht; und es liegt ein Fall der „Bekanntgabe" vor. Mit anderen Worten: Die Informationspflicht bei Auslagerung – also Art. 13 Abs. 4 VE-DSG – ist systemwidrig und steht quer in der Landschaft des VE-DSG, das eine gesteigerte Risikosituation grundsätzlich nur bei der Bekanntgabe sieht. Bereits Art. 7 Abs. 4 VE-DSG zeigt (wie das bisherige Recht), dass jedenfalls der IT-Dienstleister nicht als Dritter zu bezeichnen ist. Das DSG verpflichtet den Verantwortlichen bereits zur Einhaltung des DSG und allen weiteren Massnahmen (Auswahl des Dienstleisters, Sicherheit, etc.) – genau gleich, wie wenn er selber die IT betreibt. Wenn er diesbezüglich Fehler macht, können die Behörden sanktionieren (neu allenfalls sogar strafrechtlich). Die betroffene Person kann von der vorgeschriebenen Information nicht profitieren. Im Gegenteil, die Mitteilungspflicht würde implizit denjenigen, der seine IT selber betreibt (auch wenn er dazu die notwendigen Kompetenzen nicht hat), als sicherer darstellen als denjenigen, der diese Aufgaben einem Experten überlässt. Die Bestimmung ist also auch sachlich falsch, geradezu gegenläufig zu den Interessierten der betroffenen Person.
swissICT	DSG	14			[siehe unten bei Art. 21]

swissICT	DSG	15			**Kernanliegen: Präzisierung der Pflichten nach Art. 15 VE-DSG** Die Informationspflicht und das Äusserungsrecht nach Art. 15 Abs. 1 und 2 VE-DSG (zu letzterem s. unten) gelten, sofern eine automatisierte Einzelfallentscheidung „rechtliche Wirkungen oder erhebliche Auswirkungen“ auf die betroffene Person hat. Diese beiden Tatbestandselemente sind sehr vage, was zu Rechtsunsicherheit führt. Sie sollten daher im Text von Art. 15 Abs. 1 VE-DSG eingeschränkt werden. Zumindest wäre im Erläuternden Bericht bzw. der Botschaft festzuhalten, dass die Schwelle für „rechtliche Wirkungen“ und für „erhebliche Auswirkungen“ jeweils hoch ist und dass die Verweigerung eines Vertragsschlusses zumindest im Regelfall keine „rechtliche Wirkung“ hat (weil i.d.R. kein Rechtsanspruch auf den Abschluss eines Vertrags besteht und seine Verweigerung daher nicht in eine Rechtsstellung eingreift). Andernfalls droht eine Ausweitung der ohnehin weitgehenden Pflichten nach Art. 15 Abs. 1 und 2 VE-DSG auch auf Bagatellentscheidungen.
swissICT	DSG	15	2		**Kernanliegen: Ersatzlose Streichung des Äusserungsrechts (Art. 15 Abs. 2 VE-DSG).** Ein zentraler Punkt der Digitalisierung ist die Automatisierung. Gerade durch Automatisierung lassen sich Effizienzgewinne und damit einhergehend Aufwandreduktionen erzielen, welche im heutigen wirtschaftlichen Umfeld enorm wertvoll, wenn nicht gar unabdingbar geworden sind. Zudem wirken sie sich auch positiv für die Kunden aus, z.B. durch tiefere Preise. Automatisierte Entscheide bringen gegenüber manuellen Entscheidungsprozessen zudem erhebliche Vorteile für Anbieter und Kunden mit sich (Objektivität der Entscheidung, geringere Kosten, schnellere Prozesse). Es ist deshalb nicht einzusehen, warum vollautomatisierte Entscheide durch die Datenschutzgesetzgebung faktisch verboten werden sollten. Diese Technophobie ist unbegründet, und sie widerspricht auch dem Ziel einer technikneutralen Regelung. Das in Art. 15 Abs. 2 VE-DSG neu vorgeschlagene Recht einer betroffenen Person, sich zu einer automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern („Anhörungspflicht“), stufen wir vor diesem Hintergrund als wettbewerbs- und auch innovationsbehindernd ein. Darüber hinaus ist dieses Recht aber auch schlicht unnötig, insbesondere angesichts der ebenfalls neu eingeführten Pflicht, die betroffene Person darüber zu informieren, wenn eine automatisierte Einzelentscheidung gefällt wurde (Abs. 1 von Art. 15 VE-DSG). Unabhängig davon quasi „auf

					Vorrat“ zu informieren produziert demnach keine zusätzliche Transparenz, sondern generiert lediglich unnötigen zusätzlichen Administrativaufwand. Zudem ist zu befürchten, dass die Einführung einer Pflicht zur „Äusserung“ in der Praxis zu einer Begründungspflicht führt und letztlich die Vertragsfreiheit eines Unternehmens erheblich einschränkt. Das ist ein konsumentenschützerisches Anliegen, das nicht ins Datenschutzrecht gehört. SwissICT setzt sich deshalb vehement für eine ersatzlose Streichung der Äusserungsrechts von Art. 15 Abs. 2 VE-DSG ein. Die Relevanz bestimmter Daten für die Richtigkeit von Entscheidungen und der Grad der Wichtigkeit von automatisierten Entscheidungen i.S.v. Art. 15 VE-DSG kann von Branche zu Branche ferner massiv unterschiedlich sein. Daraus ergibt sich, dass eine generelle Regelung für die gesamte Wirtschaft jedenfalls über das Ziel hinausschiesst. Nicht zum Vornherein abwegig ist es demgegenüber, soweit nötig für einzelne ganz bestimmte branchenspezifische Datennutzungen in einschlägigen Spezialgesetzen oder in Empfehlungen der guten Praxis (Art. 9 VE-DSG) eine angemessene Regelung zu treffen, welche den Besonderheiten der betreffenden Branche gebührend Rechnung trägt. Folgerichtig ist auch der entsprechende Abschnitt in Art. 20 Abs. 3 VE-DSG zu streichen. Die Information darüber, wie bestimmte Entscheide zustande kommen, gehört zum Geschäftsgeheimnis eines Unternehmens. Eine solche Informationspflicht ist demnach, insbesondere in der aktuell vorgesehen, detaillierten Form gemäss Art. 20 Abs. 3 VE-DSG, klar unverhältnismässig. So ist zum Beispiel im Finanzbereich die Einschätzung von Ausfallrisiken bei der Kreditvergabe ein wichtiges, differenzierendes Know-How eines Finanzdienstleisters. Die Auskunft über die für diese Einschätzung genutzten Daten und deren Gewichtung führt zu einer Replizierbarkeit dieser Einschätzung und damit zur Aufgabe dieses Geschäftsgeheimnisses. Offenlegungspflichten solcher Art würden im Ergebnis jede Innovationskraft der Wirtschaft abtöten, da der dafür eingesetzte Aufwand nicht angemessen geschützt werden könnte. Sollte dem Streichantrag wider Erwarten nicht gefolgt werden, müsste jedenfalls vorab Art. 20 Abs. 3 VE-DSG als dort – unter dem allgemeinen Auskunftsrecht – sachfremde Regelung gestrichen und mit Art. 15 VE-DSG zu einer in sich stimmigen Gesamtlösung

					verbunden werden. Dabei wäre die Regelung – entsprechend dem richtigen Ansatz der DSGVO, mit welchem der VE-DSG äquivalent zu sein hat – auf schwere Fälle zu begrenzen, d.h. auf solche mit erheblichen Auswirkungen auf die betroffene Person. Sodann wäre klarzustellen, dass jedenfalls eine einmalige angemessene Information ohne ausdrückliche Einwilligung im Sinne der Gesetzessystematik ausreichend ist. Dadurch wird auch das in Art. 20 Abs. 3 VE-DSG vorgesehene Auskunftsrecht über automatisierte Einzelfallentscheidungen obsolet. Die Kunden können zudem bis zu einem gewissen Grad selbst entscheiden, ob sie zu einem Anbieter wollen, der vollautomatisierte Entscheide trifft oder zu einem Anbieter, der zusätzlich oder vollständig auf die Arbeitskraft natürlicher Personen setzt. Diese Grundentscheidung mit Bezug auf das Geschäftsmodell spiegelt sich regelmässig auch in unterschiedlichen Preisen wieder. Auf Art. 20 Abs. 3 kommen wir nochmals zurück (s. unten).
swissICT	DSG	16			Die Regelung der Datenschutz-Folgenabschätzung („DSFA“) im Vorentwurf ist an sich überflüssig. Die Forderung von Art. 8bis der revidierten Konvention 108, bei geplanten Datenbearbeitung die Risiken einzuschätzen, wird durch Art. 11 des Vorentwurfs (Datensicherheit) bereits erfüllt. swissICT wendet sich dennoch nicht gegen eine eigene gesetzliche Regelung der DSFA. Die Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen, ist im VE-DSG jedoch viel zu weit gefasst. Art. 16 ist wie folgt neu zu fassen (vgl. die folgenden einzelnen Bemerkungen): *1 Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem <u>hohen</u>~~erhöhten~~ Risiko für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen.* *2 Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person*

					sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit ~~oder der Grundrechte~~ der betroffenen Person zu verringern. *3 Der Verantwortliche ~~oder der Auftragsbearbeiter~~ benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen, sofern trotz der vorgesehenen Massnahmen hohe Restrisiken für eine Verletzung der Persönlichkeit der betroffenen Person vorauszusehen sind.* *4 Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen ~~oder dem Auftragsbearbeiter~~ innerhalb von ~~drei Monaten~~ einem Monat nach Erhalt aller erforderlichen Informationen mit.*
swissICT	DSG	16	1		**Kernanliegen: Die Bestimmung muss präzisiert werden, und der Hinweis auf die Grundrechte der betroffenen Personen ist zu streichen.** Der Ausdruck „erhöhtes Risiko“ in Abs. 1 ist viel zu unbestimmt. Er geht zudem über die europäischen Vorgaben hinaus: Art. 35 f. DSGVO und Art. 27 Ziff. 1 der Schengen-Richtlinie verlangen eine Datenschutz-Folgenabschätzung jeweils nur bei einem „hohen“ Risiko. Der VE-DSG ist entsprechend anzupassen. Ohne eine solche Anpassung müsste jede Bearbeitung, die in irgendeiner Hinsicht ein Risiko mit sich bringt (schon jede Übermittlung ins Ausland) zu einer Datenschutz-Folgenabschätzung und einer Meldung an den EDÖB führen (schon wegen des Sanktionsrisikos). Dies würde hohe Kosten verursachen, denen kein Mehrwert gegenüber steht. Es ist zudem falsch, von einem Risiko für „die Grundrechte“ der betroffenen Personen zu sprechen. Das entspricht zwar mehr oder weniger der Regelung der DSGVO. Das europäische Recht kennt aber eine direkte Drittwirkung der Grundrechte, die dem schweizerischen Recht fremd ist. Wenn Art. 16 VE-DSG vom Risiko für Grundrechte spricht, würde dies eine konzeptionelle Änderung bedeuten. Das ist abzulehnen: Es ist nicht Aufgabe privater Datenbearbeiter, die Grundrechte betroffener Personen zu schützen, soweit diese Grundrechte nicht in den einzelnen Anforderungen des DSG

					Ausdruck gefunden haben. Dazu kommt, dass völlig unklar ist, um welche Grundrechte es geht und welche Risiken dabei relevant wären. Schliesslich spricht Art. 16 Abs. 1 VE-DSG davon, dass „der Verantwortliche *oder* der Auftragsbearbeiter“ verpflichtet sind, die Datenschutz-Folgenabschätzung durchzuführen. Diese Formulierung kann nur bedeuten, dass die Pflicht den Verantwortlichen trifft, dieser aber befugt ist, die Durchführung der Datenschutz-Folgenabschätzung dem Auftragsbearbeiter zu übertragen. Die Formulierung ist aber missverständlich und daher zu präzisieren (s. oben).
swissICT	DSG	16	3		**Kernanliegen: Beschränkung der Meldepflicht auf Fälle hoher Restrisiken; Kürzung der Reaktionsfrist des EDÖB.** Viel zu weit geht auch die Meldepflicht an den EDÖB. Nach der vorgeschlagenen Regelung ist der EDÖB über jede Datenschutz-Folgenabschätzung zu informieren. Das ist strikt abzulehnen: • Jede Datenschutz-Folgenabschätzung melden zu müssen, stellt einen massiven Eingriff in die Geheimsphäre der Unternehmen dar. • Den Unternehmen würde durch eine solche Meldepflicht ein Anreiz gesetzt, im Zweifel keine Datenschutz-Folgenabschätzung durchzuführen. Das wäre kontraproduktiv. • Wenn jede Datenschutz-Folgenabschätzung meldepflichtig ist, wird der EDÖB von Meldungen überflutet. Er kann auf die zahlreichen Meldungen von Datenschutz-Folgenabschätzung nicht reagieren. Eine unterschiedslose Meldepflicht führt nur zu bürokratischen Leerläufen ohne Nutzen. • Selbst das europäische Recht verlangt nicht, die Aufsichtsbehörden von jeder Datenschutz-Folgenabschätzung zu informieren. Art. 36 Abs. 1 DSGVO verlangt eine Meldung im Gegenteil nur dann, wenn die Datenschutz-Folgenabschätzung ergibt, dass trotz der vorgesehenen Massnahmen ein hohes Risiko verbleibt. Art. 36 Abs. 1 DSGVO ist zwar unklar formuliert, doch ergibt sich dies eindeutig aus den Erwägungsgründen der DSGVO. Auch die Reaktionszeit des EDÖB von drei Monaten ist viel zu lange. Wenn Unternehmen drei Monate auf eine Antwort des EDÖB warten müssen, führt dies zu erheblichen Verzögerungen und wirkt massiv innovationshemmend. Im Fall einer Meldung hat der EDÖB ausschliesslich zu prüfen, ob die

					vorgeschlagenen Massnahmen ausreichend sind. Dafür genügt ein Monat. Dies insbesondere deshalb, weil der EDÖB diese Frist durch Nachfragen laufend verlängern kann.
swissICT	DSG	17	1		**Kernanliegen: Die Meldepflicht gegenüber dem EDÖB ist einzuschränken.** Die Pflicht sollte auf hohe Risiken eingeschränkt werden; insbesondere aufgrund der vorgesehenen Sanktionierung (vgl. Art. 50 Abs. 2 lit. d VE-DSG). Die Meldung an den EDÖB muss „unverzüglich“ erfolgen. Das ist so zu verstehen, dass die Meldung ohne unbegründete Verzögerung erfolgen sollte, nachdem der Verantwortliche vom meldepflichtigen Vorgang ausreichende Kenntnis hat, um das Risiko einschätzen zu können. In diesem Sinne ist dem Erläuternden Bericht beizupflichten, der den Ermessensspielraum des Verantwortlichen anspricht. Aus Abs. 1 VE-DSG ist nicht ersichtlich, ob dem Beauftragten lediglich die Datenschutzverletzung oder bestimmte / weitergehende Informationen hierzu mitzuteilen sind (vgl. demgegenüber Art. 33 Abs. 3 DSGVO). Das ist zu präzisieren. Unklar ist zudem, ob auch Bagatellmeldungen darunter fallen; diese sind klar auszuschliessen bzw. es sollten nur jene Datenschutzverletzungen meldepflichtig sein, die (i) relevanten Risiken (ii) mit gewisser Eintrittswahrscheinlichkeit verbunden sind.
swissICT	DSG	17	2		**Kernanliegen: Die Meldepflicht gegenüber den betroffenen Personen ist zu präzisieren.** Es ist nicht klar, wann und mit welchem Inhalt die betroffene Person genau zu informieren ist. Nach DSGVO 34 ist die betroffene Person nur zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person hat. Dies sollte im VE-DSG entsprechend angepasst werden.
swissICT	DSG	17	4		Die Informationspflicht des Auftragsbearbeiters zuhanden des Verantwortlichen sollte erst dann ausgelöst werden, wenn der Auftragsbearbeiter von einer Verletzung Kenntnis hat. Art. 17 Abs. 4 sollte daher wie folgt formuliert werden: *4 Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung, sobald er davon Kenntnis hat.*

swissICT		18			Die Formulierung von Art. 18 VE-DSG ist unklar und geht über die in Art. 25 DSGVO enthaltenen Anforderungen hinaus. swissICT vertritt zudem die Auffassung, dass Art. 18 VE-DSG systematisch zu Art. 11 VE-DSG gehört bzw. bereits durch das geltende Recht gedeckt ist Die Bestimmung sollte gestrichen und in Art. 11 VE-DSG integriert werden, wobei nicht über die Anforderungen der DSGVO hinauszugehen ist.
swissICT	DSG	20	1		**Kernanliegen: Massvolle Anwendung des Auskunftsrechts und Schutz vor Missbrauch.** Das allgemeine Auskunftsrecht ist im Kern unbestritten. Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen und überdies auf hängige Verfahren (vgl. Art. 2 Abs. 3 VE-DSG) ist jedoch unverhältnismässig. Dies gilt umso mehr, als gemäss geltender Schweizer Rechtsprechung kein Auskunftsersuchen je rechtsmissbräuchlich sein kann, weil selbst ein untergeordnetes Datenschutzinteresse ausreicht, um einen Auskunftsanspruch zu bejahen. Die Anknüpfung am bisher bewährten System der Datensammlung wäre sachgerechter und würde den betroffenen Personen ausreichenden Schutz bieten. Schliesslich ist dem zunehmenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke ein Riegel zu schieben. Die Vergangenheit hat leider gezeigt, dass datenschutzrechtliche Begründungen viel zu leicht vorgeschoben werden können, um eine kostenlose Beschaffung von Beweismitteln durchzusetzen. Die Anzahl querulatorischer, kosten- und ressourcenintensiver Fälle zu reinen Schikanezwecken hat deshalb stark zugenommen. Aus diesen Gründen ist auch der Ansatz falsch, das Auskunftsrecht generell kostenlos auszugestalten. Damit wird mit dem Verursacherprinzip ein Grundsatz verletzt, welcher ansonsten in der Rechtsordnung generell gilt. Dementsprechend ordnet auch die DSGVO keine allgemeine Kostenlosigkeit an (Art. 12 Ab. 5 DSGVO). Die von Art. 20 Abs. 1 VE-DSG angeordnete pauschale Kostenlosigkeit der Auskunft ist deshalb **nicht äquivalent** und demzufolge ersatzlos zu streichen und stattdessen ein angemessener Unkostenbeitrag vorzusehen. Zur effizienten Bekämpfung von Rechtsmissbrauch ist die Regelung überdies dahingehend auszugestalten, dass – innerhalb des Anwendungsbereichs von Rechtsmissbrauch – bei besonders aufwendigen Verfahren nach vorgängiger

					Abmahnung der betroffenen Person kein maximales Kostendach mehr gilt, sondern über den angemessenen Unkostenbeitrag hinaus die effektiven Kosten geltend gemacht werden dürfen. Dies ist mit rechtsstaatlichen Grundsätzen durchaus vereinbar bzw. von ihnen geradezu gefordert, muss es doch auch darum gehen, den Auskunftspflichtigen vor uferlosem Aufwand aufgrund von klarem Rechtsmissbrauch zu schützen. In der Formulierung von Art. 20 Abs. 1 VE-DSG ist deshalb das Wort **„kostenlos" ersatzlos zu streichen** (vgl. im Übrigen zu Art. 21 VE-DSG). Alternativ wäre analog Art. 12 Abs. 5 lit. a DSGVO dem Bundesrat die Kompetenz einzuräumen, die Ausnahmen der Kostenlosigkeit auf Verordnungsstufe festlegen zu können. Ohne diese Ermächtigung können keine Ausnahmebestimmungen Eingang in die Verordnung finden (vgl. zum Rechtsmissbrauch und den Verfahrenskosten ferner zu Art. 21 VE-DSG.
swissICT	DSG	20	2	b	Wir empfehlen entsprechend der bewährtem heutigen Regel die Präzisierung, dass die Auskunft nur die Kategorien der bearbeiteten Personendaten beinhalten muss. Dies entspricht auch Art. 15 lit. b DSGVO.
swissICT	DSG	20	2	e	Im Rahmen der allgemeinen Auskunftspflicht darf die geforderte Information über automatische Einzelfallentscheidungen nicht eine detaillierte Auflistung aller in der Vergangenheit ausgeführten automatischen Einzelfallentscheidungen verlangen. Vielmehr sollte eine allgemeine Information über auomatisierte Einzelfallentscheidungen genügen. Aus diesem Grund ist auch Art. 20 Abs. 3 zu streichen (vgl. sogl.).
swissICT	DSG	20	2	f	Wir erachten es als ausreichend, wenn die Herkunft der Personendaten dann angeben werden muss, wenn die Daten nicht bei der betroffenen Person selbst erhoben wurden. Dies entspricht Art. 15 Abs. 1 lit. g DSGVO. Anpassungsvorschlag: *f. Die verfügbaren Informationen über die Herkunft der Personendaten, falls diese nicht bei der betroffenen Person erhoben wurden.*

swissICT	DSG	20	2	g	„Empfänger“ der Daten schliesst auch Auftragsdatenbearbeiter ein. Es ist nicht praktikabel, sämtliche Auftragsbearbeiter inkl. Identität und Kontaktdaten zu nennen. Die DSGVO verlangt denn auch nur die Angabe von Kategorien von Empfängern.
swissICT	DSG	20	3		**Kernanliegen: Streichung der besonderen Auskunftspflicht bei Entscheidungen in Art. 20 Abs. 3 VE-DSG** Ein individuelles Auskunftsrecht mit Bezug auf Ergebnis, Zustandekommen und Auswirkungen jeder Entscheidung ist aus grundsätzlichen Überlegungen abzulehnen. Das Auskunftsrecht muss sich wie nach geltendem Recht auf kategorielle Informationen beschränken (wie bspw. die Auskunft zu Weitergaben an Dritte, bei denen weder alle Weitergaben noch alle Empfänger zu nennen sind, sondern nur die Kategorien der Empfänger). Die vorgeschlagene Auskunftspflicht bei Entscheidungen nach Art. 20 Abs. 3 VE-DSG würde die Auskunftspflicht daher enorm ausweiten. Sie wäre entsprechend massiv aufwendiger als bisher, ohne dass damit ein besserer Schutz der betroffenen Personen erreicht würde. Sehr viele Entscheidungen liegen ferner im Rahmen dessen, was für die betroffenen Personen ohne weiteres erkennbar ist (vgl. Art. 4 Abs. 3 VE-DSG). Die vom VE-DSG vorgeschlagene Regelung geht zudem klar über den von den EU-Anforderungen gesetzten Rahmen hinaus (vgl. Art. 15 Abs. 1 lit. h DSGVO). Dies stellt einen kontraproduktiven Swiss Finish dar, welcher dem Regulierungsziel der Äquivalenz entgegen steht und deshalb abzulehnen ist. Der von Art. 20 Abs. 3 Halbsatz 2 VE-DSG geforderte Umfang des Auskunftsrecht („Informationen über Ergebnis, Zustandekommen und Auswirkungen der Entscheidung“) ist mit Blick auf die anderweitig im VE-DSG bereits bestehenden weitreichenden Informationspflichten ferner weder sinnvoll noch nötig. Er produziert ohne Mehrwert z.B. in Form von mehr Transparenz unnötigen zusätzlichen Administrativaufwand. Eine derart weitgehende Auskunftspflicht ist datenschutzrechtlich nicht zu rechtfertigen. Insbesondere die Anwendung auf jede Art von Entscheidungen – nicht nur auf automatisierte Einzelfallentscheidungen – ist viel zu weitgehend. Sie könnte ausserdem zu einer Offenlegung von Geschäftsgeheimnissen z.B. in Form von internen Entscheid- und Ablaufverfahren führen (dazu bereits oben zu Art. 15).

					Die Regelung würde schliesslich zu Unrecht eine Vermischung des allgemeinen Auskunftsrechts mit individuellen Auskünften zu Einzelfallentscheidungen produzieren. Auskünfte nach Art. 20 VE-DSG müssen in allgemeiner, übersichtlicher und leicht verständlicher Form erfolgen. Sie dürfen deshalb nicht mit einer Auflistung sämtlicher in der Vergangenheit durchgeführten individuellen Entscheidungen wie z.B. automatisierten Einzelfallentscheidungen ergänzt werden. Solches würde den Rahmen sprengen und wäre für den Adressaten nicht mehr verständlich, sondern im Gegenteil verwirrend. Deshalb ist Abs. 3 von Art. 20 VE-DSG hier systematisch falsch zugeordnet und gehört – wenn schon – zur gesamtheitlichen Regelung von Art. 15 VE-DSG. Zusammenfassend ist die Regelung von Art. 20 Abs. 3 VE-DSG in Art. 20 zu streichen und stattdessen in die Regelung von Art. 15 DSG zu integrieren. Auch diese Integration muss sich aber an die vorstehend und überdies zu Art. 15 VE-DSG skizzierten Grundsätze halten und sich insbesondere auf eine sehr generelle Darlegung der Funktionsweise automatisierter Einzelfallentscheide beschränken.
swissICT	DSG	20	5		Wir schlagen vor, den 2. Satz von Art. 20 Abs. 5 VE-DSG zu streichen.
swissICT	DSG	20bis (neu)			**Kernanliegen: Korrektur der Ausnahmetatbestände und Missbrauchsschutz** Die Ausnahmetatbestände von Art. 21 VE-DSG sind zu eng formuliert und inkonsistent. So ist nicht einzusehen, weshalb die Informationspflicht bei Unmöglichkeit und Unzumutbarkeit nur entfallen soll, soweit der Verantwortliche die betreffenden Daten nicht Dritten bekannt gibt (Art. 14 Abs. 4 lit. a VE-DSG). Das widerspricht auch der Regel, dass die Informationspflicht generell nicht nachzuholen ist, wenn dies nicht unmöglich oder unzumutbar ist (Art. 14 Abs. 5 VE-DSG). Richtigerweise muss die Informationspflicht immer entfallen, wenn die Information nicht möglich oder unzumutbar ist, wie es auch die DSGVO vorsieht (Art. 12 Abs. 5 lit. b DSGVO). Dies gilt umso mehr, als das Auskunftsrecht neu bei jeder Datenbearbeitung greift, da es keine Beschränkung mehr auf Datensammlungen geben wird. Nicht nachvollziehbar ist auch, weshalb die Informationspflicht nach gesetzlicher Vorschrift nur bei indirekter Beschaffung durch Dritte entfallen soll (Art. 14 Abs. 2 lit. a VE-DSG). Umso mehr muss

					die Informationspflicht bei direkter Beschaffung entfallen. Zudem ist abzulehnen, dass die Informationspflicht nur dann entfällt, wenn eine gesetzliche Vorschrift *dieses Entfallen* vorsieht (Art. 14 Abs. 3 lit. a VE-DSG). Richtig wäre, die Informationspflicht entfallen zu lassen, wenn und soweit die gesetzliche Vorschrift *die Bearbeitung* vorschreibt, denn dann besteht bereits gesetzliche Transparenz, so dass die Auskunft nicht mehr erforderlich ist. Dem Auskunftsverpflichteten muss sodann nach allgemeinen Rechtsgrundsätzen generell das Recht zustehen, das Auskunftsrecht unter Berufung überwiegender eigener Interessen einzuschränken oder sogar zu verweigern. Um dieser Regel griffige Konturen zu verleihen, sind – ohne Anspruch auf Vollständigkeit – typische Fallgruppen direkt im Gesetz aufzuführen. Das datenschutzrechtliche Auskunftsrecht dient der Beseitigung eines allfälligen Informationsgefälles zwischen betroffener Person und Auskunftspflichtigem. Die datenschutzrechtliche Begründung für das Auskunftsrecht fokussiert somit auf diejenigen Daten, welche die betroffene Person gar nicht kennt und aufgrund aller Umstände, z.B. mangels Erkennbarkeit (vgl. Art. 4 Abs. 3 VE-DSG), vernünftigerweise auch gar nicht kennen kann. Naturgemäss nicht im Fokus sind demzufolge Daten, welche die betroffene Person bereits kennt bzw. erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen aller Art. Dies ist schon deshalb richtig, weil es nicht Aufgabe des Auskunftspflichtigen sein kann, einer betroffenen Partei wiederholt immer wieder und sogar unter Strafandrohung dieselben Daten liefern zu müssen, nur weil die betroffene Person z.B. den Aufwand sparen will, diese bereits erhaltenen Daten z.B. in Form von Verträgen bei sich selbst in vernünftiger Form aufzubewahren. Ebenfalls nicht herauszugeben sind Daten, welche aufgrund gesetzlicher Pflichten zu erheben und/oder aus bestimmten Gründen der betroffenen Person nicht bekannt gegeben werden dürfen, z.B. wegen Vereitelungs- oder Kollusionsgefahr in Zusammenhang mit Abklärungen zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption. Selbstredend darf das datenschutzrechtliche Auskunftsrecht auch nicht dazu führen, dass – ebenfalls rechtlich geschützte – Geschäftsgeheimnisse (vgl. Art. 162 StGB) herausgegeben werden müssen. Nicht herausgabepflichtig sind überdies rein intern bearbeitete Daten.

					Der Auskunftsverpflichtete ist auch vor Auskunftsbegehren zu schützen, welchen klarer Rechtsmissbrauch zu Grunde liegt. Typische Fallgruppen klar rechtsmissbräuchlicher Geltendmachung des Auskunftsrechts sind aus Gründen der Rechtssicherheit direkt im Gesetzestext aufzuführen, insbesondere die Geltendmachung des Auskunftsrechts ohne sachlichen Grund oder die exzessive Geltendmachung des Auskunftsrechts mit häufiger Wiederholung, welche sachlich nicht nachvollziehbar ist. Zielführend ist es deshalb, direkt im Gesetz in Art. 21 VE-DSG aufzuführen, dass Daten der vorstehend skizzierten Art nicht herauszugeben sind. Auch in der DSGVO finden sich solche Ausnahmen und Einschränkungen. Zusammenfassend handelt es sich insbesondere um nachfolgend aufgeführte Daten. Formulierungsvorschlag: Art. 20bis VE-DSG: Nicht der Auskunftspflicht unterstehen folgende Datenkategorien: a) Bereits erhaltene Daten, welche die betroffene Person bereits erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen; b) aufgrund einer gesetzlichen Pflicht bearbeitete Daten, z.B. zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption; c) Daten, welche vom Auskunftspflichtigen als Geschäftsgeheimnisse qualifiziert werden; d) rein intern bearbeitete Daten; e) Daten über Drittpersonen; f) unter rechtsmissbräuchlichen Umständen herausverlangte Daten, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder mit häufiger, sachlich nicht nachvollziehbarer Wiederholung.
swissICT	DSG	21			Mit Blick auf die dargelegte Gefahr des Missbrauchs des Auskunftsrechts, namentlich der Zweckentfremdung zur Beweismittelausforschung, ist ein Mechanismus vorzusehen, der das Auskunftsrecht für die datenschutzfremde Beweismittelausforschung verhindert. Dafür wäre eine Kostenregelung sinnvoll, die sich bspw. am Rechtsschutzinteresse des Gesuchstellers orientiert. Falls datenschutzfremde Interessen überwiegen, könnte eine höhere Gebühr verlangt werden; im umgekehrten Fall

					wäre eine geringe Gebühr angezeigt (vgl. zu den Kosten einer Auskunft ferner zu Art. 20 Abs. 1 VE-DSG). Vorschlag für einen Art. 21 Abs. 3 VE-DSG: *Bei offensichtlich unbegründeten oder aus anderen Gründen missbräuchlichen Auskunftsersuchen kann der Verantwortliche für die Erteilung der Auskunft ein angemessenes Entgelt verlangen.* Eine analoge Formulierung drängt sich überdies auch bei Art. 14 in einem neuen Abs. 6 auf.
		44	3		Vorsorgliche Massnahmen im Bereich der Datenbearbeitung können massive Konsequenzen für Unternehmen haben. Sie können einen Betrieb lahmlegen. Es sollte dem Gericht aufgrund des konkreten Einzelfalles überlassen sein zu entscheiden, die aufschiebende Wirkung zu entziehen.
swissICT]	DSG	45			**Kernanliegen: Einschränkung der Anzeigepflicht des EDÖB.** Die Pflicht des Beauftragten, Strafverfolgungsbehörden zu informieren, sollte nicht über Art. 58 DSGVO hinausgehen. Nach der DSGVO besteht ein Recht zur Anzeige, nicht jedoch eine Pflicht. Eine allgemeine Anzeigepflicht unterläuft die Informations- und Beratungspflicht des EDÖB nach Art. 49 lit. a VE-DSG: Wer mit einer Anzeige rechnen muss, wird sich hüten, in unklaren Fällen auf den EDÖB zuzugehen. Dies gilt ganz besonders angesichts der extrem weitgehenden Strafdrohung nach dem VE-DSG. Eine vertrauensvolle Zusammenarbeit mit dem EDÖB wird damit unmöglich.
swissICT	DSG	50 ff.			**Kernanliegen: konzeptionelle Änderung des Sanktionsmechanismus; angemessene Sanktionen gegen Unternehmen statt strafrechtliche Verfolgung Privater** Art. 50 ff. VE-DSG enthalten Strafbestimmungen gegen natürliche Personen. Dies steht im Gegensatz zu den entsprechenden europäischen Regelungen, die primär Sanktionen gegen Unternehmen vorsehen. Bei der Ausgestaltung des Sanktionssystems, namentlich Strafsanktionen oder Verwaltungssanktionen, lässt die DSGVO den Mitgliedstaaten Spielraum (vgl. Art. 83 Abs. 9 DSGVO sowie Erwägung 151 DSGV).

					Daher bleibt im Bereich der Aufsicht bzw. der Durchsetzung insofern ein wohl nicht unbeträchtlicher Handlungsspielraum, der eine wortwörtliche Übernahme der DSGVO nicht erforderlich macht. Verlangt wird ein der Sache nach **gleichwertiges Datenschutzniveau**, wobei im Bereich der Aufsicht/Sanktionierung im Wesentlichen wirksame, verhältnismäßige und abschreckende Sanktionen gefordert werden (Erwägung 152 DSGVO). Das Konzept des VE-DSG, zusammen mit der grossen Unbestimmtheit der Straftatbestände (dazu unten), führt somit zu einer nicht zu rechtfertigenden Bedrohung derjenigen Personen, die mit Personendaten umzugehen haben – und zwar gerade derjenigen Personen, die unternehmensintern die Einhaltung des Datenschutzes sicherstellen müssen und die durch das Datenschutzrecht deshalb zu schützen sind. Das ist auch deshalb verfehlt, weil Datenschutzverstösse viel eher an der unternehmensweiten Komplexität datenschutzrechtlicher Setups liegen (z.B. grenzüberschreitende Sachverhalte, zunehmender Trend zu Arbeitsteiligkeit, etc.) und nicht an individuellem Verschulden. Einzelne Personen zu bestrafen, wäre daher nicht sachgerecht. Es wäre zudem verfassungsrechtlich höchst bedenklich und ein klar überschiessender Swiss Finish, der massive Auswirkungen auf den Wirtschaftsstandort Schweiz hätte. Dieses verfehlte Konzept ist deshalb aufzugeben. Gleichzeitig stellt sich die Frage, ob das Strafrecht bei Datenschutzverstössen überhaupt das richtige Mittel sein kann (mit Ausnahme qualifizierter Verstösse wie etwa nach Art. 52 VE-DSG, der allerdings ebenfalls zu weit geht). Auch ein primäres Unternehmensstrafbarkeit ist daher zumindest kritisch zu hinterfragen, wenn nicht direkt abzulehnen: Ein eigentliches Unternehmensstrafrecht fehlt in der Schweiz (vgl. Art. 53 VE-DSG), und die punktuelle Unternehmensstrafbarkeit nach Art. 102 Abs. 1 StGB ist für Datenschutzverstösse gänzlich ungeeignet. Das zeigt ein Vergleich mit den Verstössen, die eine solche Strafbarkeit nach heutigem Recht auslösen können (z.B. Terrorismusfinanzierung, Korruptionsdelikte und Geldwäscherei) – Datenschutzverstösse können nicht mit organisierter Schwerkriminalität auf die gleiche Stufe gestellt werden. Die Ausgestaltung eines passenden verwaltungsrechtlichen Sanktionssystems für die Schweiz im Zusammenhang mit Verstössen gegen den Datenschutz bedarf aber zweifellos noch vertiefter Überlegungen. Aus den vorgenannten Gründen ist aber zu prüfen, ob nicht stattdessen Verwaltungssanktionen gegen fehlbare Unternehmen vorzusehen sind. Dies entspräche auch dem von der Mehrheit der europäischen Mitgliedstaaten gewählte Sanktionssystem.

					Dabei ist aber davon abzusehen, Verwaltungsverfahren anderer Bundesgesetze mit Verwaltungssanktionen ohne Weiteres und undifferenziert zu übernehmen. Hierzu folgende Ausführungen: Es fragt sich insbesondere, auf welche Weise die **Sanktionsbemessung** vorgenommen werden kann, dass sie nicht nur wirksam und abschreckend, sondern vor allem auch verhältnismässig ist (die Verhältnismässigkeit ist eine Anforderung der ERK 108 ebenso wie der DSGVO). Dabei ist zunächst eine angemessene **Obergrenze** für Unternehmensbussen festzulegen. Wichtig ist dabei, dass die Bussendrohung nicht kontraproduktiv wirkt. Die Obergrenze darf nicht so hoch ausfallen, dass ein Unternehmen in der Anwendung des Datenschutzrechts gelähmt wird. Insbesondere darf der (in der DSGVO sogar gestärkte) risikobasierte Ansatz nicht dadurch unterlaufen werden, dass Risiken durch übermässige Bussen untragbar werden. Denkbar wäre ein Höchstbetrag von CHF 500'000. Der Vollständigkeit halber sei nochmals erwähnt, dass die **Angemessenheitsentscheidung durch die EU-Kommission nicht verlangt, den Bussenrahmen der DSGVO zu übernehmen** (s. oben). Denkbar ist ferner auch ein unterschiedlich hoher Bussenrahmen je nach dem Sinn der verletzten Norm. Sollte man sodann bei der Sanktionsbemessung den Umsatz des betroffenen Unternehmens in Betracht ziehen wollen, so wäre jedenfalls sorgfältig abzuwägen, welcher Umsatz massgeblich ist – der Gesamtumsatz des betroffenen Bereichs, des betroffenen Projekts, der allfällig betroffenen Tochtergesellschaft oder des betroffenen Konzerns. Ebenso wichtig sind sodann die Kriterien der Sanktionsbemessung. Dabei muss eine angemessene Compliance des betroffenen Unternehmens erheblich mildernd ins Gewicht fallen: Datenschutzverstösse sind nicht zuletzt aufgrund der Vielzahl unbestimmter Begriffe und der Bedeutung von Wertungsentscheidungen und Risikoeinschätzungen nicht in jedem Falle vermeidbar. Sanktionswürdig ist daher nicht so sehr der Verstoss im Einzelfall – besondere Fälle vorbehalten –, sondern eine allenfalls ungenügende Prävention durch das Unternehmen. Bei einer Bemessung sollte ebenfalls eine allfällige proaktive Meldung einer Verletzung durch das Unternehmen unter Darlegung der Massnahmen berücksichtig werden. Hiermit wird durch die Revision verstärkt gewollte Kooperation zwischen dem Beauftragten und den Unternehmen Rechnung getragen.

					Wie erwähnt, sind ferner viele Pflichten des VE-DSG und damit auch die daraus abgeleiteten strafrechtlichen Tatbestände gemäss Art. 50 ff. VE-DSG zu wenig konkret. Art. 50 ff. VE-DSG erfüllen damit nicht die im Verfassungsrecht begründete Regel von „nulla poena sine lege (stricta, certa)". Vor diesem Hintergrund ist die Unbestimmtheit einer Mehrzahl der (Straf-)Tatbestände gem. Art. 50 f. VE-DSG äusserst bedenklich. Viele der Pflichten des VE-DSG und damit auch die daraus abgeleiteten Straftatbestände sind viel zu offen formuliert, dass es für ein Unternehmen auf Grund des erheblichen Auslegungsspielraumes schwierig sein wird zu verstehen, was es genau tun darf und was nicht. Aus diesem Grund sind die in dieser Stellungnahme an den betreffenden Stellen geforderten Präzisierungen umso wichtiger.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
swissICT	6 Abs. 2 lit. c	Die Erläuterungen sollten klarstellen, dass unter „Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen" auch die „Abwehr" bzw. „Verteidigung" gegen Rechtsansprüche zu verstehen sind.
swissICT	13 Abs. 3	In den Erläuterungen sollte präzisiert werden, dass bei allfälligen Änderungen keine Nachinformation erfolgen muss.
swissICT	15 Abs. 1	Siehe obige Bemerkungen zu Art. 15 Abs. 1.

SWISSMEM

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz
Bundesrain 20
Postfach
3003 Bern

BA Justiz
E -4. April 2017
Act

Arbeitgeberpolitik

Pfingstweidstrasse 102
Postfach
CH-8037 Zürich
Tel. +41 44 384 41 11
www.swissmem.ch
arbeitgeber@swissmem.ch

Zürich, 3. April 2017 Vak/Hac

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Damen und Herren

Swissmem vertritt die Interessen von mehr als 1'000 Unternehmen der schweizerischen Maschinen-, Elektro- und Metall-Industrie (MEM-Industrie) sowie verwandter technologieorientierter Branchen.

Die MEM-Industrie stellt einen der grössten industriellen Sektoren der Schweizer Wirtschaft dar und erbringt ungefähr die Hälfte der industriellen Wertschöpfung. Dies entspricht über 7 Prozent des Bruttoinlandprodukts der Schweiz.

Die MEM-Industrie ist mit rund 320'000 Beschäftigten die mit Abstand grösste industrielle Arbeitgeberin und bestreitet mit Exporten von 63 Milliarden CHF 30 Prozent der gesamten Güter-Ausfuhren der Schweiz.

Die Branche wird durch KMU geprägt; 99 Prozent der Unternehmen beschäftigen weniger als 250 Mitarbeitende. Über 59 Prozent der ausgeführten Güter der MEM-Industrie werden in die EU exportiert.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und nehmen diese gerne wahr.

Zusammenfassung der wichtigsten Positionspunkte:

- **Swissmem stützt in Bezug auf die vorgeschlagene Revision des Datenschutzgesetzes die Argumentation von economiesuisse und des VUD bzw. deren Stossrichtung. Die nachfolgende Stellungnahme beschränkt sich deshalb auf einige aus unserer Sicht besonders kritische Punkte der Revision.**
- **Die Schweiz verfügt über ein gutes und bewährtes Datenschutzgesetz. Dies gilt es punktuell zu modernisieren, damit die Gleichwertigkeit gegenüber der europäischen Gesetzgebung beibehalten werden kann.**

SWISSMEM

2. Stellungnahme

Im Rahmen der Mitarbeit in der Arbeitsgruppe Datenschutz von economiesuisse sind auch Anliegen der MEM-Branche in die Stellungnahme von economiesuisse eingeflossen. Aus diesem Grund verweist Swissmem grundsätzlich auf diese Stellungnahme. Im Folgenden nimmt Swissmem zu den für die MEM-Branche besonders kritischen Themen separat Stellung.

Allgemeine Bemerkungen

Swissmem bedauert einerseits, dass die Bestimmungen zum betrieblichen Datenschutzbeauftragten gestrichen worden sind, kann doch heute in der Schweiz die Funktion des betrieblichen Datenschutzbeauftragten als etabliert angesehen werden. Andererseits wäre eine Verpflichtung aller Unternehmen, einen Datenschutzbeauftragen zu bestellen, mit einem insbesondere für KMUs unzumutbaren Kostenaufwand verbunden gewesen, verfügen diese Betriebe ja in der Regel nicht über die entsprechenden Fachspezialisten, um diese Aufgabe intern wahrzunehmen. Im Interesse der Verminderung des administrativen Aufwands sollte jedoch denjenigen Unternehmen, die über einen betrieblichen Datenschutzbeauftragten verfügen, gewisse Erleichterungen (z.B. betr. Meldepflichten) gewährt werden.

Die pauschale Anwendung der im VE-DSG vorgesehenen Pflichten auf alle Wirtschaftszweige erscheint uns nicht sachgerecht und wäre mit enormem Aufwand verbunden. Vielmehr ist ein risikoorientiertes und abgestuftes Modell vorzusehen: Strengere Bestimmungen sollten für Geschäftstätigkeiten gelten, welche besonders sensible Datenbearbeitungen umfassen, und weniger strenge Bestimmungen sollten bei Geschäftsmodellen zur Anwendung gelangen, in welchen keine oder nur in eingeschränktem Masse besonders sensible Daten bearbeitet werden. Auch bei den Pflichten ist ein risikobasierter Ansatz vorzukehren.

Swissmem erachtet die Ausweitung der Informationspflichten auf alle Personendaten als nicht zielführend. Sie bringt den Unternehmen Mehraufwand und auf Grund des öffentlich-rechtlichen Charakters der Bestimmungen und den daraus fliessenden Sanktionsfolgen zu erheblichen Problemen in der Praxis. Die Regel muss grundsätzlich im Sinne einer risikobasierten Transparenzpflicht überarbeitet werden. Konkret ist die Informationspflicht auf besonders schützenswerte Daten i.S.v. Art. 4 DSG der betroffenen Person zu beschränken.

Für eine grosse Anzahl von Unternehmen sind berufliche Personendaten (so genannte HR Daten) der einzige Bezugspunkt zum DSG. Dass diese auf demselben hohen Niveau geschützt werden sollen wie private Personendaten erscheint mir falsch. Insbesondere der Arbeitgeber sollte die Möglichkeit haben, berufliche Personendaten zwecks Auswertungen, Effizienzsteigerungen, Analysen etc. auch ohne spezielle Einwilligung der betroffenen Mitarbeitenden auswerten zu können. Der VE-DSG sollte deshalb für den Umgang mit beruflichen Personendaten ein spezifisches, tieferes Schutzniveau definieren, insbesondere betreffend Einwilligungsanforderungen und Transfer ins Ausland.

Bsp. Die Verwendung von Google Glases am Arbeitsplatz zwecks remote trouble shooting wird dazu führen, dass Mitarbeitende bei ihrer Tätigkeit gefilmt werden, und dass externe Dritte (z.B. Google) diese Daten zwangsläufig sehen und möglicherweise auch auswerten. Dabei geht es selbstverständlich nicht primär um den Mitarbeitenden selber, sondern vielmehr um seine Tätigkeit und wie er diese ausübt. Häufig kann es sich zudem ergeben, dass Mitarbeitende rein zufällig auf dem Filmmaterial zu sehen sind, weil sie in der Peripherie des filmenden Mitarbeiters tätig waren Dabei wird sich die Frage stellen, ob alle Mitarbeitenden ihre explizite Einwilligung zur Übermittlung und Auswertung solchen Bildmaterials

SWISSMEM

- **Die Revision soll kein administratives «Monster» schaffen, sondern soll so gestaltet sein, dass auch weiterhin ein praxisnahes und schlankes Datenschutzgesetz bestehen bleibt.**
- **Swissmem erachtet verschiedene Informations- und Meldepflichten als zu weitgehend und überschiessend. Dies generiert für die Unternehmen unverhältnismässigen Aufwand und eine «Flut» an Informationen und Meldungen. Ebenso lehnen wir die damit verbundenen Pflichten, welche die Offenlegung von Geschäftsgeheimnissen beim EDÖB zur Folge haben, ab bzw. diese sind substantiell zu reduzieren. Dies betrifft insbesondere automatisierte Einzelfallentscheide, Datenschutz-Folgenabschätzungen und Meldungen von Datenschutzverstössen.**
- **Privat strafrechtliche Sanktionen sind weder verhältnismässig noch zielführend. Sie führen zu einer nicht sachgerechten Kriminalisierung der im Unternehmen mit der Datenbearbeitung beauftragten Mitarbeitenden. Zudem erachtet Swissmem die Bestrafung für fahrlässiges Verhalten als nicht sachgerecht. Die vorgesehenen Strafbestimmungen sind deshalb abzulehnen.**

1. Allgemeines

Swissmem begrüsst grundsätzlich die Revision des Datenschutzgesetzes, obwohl das bestehende Datenschutzgesetz auch heute noch immer den Anforderungen vollumfänglich genügen würde. In Anbetracht der technologischen wie auch der internationalen Entwicklungen im Bereich Datenschutz ist es für die Schweiz jedoch wichtig, dass der Zugang insbesondere zum EU-Raum nicht unnötig einschränkt wird. Damit das Schweizer Datenschutzgesetz aus Sicht der Europäischen Union als äquivalent betrachtet werden kann, sollte es jedoch ausreichend sein, wenn die grundlegenden Garantien eingehalten werden. Zusätzlich sollte sich das DSG an der Konvention 108 des Europarates anlehnen, welche für die Schweiz ebenfalls verbindlichen Charakter hat.

Aus wirtschaftspolitischer Sicht darf ein revidiertes Datenschutzgesetz die Innovationsfähigkeit der Schweizer Wirtschaft weder behindern noch Leitplanken setzen, welche diese unverhältnismässig beschränkt. Ein guter und wirtschaftsfreundlicher Datenschutzrahmen trägt dazu bei, die Wettbewerbsfähigkeit des Wirtschaftsplatzes Schweiz zu stärken. Insbesondere mit Blick auf die KMUs muss ein revidiertes Datenschutzgesetz einfach zu handhaben sein. Übertrieben weitgehende Bestimmungen («Swiss Finish»), welche zusätzlich einen unnötigen administrativen Aufwand verursachen, sind zu streichen.

Im Rahmen dieser Revision muss es das Ziel bleiben, kein praxisfernes, bürokratisches Monster zu erschaffen, sondern ein wie bisher schlankes, praxisnahes Gesetz zu bewahren, welches sich viele Jahre in der Praxis bestens bewährt hat. Es gilt das Schweizer Datenschutzgesetz gezielt zu stärken und zu modernisieren, damit gegenüber der europäischen Gesetzgebung die Gleichwertigkeit erhalten bleibt.

geben müssen, oder ob dies pauschal im Rahmen einer allgemeinen Einwilligung im Arbeitsvertrag abgewickelt werden kann

Art. 11 VE-DSG – Sicherheit für Personendaten

Die Sicherheit der Personendaten wird in der Praxis von grosser Tragweite sein. Dass der Bundesrat und nicht die Unternehmen selber entscheiden soll, welche Mittel zum Schutz sensibler Daten anzuwenden sind, scheint uns dabei grundsätzlich problematisch. Es sollte in der Eigenverantwortung der Unternehmen liegen, angemessene Schutzmittel zu definieren.

Art. 16 VE-DSG – Datenschutz-Folgenabschätzung

In Art. 16 VE-DSG wird mit der Datenschutz-Folgenabschätzung (Privacy Impact Assessment) ein Instrument eingeführt, welches aufgrund seiner offenen und unklaren Formulierung in der Praxis dazu führen wird, dass für praktisch alle Datenbearbeitungen im Vorfeld umfangreiche Abklärungen vorzunehmen sind. Einen solchen Aufwand müssen aufgrund der vorgesehenen Sanktionierung bei Verstoss unter Umständen auch KMUs betreiben. Dies ist unseres Erachtens zu verhindern oder zumindest stark einzuschränken. Eine Konkretisierung dieser Bestimmung sowie eine Beschränkung auf Fälle, bei denen ein «**hohes Risiko**» besteht, ist in jedem Fall vorzunehmen. Darüber hinaus ist die Bestimmung dahingehend zu präzisieren, dass ein Risiko für eine Persönlichkeitsverletzung bestehen muss.

Die anschliessenden umfangreichen Meldepflichten sind ein klares «Swiss Finish»; sie sind unverhältnismässig und greifen in die Geheimsphäre der Unternehmen ein. Problematisch ist auch die lange Frist, innert welcher der EDÖB Einwände mitteilen oder später eine Untersuchung einleiten kann. Damit werden falsche Anreize gesetzt. In der Gesamtheit bringt die Bestimmung keinen Mehrwert, führt jedoch zu erheblichen Rechtsunsicherheiten und innovationshemmenden Verzögerungen.

Eine Meldung an den EDÖB sollte nur dann erfolgen müssen, wenn **nach** ergriffenen Schutzmassnahmen ein grosses Restrisiko verbleibt. Es ist klar zu regeln, welche Informationen weitergeleitet werden müssen. Weiter ist die vorgesehene Reaktionszeit des EDÖB auf einen Monat zu reduzieren.

Eine Ausnahme der Meldepflicht sollte zumindest für Unternehmen mit einem betrieblichen Datenschutzbeauftragten vorgesehen werden.

Art. 17 VE-DSG Meldung von Verletzungen des Datenschutzes

Wie in Art. 16 VE-DSG finden wir auch hier in Art. 17 einen «Swiss Finish», welcher weit über das Ziel hinausgeht. Diese Meldepflicht von Datenschutzverletzungen findet im Vorentwurf auf jede Datenschutzverletzung Anwendung. Es gibt jedoch für eine derart weitgefasste Meldepflicht keinen Anlass, und sie verursacht bei den Unternehmen einen nicht vertretbar hohen administrativen Aufwand. Der Begriff des «Data Breach» sollte daher analog der DSGVO formuliert werden; hier ist eine Kompatibilität auch aus praktischen Überlegungen sinnvoll. Die DSGVO erfasst in der entsprechenden Bestimmung lediglich Sicherheitsverstösse, die zu einem Verlust des Gewahrsams an den Daten führt.

Die parallele Bestrafung der Meldepflicht wie auch der Verletzung der Datensicherheit betrachtet Swissmem als rechtsstaatlich bedenklich, da es die Mitarbeitenden zwingt, sich gegenseitig anzuzeigen. Unseres Erachtens ist eine Meldung zudem nur sinnvoll, sofern eine grössere Anzahl von Personen betroffen ist und die Datenschutzverletzung eine bestimmte Schwere erreicht. Alles andere ist in der Praxis nicht umsetzbar.

Art. 19 VE-DSG Dokumentationspflicht

Swissmem stellt sich auf den Standpunkt, dass der Inhalt und das Ausmass der Pflicht zur Dokumentation der Datenbearbeitung gemäss lit. a einzig auf das Führen eines Verzeichnisses sämtlicher Datenverarbeitungen beschränkt werden sollte, für die der Verantwortliche zuständig ist. In keinem Fall sollte diese Pflicht erweitert werden und über die in Art. 30 DSGVO enthaltenen Pflichten hinausgehen. Eine darüber hinausgehende Erweiterung dieser Dokumentationspflichten würde wiederum für die Wirtschaft und die Unternehmen zu einem unverhältnismässigen Aufwand führen, welcher durch keinen Mehrwert für den Datenschutz gerechtfertigt ist.

Die Informationspflicht gemäss Art. 19 lit. b VE-DSG soll höchstens für die Berichtigung, Löschung und Vernichtung von Daten gelten. Ausgenommen davon muss die Verletzung des Datenschutzes und die Einschränkung der Bearbeitung gemäss Art. 25 Abs. 2 oder 34 Abs. 2 VE-DSG sein.

Unseres Erachtens geht zudem die Pflicht, die Empfänger von Personendaten über Berichtigungen, Löschungen etc. zu informieren, deutlich zu weit. Vorgänge dieser Art finden laufend statt, und deren Mitteilung an Empfänger macht keinerlei Sinn. Die Pflicht zur Information ist auf Fälle zu beschränken, in welchen die betroffene Person dies verlangt und über ein schützenswertes Interesse verfügt.

Dass die Pflicht zur Information auch eine solche über Datenschutzverstösse umfasst, ist nicht nachvollziehbar. Sie geht sogar weiter als die Pflicht zur Information der betroffenen Person selbst. Die DSGVO sieht auch keine solche Information vor. Sie ist daher zu streichen.

Art. 23 VE-DSG

Swissmem ist der Meinung, dass die Einwilligung für ein Profiling gestrichen werden muss. Es wird nicht bestritten, dass es in der Praxis heikle Profilings gibt, jedoch sind viele dieser Vorgänge völlig harmlos (z.B. Berechnung des Alterskapitals einer Person gemäss BVG). Es scheint uns praxisfremd, auch für solche Vorgänge die neu strengeren Voraussetzungen zur Anwendung zu bringen und diese Handlung aufgrund des neu vorgeschlagenen Wortlauts als Persönlichkeitsverletzung zu betrachten. Es erscheint uns nicht sachgerecht, dass bereits im Rahmen der Anwendung der Bearbeitungsgrundsätze das mit einer Datenbearbeitung verbundene Risiko für die betroffene Person zu berücksichtigen ist. Eine solche Regelung würde die Unternehmen und insbesondere die Personalabteilungen zwingen, für beinahe sämtliche Datenbearbeitungen vorgängig ein Einverständnis einzuholen.

Art. 50 – 55 VE-DSG Strafbestimmungen

Die im VE-DSG vorgesehenen Strafbestimmungen lehnt Swissmem ab. Diese Strafbestimmungen kriminalisieren unsachgemäss sämtliche mit dem Datenschutz in Berührung kommenden Mitarbeitenden in einem Unternehmen. In der Praxis wäre sich eine Vielzahl dieser Mitarbeitenden (insbesondere in den kleinen Unternehmen) gar nicht bewusst, welchen formellen mit Strafe bedrohten Handlungsweisen sie ausgesetzt sind. Dies macht weder aus Sicht des Datenschutzes noch aus betriebswirtschaftlicher Perspektive irgendeinen Sinn. Die Gefahr der Strafverfolgung wird es zudem schwieriger machen, geeignete Fachleute für die betreffenden Stellen in den Unternehmen zu rekrutieren.

Swissmem erachtet die Bestrafung **fahrlässigen Verhaltens** als absolut nicht sachgerecht und ist zudem auch europarechtlich nicht gefordert. Es handelt sich auch hier um einen «Swiss Finish», welcher weder erforderlich noch notwendig ist. Eine solche Sanktionierung würde den oben erwähnten Effekt noch verstärken.

SWISSMEM

Eine allfällige Sanktionierung sollte in erster Linie das Unternehmen betreffen und nicht die einzelnen Mitarbeitenden. Für die Verschärfung der heute in Art. 35 DSG geregelten **beruflichen Schweigepflicht** besteht kein Anlass, und die bestehende Norm ist so zu belassen. Der Vorschlag im VE-DSG würde Unternehmen dazu zwingen, ein «scharfes» Berufsgeheimnis zu befolgen, für das kein Bedarf besteht und das in der Praxis auch nicht gelebt würde.

3. Fazit

Swissmem anerkennt die im Vorentwurf zur Revision des Datenschutzgesetzes geleistete Arbeit des Bundesamtes für Justiz. Wir sehen jedoch noch einige Mängel, welche nun nach Beendigung der Vernehmlassung korrigiert werden müssen.

Neben der Überarbeitung verschiedener Bestimmungen bedarf es nach Meinung von Swissmem einiger weiterer grundsätzlichen Überlegungen zur Konzeption des DSG. Der Eindruck ist nicht von der Hand zu weisen, dass der Entwurf zu wenig die Praktikabilität und die Auswirkungen auf die Wirtschaft und die Unternehmen berücksichtigt, welche diese Bestimmungen im Alltag umsetzen müssen. Wie bereits erwähnt, sollte das revidierte Datenschutzgesetz schlank und praktikabel bleiben. Insbesondere der Umstand, dass der Vorentwurf in einigen Punkten grundlos über die Anforderungen des DSGVO hinausgeht, ist Grund genug, nochmals über die Bücher zu gehen.

Die Wirtschaft wird in vielen Fällen in den Anwendungsbereich des DSG und der DSGVO fallen und durch die parallele Anwendbarkeit der beiden Rechtserlasse belastet werden. Mit einem DSG, welches in verschiedenen Bestimmungen noch über die DSGVO hinausgeht, wird die Umsetzung und Beachtung dieser Bestimmungen für die Wirtschaft und die Unternehmen nochmals kostspieliger, als es bereits ohnehin ist. Dies kann aus Sicht der MEM-Industrie nicht akzeptiert werden.

Mit der Umsetzung eines revidierten Datenschutzgesetzes kommen erhebliche Kosten und Mehrarbeit auf die MEM-Industrie zu. Wir erinnern dabei nur an die verschärfte Datenschutz-Governance, die neuen und stark erweiterten Informations- und Auskunftspflichten und Strafbestimmungen. Die Schweizer Wirtschaft und insbesondere die MEM-Industrie setzen sich zum grossen Teil aus KMU-Betrieben zusammen. Diese Unternehmen müssten massiv in diesen Bereich investieren und die erforderlichen Prozesse implementieren und Dokumentationen schaffen. In Anbetracht der bereits aufgrund der Frankenstärke schwierigen Situation in der MEM-Branche werden den Unternehmen nochmals zusätzliche Kosten und administrativer Aufwand aufgebürdet. Dies schwächt nicht nur jedes einzelne Unternehmen per se, sondern den ganzen Wirtschaftszweig insgesamt. Aus diesem Grund bitten wir Sie, in der Botschaft des Bundesrats die notwendigen Korrekturen im oben erwähnten Sinne vorzunehmen.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme.

Freundliche Grüsse

Kareen Vaisbrot
Mitglied der Geschäftsleitung

Claudio Haufgartner
Stv. Bereichsleiter Arbeitgeberpolitik

Swiss Payment Association

Ohmstrasse 11, 8050 Zürich
office@swiss-p-a.ch, +41 (0)58 426 25 55

Bundesamt für Justiz
Herr Jonas Amstutz
Bundesrain 20
3003 Bern

Per Mail: jonas.amstutz@bj.admin.ch

Zürich, 4. April 2017

Vernehmlassung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz: Stellungnahme der Swiss Payment Association

Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 21. Dezember 2016 eröffnete Vernehmlassung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) und die Änderung weiterer Erlasse und bedanken uns für die Möglichkeit zur Stellungnahme. In der vorliegenden Eingabe äussern wir uns ausschliesslich zu den Regelungen des VE-DSG, welche die Privatwirtschaft betreffen, während auf eine Stellungnahme zu den übrigen Regeln des VE-DSG und zu den Anpassungen in Zusammenhang mit den Schengener Übereinkommen verzichtet wird.

Vorab gestatten wir uns den Hinweis, dass der Swiss Payment Association (SPA) alle Schweizer Herausgeber[1] (Issuer) von Kreditkarten der internationalen Kartenorganisationen angehören. Als Branchenorganisation vertritt die SPA die Positionen ihrer Mitglieder im Dialog mit all deren Anspruchsgruppen.

Management Summary

Wettbewerbsfähigkeit stärken und Chancen der Digitalisierung nutzen
Die zentralen Anliegen nach Förderung der Wettbewerbsfähigkeit der Schweizer Wirtschaft, Gewährleistung des freien Verkehrs personenbezogener Daten und Chancennutzung im Bereich der Digitalisierung werden vom VE-DSG nicht aufgenommen bzw. in diesem nicht umgesetzt. Der VE-DSG fokussiert einseitig auf den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, ohne mit den vorgeschlagenen Instrumenten diese Ziele auch nachhaltig zu verfolgen. Mit seiner Einseitigkeit trägt der VE-DSG einerseits dem notwendigen Ausgleich zwischen den Interessen der betroffenen Person an einem hohen Schutz der Persönlichkeit und den Interessen der Wirtschaft an einer optimalen und legitimen Nutzung von Daten keine Rechnung. Andererseits leistet der VE-DSG keinen Beitrag

[1] Mitglieder der Swiss Payment Association sind die Schweizer Kreditkarten-Herausgeber BonusCard.ch AG, Cembra Money Bank AG, Cornèr Bank AG, PostFinance AG, Swisscard AECS GmbH, UBS Switzerland AG und Viseca Card Services SA.

zur Stärkung der wirtschaftlichen Wettbewerbsfähigkeit und hilft nicht, die Chancen der fortschreitenden Digitalisierung zu nutzen. Zudem trägt es auch der vom Bundesrat verabschiedeten Strategie „Digitale Schweiz“ nicht gebührend Rechnung. Der Gesetzesvorschlag ist daher grundlegend neu auszurichten.

Prinzipien und Selbstverantwortung ins Zentrum der Regulierung stellen
Wenn im Gesetz vom „Verantwortlichen“ gesprochen wird, dann soll der Gesetzgeber diesem auch (Eigen-)Verantwortung übertragen. In der Konsequenz heisst das z.B., dass dem Verantwortlichen nicht eine Vielzahl von Genehmigungs-/Meldepflichten aufgebürdet werden soll. Zudem ist prinzipienbasiert (und nicht regelbasiert) zu legiferieren, sodass den Rechtsunterworfenen Raum für eine effiziente und effektive Regulierungsumsetzung verbleibt.

Kein Swiss Finish
Gegenüber dem internationalen Datenschutzniveau ist kein Swiss Finish vorzunehmen (exemplarisch für den vielfach vorgenommenen Swiss Finish sei hier auf die im VE-DSG vorgesehene breite Begriffsbestimmung des Profilings verwiesen). Einerseits ist ein solcher für die angestrebte Äquivalenz mit dem europäischen Datenschutzniveau nicht erforderlich, anderseits würde er die Schweizer Wirtschaft bzw. deren internationale Wettbewerbsfähigkeit ungebührlich belasten. Zudem würde ein Swiss Finish unverhältnismässig in die fragile Balance zwischen zweckmässiger bzw. notwendiger Datenbearbeitung und legitimem Datenschutz eingreifen.

Abstimmung zwischen Datenschutzgesetz und Aufsichtspraxis der FINMA
Für Finanzintermediäre bestehen mit dem sich derzeit in Überarbeitung befindlichen FINMA-Rundschreiben 2008/7 (Outsourcing Banken) und mit Anhang 3 zum FINMA-Rundschreiben 2008/21 (Operationelle Risiken Banken) bereits weitreichende Vorgaben zum Outsourcing und zum Umgang mit elektronischen Kundendaten. Diese Vorgaben dürfen durch die Neufassung des Datenschutzgesetzes nicht weiter verschärft werden, und es darf auch nicht zu Redundanzen oder Widersprüchen in der praktischen Umsetzung der verschiedenen Regulative kommen.

Verzicht auf strafrechtliche Sanktionen
Strafrechtliche Sanktionen sind für die Äquivalenz zum europäischen Datenschutzniveau in keiner Weise erforderlich. Dies umso weniger, als die DSGVO zur Durchsetzung das verwaltungsrechtliche Verfahren vorsieht. Dabei ist es durchaus möglich, dass der gleiche Lebenssachverhalt sowohl unter den Geltungsbereich der DSGVO als auch unter denjenigen des DSG fällt. Dies ist insbesondere dann denkbar, wenn eine Vielzahl von Handlungen oder Unterlassungen, mithin ein unternehmerischer Prozess, sanktioniert werden soll. Nicht kongruente Sanktionssysteme würden unter diesen Umständen zu einer mehrfachen Sanktionierung der natürlichen Person und der Unternehmung für den gleichen Lebenssachverhalt und letztlich zu völlig unhaltbaren Resultaten führen. Darüber hinaus ist die Androhung strafrechtlicher Sanktionen – erst Recht persönlicher strafrechtlicher Sanktionen – unverhältnismässig und in hohem Masse kontraproduktiv. Ganz besonders stossend ist dabei die Strafbarkeit von fahrlässigen DSG-Verstössen. Hinzu kommt, dass viele der mit strafrechtlichen Sanktionen belegten DSG-Bestimmungen – zu Recht – weniger regel- und eher prinzipienbasiert konzipiert sind. Prinzipienbasierte Normen eignen sich jedoch nicht dafür, mit strafrechtlichen Sanktionen verknüpft zu werden, da für die Rechtsunterworfenen unter strafrechtlichen Gesichtspunkten zu wenig klar eingegrenzt ist, welches Verhalten mit Strafe bedroht ist (nulla poena sine lege certa). Zudem werden fundamentale EMRK Garantien wie „nemo tenetur“ ausgehöhlt. Auf die Artikel 50 bis 55 VE-DSG ist daher zu verzichten.

1. Abkürzungen von Rechtserlassen

- DSGVO: Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- Schengen-RL: Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
- SEV 108: Revisionsvorlage des Europarats-Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Stand: September 2016)
- VE-DSG: Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes vom 21. Dezember 2016

2. Grundsätzliche Ausführungen

2.1 Wettbewerbsfähigkeit stärken und Chancen der Digitalisierung nutzen

Gemäss Erläuterungsbericht soll das neue Datenschutzgesetz die Wettbewerbsfähigkeit der Schweiz erhalten und stärken, indem ein Umfeld geschaffen wird, welches den grenzüberschreitenden Datenverkehr erleichtert und die Attraktivität der Schweiz für neue Aktivitäten im Zusammenhang mit der digitalen Gesellschaft steigert (Ziff. 1.3 des Erläuterungsberichts). Diesen Zielsetzungen, das heisst der Förderung der Wettbewerbsfähigkeit, der Gewährleistung des freien Verkehrs personenbezogener Daten und der Chancennutzung im Bereich der Digitalisierung, wird der Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes zu weiten Teilen nicht gerecht. Exemplarisch zeigt sich dies bereits in der Zweckbestimmung: Gemäss Art. 1 VE-DSG wird einseitig lediglich der Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen bezweckt. Die Stärkung der Wettbewerbsfähigkeit der Schweiz oder die Erleichterung des sicheren und freien Verkehrs personenbezogener Daten wird dagegen nicht verankert. Damit missachtet der Vorentwurf, dass das Recht auf Schutz der personenbezogenen Daten kein absolutes bzw. uneingeschränktes Recht ist, sondern dass ein bestmöglicher Ausgleich der Interessen aller dem Datenschutzgesetz Unterliegenden – also der Datenbearbeiter und der betroffenen Personen – erreicht werden muss.

Ebenso findet die vom Bundesrat am 20. April 2016 verabschiedete Strategie "Digitale Schweiz", mit welcher die Schweiz die Chancen der Digitalisierung in allen Lebensbereichen konsequent nutzen will, im Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes keinen genügenden Niederschlag. So sehen viele der neue Bestimmungen im VE-DSG zusätzliche Hürden und Erschwernisse vor, welche die Chancennutzung im Bereich der Digitalisierung erschweren anstatt sie zu fördern und so Innovationen hemmen.

Die Swiss Payment Association beantragt daher, den Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes so zu überarbeiten, dass er auch den legitimen Interessen nach Erhaltung und Steigerung der Wettbewerbsfähigkeit der Schweizer Wirtschaft sowie der Chancennutzung im Bereich der Digitalisierung gerecht wird.

2.2 Prinzipien und Selbstverantwortung ins Zentrum der Regulierung stellen

Wir anerkennen die Notwendigkeit, im Rahmen der Totalrevision des Datenschutzgesetzes weiterhin über ein Datenschutzniveau zu verfügen, das äquivalent zum europäischen Schutzniveau ist und so den reibungslosen grenzüberschreitenden Datenverkehr gewährleistet. Wichtig ist aus unserer Warte, dass die erforderliche Äquivalenz über eine prinzipienbasierte Regulierung – und nicht eine regelbasierte – hergestellt wird, welche Raum für praxisnahe, effiziente und effektive Lösungen lässt, die innerhalb des gesteckten Rahmens von den regulierten Akteuren selbstverantwortlich entwickelt werden können. Dieses auf eine lange und erfolgreiche Tradition zurückblickende Schweizer Regulierungskonzept darf nicht verlassen werden, denn es trägt ganz wesentlich zur Verträglichkeit der Schweizer Gesetzgebung und zur internationalen Wettbewerbsfähigkeit der Schweizer Volkswirtschaft bei. Wenn im Gesetz vom „Verantwortlichen" gesprochen wird, dann soll der Gesetzgeber diesem auch zutrauen, dass er seine (Eigen-)Verantwortung wahrnimmt. Konkret heisst das zum Beispiel, dass dem Verantwortlichen nicht eine Vielzahl von Genehmigungs- und Meldepflichten aufgebürdet werden soll. **Die Swiss Payment Association setzt sich deshalb für eine prinzipienbasierte Regulierung ein, welche den Regulierten Selbstverantwortung belässt.**

2.3 Kein Swiss Finish

Nebst diesen Grundanforderungen ist es genau so wichtig, dass gegenüber dem internationalen Datenschutzniveau kein Swiss Finish, verstanden als verschärfte Regelung im Vergleich zur Europäischen Union, vorgenommen wird. Einerseits ist ein solcher für die Äquivalenz mit dem europäischen Datenschutzniveau unnötig, anderseits würde er die Schweizer Wirtschaft bzw. deren internationale Wettbewerbsfähigkeit ungebührlich belasten. Zur Illustration sei als Beispiel angeführt, dass ausländische Kreditkartenverarbeiter ihre Dienstleistungen einer Vielzahl von Kreditkartenanbietern offerieren. Schweizer Kreditkartenanbieter, welche Dienstleistungen dieser Verarbeiter beziehen wollen, müssen jeglichen Mehraufwand für einen Swiss Finish teuer bezahlen – sofern der Anbieter überhaupt bereit ist, diesen Mehraufwand zu treiben. Das erhöht die Kosten des Zahlungsverkehrs. Soweit die Kosten auf die Kartenkunden oder Händler überwälzt werden können, erhöht dies auch das Preisniveau in der Schweiz.

Zudem würde ein Swiss Finish unverhältnismässig in die fragile Balance zwischen zweckmässiger bzw. notwendiger Datenbearbeitung und legitimem Datenschutz eingreifen. **Die Swiss Payment Association lehnt daher Swiss-Finish-Normen ab und beantragt, konsequent auf solche zu verzichten** (siehe dazu die nachfolgenden Ausführungen zu den einzelnen Themen). Dort, wo europäische Normen über das Ziel hinausschiessen, soll der Schweizer Gesetzgeber auch den Mut haben, diese nicht nachzuahmen, sondern eine angemessene Schweizer Lösung zu implementieren. Das gilt ganz besonders dort, wo ein europäisches Normenniveau punkto Äquivalenz nicht von Bedeutung ist. Denn Äquivalenz mit dem Datenschutz-Regime der Europäischen Union erfordert keine Identität sondern „lediglich" Adäquanz mit der DSGVO.

3. Ausführungen zu einzelnen Themen / Kritikpunkte und Anträge der Swiss Payment Association

Nachstehend finden sich zu ausgewählten Themenkreisen bzw. den zugehörigen Bestimmungen des VE-DSG die Überlegungen und Anträge der SPA:

3.1 Zweckbestimmung (Art. 1 VE-DSG)

- Antrag: Ergänzung des Zweckartikels (Art. 1 VE-DSG)

  Wie bereits oben unter Ziffer 2.1 dargelegt, beinhaltet der Zweckartikel einseitig nur den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, nicht aber die Förderung der Wettbewerbsfähigkeit der Schweiz, die Chancennutzung im Bereich der Digitalisierung und die Gewährleistung des freien Verkehrs personenbezogener Daten. Wir beantragen daher, den Zweckartikel wie folgt zu ergänzen (Ergänzung = unterstrichen):

  > „Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden, sowie die Stärkung der Wettbewerbsfähigkeit und die Förderung des sicheren und freien Verkehrs von Personendaten."

3.2 Grundsätze (Art. 4 VE-DSG)

- Antrag: Verzicht auf das Adjektiv „klar" in Art. 4 Abs. 3 VE-DSG

  Auf das Zusatzerfordernis, dass der Zweck „klar" erkennbar sein muss ist zu verzichten. Diese Anforderung schafft keinen Mehrwert und würde lediglich zu unnötigen Auslegungsfragen führen. Zudem kennen weder DSGVO noch SEV 108 das Erfordernis, dass der Zweck *klar* erkennbar sein muss.

  Wir beantragen daher, in Art. Abs. 3 VE-DSG das Adjektiv „klar" zu streichen:

  > „Personendaten dürfen nur zu einem bestimmten und für die betroffene Person ~~klar~~ erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist."

- Antrag: Vermerk in der Botschaft, dass die Einwilligung im Datenschutzgesetz eine Willenserklärung im Sinne des Obligationenrechts ist (Art. 4 Abs. 6 VE-DSG)

  In der Botschaft zu einem neuen Datenschutzgesetz ist festzuhalten, dass es sich bei der Einwilligung im Datenschutzgesetz um eine Willenserklärung im Sinne des Obligationenrechts handelt. Demnach kann Stillschweigen als affirmatives Verhalten dann genügen, wenn die Parteien dies vorab gültig vereinbart haben (Art. 6 OR).

  Diese Klarstellung dient dazu, die vom Datenschutzrecht vorgesehenen Einwilligungen in der Praxis angemessen handhaben zu können.

  > Vermerk in die Botschaft zum Datenschutzgesetz aufnehmen, dass die Einwilligung im Datenschutzgesetz eine Willenserklärung im Sinne des Obligationenrechts ist.

- Antrag: Klärung bzw. Abgrenzung der Begriffe „eindeutig" und „ausdrücklich" (Art. 4 Abs. 6 VE-DSG)

  Die Unterscheidung zwischen der in Art. 4 Abs. 6 VE-DSG verwendeten Begriffe „eindeutig" und „ausdrücklich" ist – trotz Ausführungen im Erläuternden Bericht – nicht abschliessend klar. Würde unter „ausdrücklich" tatsächlich verstanden, dass ein Stillschweigen nicht genügen würde, ergäben sich daraus im Wirtschaftsleben nicht praktikable Zustände. So wären in bestimmten Fällen Anpassungen von AGB auf demjenigen Weg, dass sie als genehmigt gelten, wenn der Kunde nicht innert Frist widerspricht, nicht mehr möglich. In solchen Fällen eine schriftliche Erklärung, eine mündliche Äusse-

rung oder ein Zeichen des Kunden zu verlangen, wäre in der Praxis nicht vernünftig durchführbar.

Klärung bzw. Abgrenzung der Begriffe „eindeutig“ und „ausdrücklich“ und Verzicht darauf, dass in bestimmten Fällen für die rechtsgenügliche Einwilligung der betroffenen Person zur Bearbeitung von Personendaten eine schriftliche Erklärung, eine mündliche Äusserung oder ein Zeichen erforderlich ist.

3.3 Bekanntgabe ins Ausland (Art. 5f. VE DSG)

- Antrag: Ergänzung von Art. 5 Abs. 3 VE-DSG

  Für den Fall, dass (noch) kein Entscheid des Bundesrats hinsichtlich der Angemessenheit des Datenschutzes in einem Land vorliegt, soll aus Gründen der Praktikabilität und zur Vermeidung von unnötigen Verzögerungen weiterhin der Verantwortliche die Angemessenheit eigenverantwortlich prüfen können. Entsprechend beantragen wir Art. 5 Abs. 3 VE-DSG wie folgt zu ergänzen (Ergänzung = unterstrichen):

  „Liegt kein Entscheid des Bundesrats nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn der Verantwortliche selbst festgestellt hat, dass ein angemessener Schutz gewährleistet ist, oder wenn ein geeigneter Schutz gewährleistet ist durch: […]

- Antrag: Streichung der in Art. 5 Abs. 3 lit. c. Ziff. 1 und lit. d. sowie Abs. 5 VE-DSG postulierten Genehmigungspflichten

  Die in Art. 5 Abs. 3 lit. c. Ziff. 1 und lit. d. sowie in Abs. 5 VE-DSG vorausgesetzte Genehmigung von vertraglichen Garantien durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragten) führen zu weit. Solche Pflichten würden zu erheblichen Mehraufwänden und zu Projektverzögerungen bei den betroffenen Unternehmen führen – nicht zuletzt auch deshalb, weil sie die Kapazitäten des Beauftragten überbeanspruchen würden und so keine angemessenen Genehmigungsfristen gegeben wären (auch wenn Ordnungsfristen ins Gesetz aufgenommen würden). Zudem würde eine Genehmigungspflicht nicht zu einem besseren Datenschutz beitragen, steht doch das Unternehmen ohnehin selbst in der Verantwortung. Die vom VE-DSG vorgesehenen Genehmigungspflichten wären ein überschiessender Swiss Finish, welcher den grenzüberschreitenden Datenfluss erheblich und ohne Nutzen erschweren würde. Entsprechend beantragen wir, in Art. 5 in den Abs. 3 und 5 VE-DSG folgende Ergänzung (= unterstrichen) bzw. folgende Streichungen vorzunehmen:

  „[3] Liegt kein Entscheid des Bundesrats nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn der Verantwortliche selbst festgestellt hat, dass ein angemessener Schutz gewährleistet ist, oder wenn ein geeigneter Schutz gewährleistet ist durch:
  […]
  c. standardisierte Garantien, insbesondere durch Vertrag;
  ~~1. welche der Beauftragte vorgängig genehmigt hat, oder~~
  2. welche der Beauftragte ausgestellt oder anerkannt hat;
  d. verbindliche unternehmensinterne Datenschutzvorschriften;~~, die vorgängig genehmigt wurden:~~
  ~~1. durch den Beauftragten, oder~~

~~2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet~~.
[…]
~~5 Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht.~~"

- Antrag: Streichung von Art. 5 Abs. 6 VE-DSG

  In Art. 5 Abs. 6 VE-DSG soll eine Meldepflicht angeordnet werden. Dies ist unseres Erachtens systemfremd, geht es doch um bereits vorliegende, standardisierte Garantien. Weshalb die Verwendung solcher Standards in jedem Verwendungsfall erneut eine Meldepflicht auslösen sollen, ist für uns nicht nachvollziehbar. Dies umso weniger, als es sich auch dabei gegenüber dem EU-Recht um einen Swiss Finish handelt (vgl. EuGH-Entscheid Schrems und gestützt darauf ergangener Entscheid der EU-Kommission vom 16.12.2016, wonach von ihr genehmigte Datenschutz-Standardklauseln nicht einer erneuten Bewilligung im Einzelfall bedürfen und deshalb ohne Einschränkung verwendet werden dürfen; Art. 46 DSGVO). Demzufolge beantragen wir, Absatz 6 von Artikel 5 VE-DSG ersatzlos zu streichen.

  Streichung von Art. 5 Abs. 6 VE-DSG

- Antrag: Streichung von „im Einzelfall" in Art. 6 Abs. 1 lit. a. VE-DSG

  Die Einschränkung „im Einzelfall" ist nicht notwendig und nicht sinnvoll. Auch im Falle wiederholter Sachverhalte reicht bei Erkennbarkeit und entsprechendem Erwartungshorizont eine einmalige Einwilligung aus. Der Zusatz „im Einzelfall" widerspricht zudem der Gesetzessystematik, weil nur für die in Art. 6 Abs. 1 unter lit. c. und d genannten Fälle die „Bekanntgabe im Einzelfall" geregelt wird. Ferner ist in Art. 49 Abs. 1 DSGVO „eine Reihe von Übermittlungen" ausdrücklich zugelassen. Auch diesbezüglich ist auf einen Swiss Finish zu verzichten. Entsprechend beantragen wir, in Art. 6 Abs. 1 lit. a. VE-DSG folgende Streichung vorzunehmen:

  „In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:
  a. die betroffene Person ~~im Einzelfall~~ eingewilligt hat;
  […]"

- Antrag: Erweiterung der Zulässigkeit der Datenübermittlung im Zusammenhang mit Verträgen in Art. 6 Abs. 1 lit. b. VE-DSG

  Ganz grundsätzlich, aber auch im Vergleich zur europäischen Lösung, ist der vorgeschlagene Art. 6 Abs. 1 lit. b. VE-DSG zu eng gefasst. Im Zusammenhang mit Verträgen sollen nicht nur die Daten des jeweiligen Vertragspartners sondern insbesondere auch Daten, welche zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person vom Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags nötig sind, übermittelt werden können (vgl. auch Art. 49 Abs. 1 lit. c. DSGVO). Wir beantragen, Art. 6 Abs. 1 lit. b. VE-DSG wie folgt zu ergänzen (Ergänzung = unterstrichen):

„In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:
a. […]
b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners oder von Personen, in deren Interesse der Vertrag abgeschlossen werden soll, handelt;
[…]"

- Antrag: Ergänzung von in Art. 6 Abs. 1 lit. c. Ziff. 1 VE-DSG um den Fall der Übermittlung von Personendaten aus eigenem überwiegenden Interesse

  Im VE-DSG fehlt (weiterhin) eine Bestimmung, welche eine Übermittlung von Personendaten „aus eigenem überwiegenden Interesse" ermöglicht, wie dies Art. 12 Abs. 4 lit. c. SEV 108 und Art. 49 Abs. 1 DSGVO vorsehen. Wir beantragen daher, Art. 6 Abs. 1 lit. c. Ziff. 1 VE-DSG wie folgt zu ergänzen (Ergänzung = unterstrichen):

„In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:
[…]
c. die Bekanntgabe im Einzelfall unerlässlich ist für:
1. die Wahrung eines überwiegenden öffentlichen oder privaten Interesses, oder
[…]"

- Antrag: Streichung von Meldepflichten in Art. 6 Abs. 2 VE-DSG

  Die Mitteilung an den Beauftragten, wenn Personendaten zum Abschluss eines Vertrags oder zur Vertragsabwicklung oder zur Durchsetzung von Rechtsansprüchen übermittelt werden, ist unverhältnismässig und ohne Nutzen. Es ist deshalb darauf zu verzichten.

  Wir beantragen, in Art. 6 Abs. 2 VE-DSG folgende Streichung und folgende Ergänzung (= unterstrichen) vorzunehmen:

„Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben ~~b,~~ c Ziffer 1 und d bekannt gibt."

3.4 Auftragsdatenbearbeitung (Art. 7 VE DSG)

- Antrag: Keine zusätzlichen Präzisierungen der Pflichten des Auftragsbearbeiters durch den Bundesrat (Art. 7 Abs. 2 VE-DSG)

  In Art. 7 Abs. 2 VE-DSG soll der Bundesrat verpflichtet werden, die weiteren Pflichten des Auftragsbearbeiters zu präzisieren. Dafür bestehen – neben den gesetzlichen Regeln und den vertraglichen Vereinbarungen zwischen Verantwortlichem und Auftragsbearbeiter – keine Notwendigkeit und kein Bedarf. Zudem könnte – falls es wider Erwarten doch noch einen zusätzlichen Regelungsbedarf gäbe – auf die Empfehlungen der guten Praxis des Beauftragten abgestützt werden, womit das Thema an der fachlich kompetentesten staatlichen Stelle verortet wäre. Wir beantragen daher, in Art. 7 Abs. 2 VE-DSG folgende Streichung vorzunehmen:

„Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. ~~Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters.~~"

- Antrag: Präzisierung des Begriffs „anderer Auftragsbearbeiter“ in Art. 7 Abs. 3 VE-DSG

  Es besteht unseres Erachtens Unklarheit darüber, wer als „anderer Auftragsbearbeiter“ im Sinne von Art. 7 Abs. 3 DSG gilt. Der Terminus sollte begrifflich eng gefasst werden, damit – nebst jedwedem Unterbeauftragten – potenziell nicht auch jedwede Verhältnisse zu Hilfspersonen erfasst werden (beispielsweise im Rahmen von IT-Leistungen, bei denen zwar grundsätzlich Kontakt zu Personendaten besteht, die Leistung des Dritten jedoch nicht die Bearbeitung der Daten selbst vorsieht). Wir beantragen daher, in Art. 7 Abs. 3 VE-DSG folgende Anpassung (= unterstrichen) vorzunehmen:

  „Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem ~~anderen Auftragsbearbeiter~~ Unterbeauftragten übertragen.“

- Antrag: Zustimmung soll in Form einer allgemeinen schriftlichen Einwilligung erteilt werden können (Art. 7 Abs. 3 VE-DSG)

  Die in Art. 7 Abs. 3 VE-DSG postulierte stetige vorgängige schriftliche Zustimmung des Verantwortlichen gegenüber dem Auftragsbearbeiter bei Übertragung der Bearbeitung an einen „anderen Auftragsbearbeiter“ ist zu umständlich und daher nicht praxistauglich. Sie bringt auch keinen Nutzen für die betroffene Person. Zudem stellt sie gegenüber dem europäischen Referenzrahmen einen unnötigen Swiss Finish dar. Die europäische Regelung sieht vor, dass der vom Verantwortlichen beauftragte Auftragsverarbeiter auch auf Basis einer allgemeinen schriftlichen Einwilligung weitere Auftragsverarbeiter in Anspruch nehmen kann, wenn er den Verantwortlichen hierüber informiert, wodurch der Verantwortliche die Möglichkeit erhält, hiergegen Einspruch zu erheben. Im Erläuternden Bericht zum Vorentwurf wird zwar unter Ziff. 8.1.2.4 die Zulässigkeit einer allgemeinen Einverständniserklärung erwähnt, jedoch sollte sich dies aus Gründen der Rechtssicherheit explizit so aus dem Gesetz ergeben. Wir beantragen daher, Art. 7 Abs. 3 VE-DSG wie folgt zu ergänzen (Anpassung bzw. Ergänzung = unterstrichen):

  „Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem ~~anderen Auftragsbearbeiter~~ Unterbeauftragten übertragen. Diese Zustimmung kann in genereller Weise erteilt werden.“

- Antrag: Abstimmung zwischen Datenschutzgesetz und Aufsichtspraxis der FINMA (FINMA-Rundschreiben)

  Für Finanzintermediäre bestehen mit dem sich derzeit in Überarbeitung befindlichen FINMA-Rundschreiben 2008/7 (Outsourcing Banken) und mit Anhang 3 zum FINMA-Rundschreiben 2008/21 (Operationelle Risiken Banken) bereits weitreichende Vorgaben zum Outsourcing und zum Umgang mit elektronischen Kundendaten. Diese Vorgaben dürfen durch die Neufassung des Datenschutzgesetzes nicht weiter verschärft werden, und es darf auch nicht zu Redundanzen oder Widersprüchen in der praktischen Umsetzung der verschiedenen Regulative kommen.

  Das neue Datenschutzgesetz ist mit der Aufsichtspraxis der FINMA (FINMA-RS) im Bereich Outsourcing/Umgang mit elektronischen Kundendaten abzustimmen.

3.5 Profiling (Art. 3 lit. f., Art. 4 Abs. 6, Art. 23 Abs. 2 lit. d., Art. 24 Abs. 2 VE-DSG)

- Antrag: Die Begriffsbestimmung „Profiling" in Art. 3 lit. f. VE-DSG ist enger zu fassen: Kein Einbezug von Nicht-Personendaten und kein Einbezug nicht-automatisierter Datenbearbeitung

  Die in Art. 3 lit. f. VE-DSG vorgesehene Regelung umfasst im Gegensatz zur Regelung der DSGVO (Art. 4 Ziff. 4) auch die Verarbeitung nicht-personenbezogener Daten sowie die nicht-automatisierte Auswertung von Daten. Zudem schränkt der Wortlaut der Bestimmung den Anwendungsbereich nicht auf das Profiling der Daten einer betroffenen Person ein. Der Wortlaut umfasst somit auch eine Auswertung von anonymisierten Daten und/oder Sachdaten sowie potenziell auch eine Auswertung hinsichtlich der Merkmale von Personengruppen. Damit geht der Vorentwurf nicht nur ganz erheblich über die Regelung auf europäischer Ebene hinaus (Swiss Finish), sondern schiesst ganz generell über das Ziel hinaus. Die vorgeschlagene weite Begriffsbestimmung des Profiling würde zu einschneidenden Einschränkungen und neuen Risiken in der Datenbearbeitung für Unternehmen führen – und das ganz besonders auch in Bezug auf statistische Auswertungen und Forschungstätigkeiten. Viele Datenbearbeitungen zu statistischen Zwecken oder bei der Entwicklung neuer Produkte und Leistungen werden mit Daten vorgenommen, die nicht personenbezogen sind. Eine solche Datenbearbeitung stellt für die Persönlichkeit der betroffenen Person kein erhöhtes Risiko dar, da die Auswertung anonymisiert erfolgt, weshalb eine Subsumierung solcher Tätigkeiten unter den Begriff „Profiling" unangebracht bzw. unverhältnismässig wäre.

  Dasselbe gilt für den Fall, dass Daten nicht automatisiert ausgewertet werden. In solchen Fällen ergibt sich per se kein erhöhtes Risiko für die betroffene Person. Einerseits bleibt der Umfang der Datenbearbeitung naturgemäss limitiert, andererseits unterliegt ein nicht-automatisiertes Profiling als Datenbearbeitung ganz normal dem Datenschutzgesetz. Den Schutz darüber hinaus durch die Ausweitung des Begriffs „Profiling" weiter zu erhöhen, entbehrt einer Grundlage und lässt sich daher nicht rechtfertigen.

  Wir beantragen, die Begriffsbestimmung zum Profiling deutlich enger zu fassen und auf den Einbezug von Nicht-Personendaten und von nicht-automatisierter Datenbearbeitung zu verzichten. Zudem ist klarzustellen, dass sich Profiling immer auf eine bestimmte Person beziehen muss und nicht die Auswertung hinsichtlich ganzer Personengruppen oder Segmente umfasst. Wir beantragen somit, in Art. 3 lit. f. VE-DSG folgende Streichung bzw. folgende Ergänzungen (= unterstrichen) vorzunehmen:

  „Profiling: jede automatisierte Auswertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale der betroffenen Person zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich ihrer Arbeitsleistung, wirtschaftlichen Lage, Gesundheit, Intimsphäre oder Mobilität."

- Antrag: Keine *ausdrückliche* Einwilligung für das Profiling (Art. 4 Abs. 6 VE-DSG)

  Weder DSGVO noch SEV 108 verlangen generell die Ausdrücklichkeit der Einwilligung in das Profiling. Die DSGVO fordert eine ausdrückliche Einwilligung nur, wenn eine automatisierte Einzelentscheidung gestützt auf Profiling getroffen wird, nicht jedoch für Profiling selbst. Der VE-DSG will in Art. 4 Abs. 6 darüber hinausgehen und generell eine *ausdrückliche* Einwilligung für das Profiling statuieren. Auf diesen Swiss Finish ist zu verzichten. Dementsprechend ist „das Profiling" in Art. 4 Abs. 6 VE-DSG nicht aufzuführen:

„Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen."

- Antrag: Profiling ohne *ausdrückliche* Einwilligung stellt keine Persönlichkeitsverletzung dar (Art. 23 Abs. 2 lit. d. VE-DSG)

  In Konsequenz der vorstehenden Erörterungen ist es auch nicht angemessen, ein Profiling ohne *ausdrückliche* Einwilligung als Persönlichkeitsverletzung zu taxieren.

  Wir beantragen daher, Buchstabe d. von Art. 23 Abs. 2 VE-DSG ersatzlos zu streichen.

„Eine Persönlichkeitsverletzung liegt insbesondere vor:
[…]
~~d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.~~"

- Antrag: Verankerung eines Rechtfertigungstatbestandes für das Profiling (Art 24 Abs. 2 VE-DSG)

  Art. 23 Abs. 2 lit. d. VE-DSG legt zudem nahe, dass eine Rechtfertigung des Profilings ausschliesslich über eine ausdrückliche Einwilligung möglich ist und somit Profiling nie nach Art. 24 VE-DSG gerechtfertigt sein kann. Das führt zu weit und würde sich insbesondere für die Anbieter von Zahlungsdienstleistungen verheerend auswirken. Für Zahlungsdienstanbieter sind Datenbearbeitungen, inklusive Profiling, insbesondere zur Bekämpfung von Betrug und zur Erhöhung der Sicherheit für die betroffene Person – aber auch für ganze Zahlungssysteme und deren Teilnehmer (z.B. für die Händler, die Acquirer und die Issuer) – unverzichtbar. Die Datenbearbeitung (inklusive Profiling) erfolgt gleichermassen im Interesse der Konsumentinnen/Konsumenten und Händler, welche die Zahlungsmittel nutzen, wie der Zahlungsdienstleister selbst. Dabei müssen die Datenbearbeitungen bzw. die Profile regelmässig den neuesten Bedrohungen und den durch das Zahlungsverhalten der betroffenen Person herbeigeführten Veränderungen angepasst und entsprechend weiterentwickelt werden können. Eine Rechtfertigung dieser Datenbearbeitungen über eine ausdrückliche Einwilligung darf daher – wie bis anhin – nicht vorgeschrieben werden (sofern die allgemeinen Bearbeitungsgrundsätze eingehalten werden). Vielmehr ist in Art. 24 Abs. 2 VE-DSG über einen entsprechenden Rechtfertigungsgrund sicherzustellen, dass Profiling weiterhin ohne ausdrückliche Einwilligung (gestützt auf ein überwiegendes Interesse) zulässig ist. Alles andere wäre unpraktikabel und würde die effiziente und effektive Betrugsbekämpfung unnötig untergraben.

  Wir beantragen daher, in Art. 24 Abs. 2 VE-DSG unter lit. g. einen weiteren Rechtfertigungstatbestand einzuführen bzw. Art 24 Abs. 2 VE-DSG wie folgt zu ergänzen (= unterstrichen):

„Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser ~~r~~ insbesondere:
[…]
g. die Daten zur Erhöhung der Sicherheit und Vermeidung von Nachteilen für die betroffene Person oder andere Personen bearbeitet, wofür sie auch Profiling betreiben kann."

3.6 Informationspflichten gegenüber der betroffenen Person (Art. 13, 14 und 15 VE-DSG)

Betreffend Informationspflichten ist allgemein darauf hinzuweisen, dass generell die rechtsgenügliche Möglichkeit bestehen muss, bei der Beschaffung von Personendaten auf eine bestimmte Plattform (z.B. Webseite) verweisen zu können, auf welcher detaillierte Informationen zur Datenbearbeitung eingesehen werden können. Dies erfüllt die Vorgaben der SEV 108, wonach der Zugang zu den Informationen gesichert sein muss. Die Erläuterungen zum VE-DSG lassen demgegenüber vermuten, dass es nach dem aktuellen Vorentwurf nicht ausreicht, wenn die betroffene Person bereitgestellte Informationen selbst abrufen bzw. konsultieren muss.

Es ist im VE-DSG klar festzuhalten, dass es betreffend Informationspflicht ausreicht, wenn die betroffene Person auf eine bestimmte Plattform verwiesen wird, auf der sie bereitgestellte Informationen selbst abrufen bzw. konsultieren kann.

- Antrag: Streichung von Art. 13 Abs. 4 VE-DSG

  Gemäss der in Art. 13 Abs. 4 VE-DSG vorgeschlagenen Bestimmung hat der Verantwortliche die betroffene Person über die Identität und die Kontaktdaten der Auftragsbearbeiter – und konsequenterweise auch aller Unterauftragsbearbeiter – zu informieren. Dies geht sowohl über die DSGVO als auch die SEV 108 hinaus und wäre mit vertretbarem Aufwand nicht realisierbar bzw. würde betroffene Geschäftsprozesse verunmöglichen. Zudem gehört die Information, mit welchen Dienstleistern ein Unternehmen zusammenarbeitet, häufig zum Geschäftsgeheimnis eines Unternehmens.

  Eine solche Bestimmung ist aber auch deshalb nicht nötig, weil die Auslagerung von Dienstleistungen und der zugehörigen Datenbearbeitungen zum täglichen Geschäftsbetrieb jedes Unternehmens gehört und die betroffene Person weiss bzw. davon ausgeht, dass nicht jedes Unternehmen sämtliche Dienstleistungen selbst erbringen kann bzw. erbringt. Aus Sicht des Persönlichkeitsschutzes ist nicht entscheidend, dass die betroffene Person Identität und Kontaktdaten des Auftragsbearbeiters kennt, sondern dass sichergestellt ist, dass die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben erfolgt. Dies zu regeln ist Gegenstand von Art. 7 VE-DSG. Eine darüberhinausgehende Informationspflicht bringt aus datenschutzrechtlicher Sicht keinerlei Mehrwert, verursacht jedoch gewichtige Nachteile.

  Wir beantragen, Art. 13 Abs. 4 VE-DSG zu streichen.

Streichung von Art. 13 Abs. 4 VE-DSG

- Antrag: Verzicht auf die in Art. 14 Abs. 4 lit. a VE-DSG enthaltene Einschränkung

  Für die in Art. 14 Abs. 4 lit. a VE-DSG formulierte Einschränkung „und er die Personendaten nicht Dritten bekannt gibt“ gibt es aus datenschutzrechtlichen Überlegungen keinerlei Berechtigung: Sollten die Interessen der betroffenen Person durch die Bekanntgabe an einen Dritten tatsächlich beeinträchtigt sein, so ist dies bereits im Rahmen der allgemeinen Interessenabwägung im Sinne von Art. 24 VE-DSG berücksichtigt. Alles andere wäre das Resultat einer pauschal vorweggenommenen Interessenabwägung und würde zu absurden Situationen führen: So dürfte ein Konzernunternehmen, welches Daten mit einem anderen Konzernunternehmen teilt, nicht auf ein überwiegendes eigenes Interesse abstellen, während ein Unternehmen, das Daten innerhalb der gleichen juristischen Person ins Ausland liefert, dies nach wie vor könnte.

Wir beantragen daher, Art. 14 Abs. 4 lit. a mittels einer Streichung wie folgt anzupassen:

„Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten: a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern ~~und er die Personendaten nicht Dritten bekannt gibt~~;“

- Antrag: Streichung von Art. 14 Abs. 5 VE-DSG

  Die in Art 14 Abs. 5 statuierte Pflicht, beim Wegfall des Grundes für den Verzicht, die Einschränkung oder das Aufschieben die Information nachträglich mitzuteilen, ist ohne grossen Nutzen, würde aber unverhältnismässig hohen Aufwand verursachen. Eine solche Pflicht hätte zur Folge, dass Unternehmen über jede einzelne, gestützt auf eine Interessenabwägung gefällte Entscheidung für einen Informationsverzicht etc. Buch führen müssten, um diese Entscheidungen anschliessend permanent zu überwachen und sicherzustellen, dass – wenn beispielsweise keine überwiegenden Interessen Dritter mehr vorliegen – die nun fällige werdende Information nachgeholt würde. Das ist vollkommen unpraktikabel.

  Wir beantragen daher, Art. 14 Abs. 5 VE-DSG ersatzlos zu streichen.

Streichung von Art. 14 Abs. 5 VE-DSG.

- Antrag: Einschränkende Präzisierung in Art. 15 Abs. 1 VE-DSG

  In der aktuellen Formulierung ist der Anwendungsbereich von Art. 15 Abs. 1 VE-DSG weit überschiessend. Er umfasst längst nicht nur die im Erläuternden Bericht erwähnten Situationen (Vertragsabschluss und Verkehrsbussen), sondern z.B. auch automatisierte Kontrollen von Transaktionen (Kontrolle Zahlungseingang inkl. Buchung und Auslösung von Mahnungen etc.) oder Sicherheitsmechanismen wie Spamfilter. Es ist daher zwingend Klarheit zu schaffen, dass nicht jede (rechtliche) Wirkung, wie z.B. ein Geldbezug am Bankomat (Entscheid, ob Geld ausbezahlt wird, erfolgt automatisch) betroffen ist. Dazu ist die Einschränkung „erhebliche“ wiederholt zu verwenden.

  Wir beantragen, Art. 15 Abs. 1 VE-DSG wie folgt zu ergänzen (Ergänzung = unterstrichen):

Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese <u>erhebliche</u> rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.

- Antrag: Streichung von Art. 15 Abs. 2 VE-DSG

  Eine Datenbearbeitung mit ausschliesslich automatisierten Mitteln ist nicht per se ein schwererer Eingriff in Persönlichkeitsrechte als eine rein "menschliche" Bearbeitung. Im Gegenteil, eine algorithmenbasierte Datenbearbeitung, die den zwingenden Grundsätzen der Privacy by Default und Design folgt, kann eine grosse Gewähr der Rechtskonformität bieten, da der Risikofaktor "Mensch" ausgeschlossen wird. Aus diesem Grund ist das fragliche Äusserungsrecht für die betroffene Person unverhältnismässig und ein sachlich nicht begründeter Ausdruck eines generellen Misstrauens gegenüber "der Maschine".

Weiter ist das vorgesehene Äusserungsrecht auch deshalb unnötig, weil die betroffene Person nach Art. 15 Abs. 1 VE-DSG informiert werden muss und so selbst entscheiden kann, ob sie weiterhin von einem Anbieter Dienstleistungen beziehen möchte, der vollautomatisierten Entscheide trifft, oder ob sie zu einem Anbieter wechseln möchte, der zusätzlich oder vollständig auf die Arbeitskraft natürlicher Personen setzt.

Wir beantragen daher, Art. 15 Abs. 2 VE-DSG ersatzlos zu streichen.

Streichung von Art. 15 Abs. 2 VE-DSG

- Antrag: Verzicht auf die in Art. 15 Abs. 3 VE-DSG vorgesehene Informationspflicht gestützt auf eine Vereinbarung zwischen der betroffenen Person und dem Verantwortlichen

  Die Informationspflicht betreffend automatisierte Einzelentscheidungen sollte nicht nur wegfallen, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht, sondern auch dann, wenn die automatisierten Einzelentscheidungen gestützt auf eine Vereinbarung zwischen der betroffenen Person und dem Verantwortlichen gefällt werden und sie den erkennbaren Kern der Vereinbarung ausmachen. Dies kann z.B. bei einem Vertrag betreffend die automatisierte Verwaltung des Vermögens der betroffenen Person gegeben sein (z.B. RoboAdvice – hier möchte der Kunde gerade ausschliesslich automatisierte Einzelentscheidungen). In solchen Fällen sind der betroffenen Person die zugrundeliegenden Parameter bekannt bzw. sie hat diese mit dem Verantwortlichen vereinbart. Entsprechend beantragen wir, dass in Art. 15 Abs. 3 VE-DSG festgehalten wird, dass die Informationspflicht nicht besteht, wenn eine Vereinbarung zwischen dem Verantwortlichen und der betroffenen Person die Abgabe (ev. einer Vielzahl) von automatisierten Einzelentscheidungen bezweckt und dies aus der Vereinbarung erkennbar ist. Dies umso mehr, als eine Schlechterstellung einer erkennbaren Datenbearbeitung im privaten Bereich gegenüber dem öffentlich-rechtlichen (Gesetz) nicht gerechtfertigt ist.

  Wir beantragen daher, Art. 15 Abs. 3 VE-DSG mittels einer Streichung und einer Ergänzung (= unterstrichen) wie folgt anzupassen:

Die Informations~~- und Anhörungs~~pflicht gilt nicht, wenn ein Gesetz oder ein Vertrag zwischen Verantwortlichem und betroffener Person eine automatisierte Einzelentscheidung ~~vorsieht~~ vorsehen.

3.7 Datenschutz-Folgenabschätzung (Art. 16 VE-DSG)

- Antrag: Streichung von Art. 16 VE-DSG

  Zur Einhaltung der Bestimmungen des Datenschutzgesetzes braucht ein Unternehmen bereits heute laufend fachkundige Beurteilungen und darauf abgestützte Massnahmenpakete. Diese Grundvoraussetzung – speziell das Durchführen einer Datenschutz-Folgenabschätzung (DFA) – gesetzlich zu verankern, bringt keinen Mehrwert, sondern verursacht – insbesondere auch in Zusammenhang mit der Konsultationspflicht beim Beauftragten – erhebliche Rechtsunsicherheit und das Risiko von ungerechtfertigten Verzögerungen.

  Wir beantragen daher, Art. 16 VE-DSG ersatzlos zu streichen.

Streichung von Art. 16 VE-DSG

- Eventualantrag 1: Präzisierung von Art. 16 VE-DSG

  Sollte entgegen dem vorstehenden Antrag an Art. 16 VE-DSG grundsätzlich festgehalten werden, beantragen wir, die unglückliche Formulierung von Absatz 1 („… voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person, …") anzupassen.

  Einerseits beantragen wir „erhöht" durch „hoch" zu ersetzen, um klarzustellen, welcher Risikograd gemeint ist (vgl. auch Art. 35 Abs. 1 und Erwägung 91 DSGVO). Eine gesetzliche Pflicht zur Datenschutz-Folgenabschätzung soll auf Datenbearbeitungen mit hohen Risiken beschränkt werden. Damit sind nach EU-Doktrin solche gemeint, welche auch nach Implementierung geeigneter Massnahmen immer noch hohe Risiken aufweisen. Andernfalls würde dies – da jede Datenbearbeitung zu einem erhöhten Risiko gegenüber keiner Bearbeitung führt – bedeuten, dass letztlich bei jeder Datenbearbeitung eine formelle DFA durchzuführen wäre. Dies hätte zur Folge, dass neue Vorhaben, für die Personendaten bearbeitet werden müssen, stark verzögert würden. Nicht zu unterschätzen wären auch der Mehraufwand und die Notwendigkeit von zusätzlichen Ressourcen für das Management von DFA. Insbesondere für kleinere Unternehmen oder Startups würde dies prohibitiv wirken.

  Andererseits beantragen wir, die Begriffe „Persönlichkeit oder Grundrechte" durch den Begriff „Persönlichkeitsverletzung" zu ersetzen; dies entsprechend der Schweizer Gesetzesterminologie (vgl. dazu auch Art. 23 ff. VE-DSG).

  Schliesslich ist es auch unglücklich, dass in Art. 16 VE-DSG mehrmals vom „Verantwortlichen oder vom Auftragsbearbeiter" gesprochen wird. Dies führt zu einer Verwischung der Verantwortlichkeit bzw. zu Unsicherheiten, wem die jeweilige Pflicht obliegt. Wir beantragen, (durch Weglassung des Auftragsbearbeiters) klar zu stellen, dass nur der Verantwortliche die Verantwortung für Durchführung einer DFA trägt.

  Damit beantragen wir eventualiter Art. 16 VE-DSG mittels Streichungen und Neuformulierungen wie folgt anzupassen (Neuformulierungen = unterstrichen):

  „Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem ~~erhöhten~~ hohen Risiko ~~für die Persönlichkeit oder die Grundrechte~~ einer Persönlichkeitsverletzung der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen.

  Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, ~~die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person~~ das Risiko einer Persönlichkeitsverletzung sowie die Massnahmen, die vorgesehen sind, um das Risiko einer ~~Verletzung der Persönlichkeit oder der Grundrechte~~ Persönlichkeitsverletzung der betroffenen Person zu verringern.

  Der Verantwortliche ~~oder der Auftragsbearbeiter~~ benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen.

  Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen ~~oder dem Auftragsbearbeiter~~ innerhalb von drei Monat nach Erhalt aller erforderlichen Informationen mit."

- Eventualantrag 2: Streichung von Art. 16 Abs. 3 und 4 VE-DSG

  Sollte entgegen dem obenstehenden Antrag an Art. 16 VE-DSG grundsätzlich festgehalten werden, beantragen wir, zumindest die Absätze 3 und 4 zu streichen. Die Kon-

sultationspflicht beim Beauftragten schiesst über das Ziel – und auch über das europäische Regulierungsniveau – hinaus. Gemäss DSGVO ist eine Konsultation nur bei erheblichen Restrisiken vorgesehen (vgl. Art. 36 DSGVO und Erwägung 84). Darüber hinaus ist die vorgesehene dreimonatige Frist für Einwände des Beauftragten zu lange und schafft auch keinerlei Mehrwert, da weder eine Sperrwirkung vorgesehen ist, noch die Einwände als Präjudiz gelten sollen. Hingegen wirkt sie als Innovationshemmer und behindert die internationale Wettbewerbsfähigkeit der Schweizer Wirtschaft (unnötige Verlängerung der time to market). Dass darüber hinaus der Beauftragte später (auch falls er sich nicht vernehmen liess) noch eine Untersuchung soll einleiten können, schafft zusätzlich Rechtsunsicherheit. Schliesslich würde durch die vorgesehene Konsultationspflicht auch beim Beauftragten ein erheblicher Bürokratieschub bzw. ein erheblicher Mehraufwand entstehen, was sich insgesamt nachteilig auf die Zusammenarbeit zwischen Wirtschaft und Beauftragtem bzw. nachteilig auf die Wettbewerbsfähigkeit der Schweizer Wirtschaft auswirken dürfte.

Damit beantragen wir eventualiter, Art. 16 Abs. 3 und 4 VE-DSG ersatzlos zu streichen.

Streichung von Art. 16 Abs. 3 und 4 VE-DSG

3.8 Meldungen von Verletzungen des Datenschutzes (Art. 17 VE-DSG)

- Antrag: Präzisierungen und Ergänzungen von Art. 17 VE-DSG

  Die in Absatz 1 und 4 von Art. 17 VE-DSG enthaltene Formulierung, dass Meldungen „unverzüglich“ zu erfolgen haben, ist zu absolut (auch gegenüber der DSGVO, welche in Art. 33 Abs. 1 als Richtschnur 72 Stunden angibt). Wir beantragen daher, dass die Meldungen „ohne unnötigen Verzug“ zu erfolgen haben.

  Weiter ist in Absatz 1 von Art. 17 festgehalten, dass Meldungen bei „unbefugter Datenbearbeitung oder Verlust von Daten“ zu erstatten sind. Wir erachten diese Begriffe als unzutreffend. Schutzobjekt ist die Persönlichkeit der betroffenen Person bzw. die Sicherheit von Personendaten, weshalb wir beantragen, letztere Terminologie zu verwenden, womit Meldungen dann zu erfolgen haben, wenn eine Verletzung der Sicherheit von Personendaten vorliegt. Dies steht auch im Einklang mit dem EU-Recht, nach welchem eine Meldung nur dann erforderlich ist, wenn eine getroffene Massnahme zum Schutz von Personendaten verletzt wurde (z.B. durch Hacking oder Datendiebstahl) und diese Verletzung zu einem Bruch oder Verlust des Gewahrsams an den Personendaten geführt hat. Alles was über diese Regelung hinausgeht, ist unnötiger Swiss Finish.

  Zudem muss dafür gesorgt werden, dass die Verhältnismässigkeit gewahrt bleibt. So darf es beispielsweise nicht sein, dass jedes fehlgeleitete Mail gemeldet werden müsste. Eine Meldepflicht auslösen sollte nur eine Verletzung der Sicherheit einer erheblichen Zahl von Personendaten.

  Schliesslich ist zur Gewährleistung einer hohen Praxistauglichkeit von Art. 17 auch sicherzustellen, dass die verlangten Meldungen bzw. „Selbstanzeigen“ ohne strafrechtliche Konsequenzen bleiben. Andernfalls würden fundamentale strafrechtliche Garantien wie «Nemo tenetur se ipsum accusare» missachtet und damit auch die EMRK verletzt.

  Abschliessend ist in Absatz 2 von Art. 17 im Sinne einer verhältnismässigen Regelung nur dann eine Informationspflicht an die betroffene Person zu statuieren, wenn der Beauftragte diese Information verlangt. Damit ergibt sich aus der Meldung des Verantwortlichen an den Beauftragten ein konkreter Nutzen für den Verantwortlichen.

Somit beantragen wir, Art. 17 VE-DSG – unter Berücksichtigung der terminologischen Änderung in Art. 16 VE-DSG – wie folgt anzupassen (Anpassungen = unterstrichen):

> Der Verantwortliche meldet dem Beauftragten ~~unverzüglich~~ ohne unnötigen Verzug eine Verletzung der Sicherheit einer erheblichen Zahl von Personendaten ~~unbefugte Datenbearbeitung oder den Verlust von Daten~~, es sei denn die Verletzung des Datenschutzes beinhaltet voraussichtlich nicht das Risiko einer Persönlichkeitsverletzung. Die gemeldete Verletzung wird strafrechtlich nicht verfolgt.
>
> Der Verantwortliche informiert ausserdem die betroffene Person, wenn ~~es zum Schutz der betroffenen Person erforderlich ist oder~~ der Beauftragte es verlangt.
>
> Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten.
>
> Der Auftragsbearbeiter informiert den Verantwortlichen ~~unverzüglich~~ ohne unnötigen Verzug über eine Verletzung gemäss Absatz 1. ~~unbefugte Datenbearbeitung~~.

3.9 Weitere Pflichten des Verantwortlichen und des Auftragsbearbeiters (Art. 19 VE-DSG)

- Antrag: Reduktion bzw. engere Umschreibung der Weiteren Pflichten in Art. 19 VE-DSG

  Umfang und Inhalt der uneingeschränkten Dokumentationspflicht gemäss Art. 19 lit. a VE-DSG sind unklar. Offensichtlich ist aber, dass die vorgeschlagene Regelung über die vergleichbare Bestimmung der DSGVO (Art. 30) hinausgeht. Letztere verlangt ein Verzeichnis. Ein solches – und nur ein solches – ist auch für das Schweizer Datenschutzrecht vorzusehen. Andernfalls müsste z.B. jede E-Mail, jede Chatnachricht etc. dokumentiert werden, was mit einem unverhältnismässigen, nicht praxistauglichen Aufwand einherginge.

  Auch Art. 19 lit. b VE-DSG ist viel zu weit gefasst und unverhältnismässig. Einerseits müssten Verantwortliche und Auftragsbearbeiter über heikle bzw. sensible Datenschutzverletzungen eine Vielzahl Dritter informieren. Andererseits wäre der Aufbau einer neuen Infrastruktur, welche zentralisiert sämtliche Empfängerinnen und Empfänger von Personendaten über Jahrzehnte verwaltet im Vergleich zum Nutzen nicht verhältnismässig. Auf Art. 19 lit. b VE-DSG ist daher zu verzichten.

  Wir beantragen daher, folgende Streichungen bzw. Neuformulierung in Art. 19 VE-DSG vorzunehmen (Neuformulierung = unterstrichen):

  > Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet:
  > ~~a. Sie dokumentieren ihre Datenbearbeitung~~ Sie erstellen ein Verzeichnis für regelmässige Datenbearbeitungen.
  > b. ~~Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2, es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.~~

3.10 Rechte der betroffenen Person (Art. 20 und 21 VE-DSG)

Kernanliegen der nachstehenden Anträge ist es, einem Missbrauch des Auskunftsrechts der betroffenen Person vorzubeugen.

- Antrag: Verzicht auf in jedem Fall kostenlose Auskunft (Art. 20 Abs. 1 VE-DSG)

  Dem zunehmenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke ist entgegenzuwirken. Die Praxis zeigt, dass aktuell einerseits datenschutzrechtliche Begründungen viel zu leicht vorgeschoben werden können, um eine kostenlose Beschaffung von Beweismitteln zur Vorbereitung von Gerichtsverfahren durchzusetzen. Andererseits hat die Anzahl querulatorischer, kosten- und ressourcenintensiver Fälle zu Schikanezwecken ebenfalls spürbar zugenommen. Damit wird das Auskunftsrecht missbräuchlich angewandt.

  Wir beantragen daher, die generelle Kostenlosigkeit der Auskunft zu streichen und stattdessen einen angemessenen Unkostenbeitrag vorzusehen. Ergänzend soll dem Bundesrat die Kompetenz eingeräumt werden, auf Verordnungsstufe festzulegen, in welchen Fällen die Auskunft kostenlos zu erteilen ist.

  Wir beantragen daher, Art. 20 Abs. 1 wie folgt anzupassen (Ergänzungen = unterstrichen):

  „Jede Person kann vom Verantwortlichen ~~kostenlos~~ Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Der Verantwortliche kann für die Auskunft einen angemessenen Unkostenbeitrag erheben. Der Bundesrat regelt, in welchen Fällen die Auskunft kostenlos erfolgt.“

- Antrag: Auskunftsrecht weiterhin am System der Datensammlung anknüpfen (Art. 20 Abs. 1 VE-DSG)

  Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen sowie auch auf hängige Verfahren ist unverhältnismässig. Dies gilt umso mehr, als dass gemäss der in Schweiz geltenden Rechtsprechung kaum ein Auskunftsersuchen je rechtsmissbräuchlich sein kann, weil selbst ein untergeordnetes Datenschutzinteresse ausreicht, um einen Auskunftsanspruch zu bejahen. Die fortgesetzte Anknüpfung am bisher bewährten System der Datensammlung ist sachgerecht und bietet den betroffenen Personen ausreichend Schutz.

  Wir beantragen daher, Art. 20 Abs. 1 VE-DSG (im Konnex mit unseren vorstehenden Ausführungen unter Ziffer 2.9) wie folgt zu formulieren (Ergänzung = unterstrichen):

  Jede Person kann vom Verantwortlichen ~~kostenlos~~ Auskunft darüber verlangen, ob Personendaten über sie im erstellten Verzeichnis gemäss Art. 19 bearbeitet werden.

- Antrag: Verzicht auf zu weit gefasste Informationspflichten (Art. 20 Abs. 3 VE-DSG)

  Art. 20 Abs. 3 VE-DSG ist zu weit gefasst. Zum einen ist es überschiessend, wenn bei jeder aufgrund einer Datenbearbeitung gefällten Entscheidung eine Informationspflicht bestehen würde, weshalb eine solche nur für automatisierte Einzelentscheidung vorzusehen ist. Zum anderen ist der Schluss von Art. 20 Abs. 3 VE-DSG ersatzlos zu streichen. Eine derart weitgehende Begründungs- bzw. Rechtfertigungspflicht ist ein überschiessender Swiss Finish und datenschutzrechtlich nicht zu rechtfertigen. Er würde ausserdem zwangsläufig zu einer Offenlegung von Geschäftsgeheimnissen sowie internen Entscheid- und Ablaufverfahren führen.

Wir beantragen daher, Art. 20 Abs. 3 mittels einer Neuformulierung (= unterstrichen) und einer Streichung wie folgt anzupassen:

Wird aufgrund einer Datenbearbeitung eine automatisierte Einzelentscheidung gefällt, erhält die betroffene Person Informationen über das Ergebnis~~, das Zustandekommen und die Auswirkungen der Entscheidung~~.

- Antrag: Mechanismus gegen Missbrauch des Auskunftsrechts zur Prozessvorbereitung (Art. 21 VE-DSG)

  Angesichts des oben dargelegten Missbrauchs des Auskunftsrechts zur Prozessvorbereitung sollte im totalrevidierten Datenschutzgesetz ein effektiver Abwehrmechanismus vorgesehen werden. Wir schlagen diesbezüglich vor, dass der Verantwortliche die Auskunft verweigern kann, wenn das Ersuchen im Kern nicht datenschutzrechtlichen Zwecken dient. Lehnt der Verantwortliche ein Auskunftsersuchen ab, soll die betroffene Person die Möglichkeit haben zu verlangen, dass der Beauftragte entscheidet, ob das Ersuchen genügend datenschutzrechtlich motiviert ist oder nicht.

  Wir beantragen daher, den datenschutzrechtlichen Zweck als zwingende Voraussetzung für das Auskunftsrecht vorzusehen und Art. 21 um einen neuen Abs. 2 zu ergänzen (= unterstrichen):

„Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. Ausserdem kann die Auskunft nach diesem Gesetze verweigert werden, wenn das Ersuchen im Kern nicht datenschutzrechtlichen Zwecken dient. Lehnt der Verantwortliche ein Ersuchen nach diesem Absatz ab, kann die betroffene Person verlangen, dass der Beauftragte entscheidet, ob das Ersuchen genügend datenschutzrechtlich motiviert ist. Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.“

  Ergänzend oder alternativ kann für den Fall eines im Kern nicht datenschutzrechtlichen Zwecken dienenden Auskunftsgesuches in Art 14 Abs. 4 VE-DSG ein zusätzlicher Rechtfertigungsgrund für die Einschränkung, Aufschiebung oder den Verzicht der Übermittlung von Informationen aufgenommen werden.

3.11 Verwaltungsrechtliche Befugnisse und strafrechtliche Sanktionen (Art. 41ff. und Art. 50ff. VE DSG)

- Antrag: Streichung von Art. 41 Abs. 3 VE-DSG

  Dem Grundsatz „nemo tenetur“ folgend, ist es zumindest fragwürdig, dass dann, wenn jemand seine Mitwirkungspflicht verletzt, eine Hausdurchsuchung vorgenommen werden kann.

  Wir beantragen daher, Art. 41 Abs. 3 VE-DSG zu streichen:

Streichung von Art. 41 Abs. 3 VE-DSG

- Antrag: Streichung von Art. 44 Abs. 3 VE-DSG

  Dass Beschwerden gegen vorsorgliche Massnahmen generell keine aufschiebende Wirkung haben sollen, ist unverhältnismässig. Vorsorgliche Massnahmen können für die Betroffenen mit erheblichen Schäden bzw. Kostenfolgen verbunden sein. Es ist deshalb unerlässlich, dass sich ein Verantwortlicher gegen ein unverhältnismässiges Vorgehen in jedem Verfahrensstadium wirksam zur Wehr setzen kann.

  Wir beantragen daher, Art. 44 Abs. 3 VE-DSG zu streichen:

Streichung von Art. 44 Abs. 3 VE-DSG

- Antrag: Anzeigepflicht in Art. 45 VE-DSG in ein Anzeigerecht umwandeln

  Die in Art. 45 VE-DSG vorgesehene Anzeigepflicht stellt gegenüber dem EU-Datenschutzniveau (Anzeigerecht gemäss Art. 58 Abs. 5 DSGVO / Art. 12bis Ziff. 2 lit. d. SEV 108) einen Swiss Finish dar, auf den zu verzichten ist.

  Wir beantragen daher, Art. 45 VE-DSG wie folgt anzupassen (Anpassungen = unterstrichen):

Art. 45 ~~Anzeigepflicht~~ Anzeigerecht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so ~~teilt~~ ist er befugt, dies den Strafverfolgungsbehörden mitzuteilen.

- Antrag: Streichung der Artikel 50 bis 55 VE-DSG

  Strafrechtliche Sanktionen sind für die Äquivalenz zum europäischen Datenschutzniveau in keiner Weise erforderlich. Weiter ist zu beachten, dass es durchaus möglich ist, dass der gleiche Lebenssachverhalt sowohl unter den räumlich sachlichen Geltungsbereich der DSGVO (verwaltungsrechtliches Verfahren) als auch unter denjenigen des DSG fällt. Dies ist insbesondere dann denkbar, wenn eine Vielzahl von Handlungen oder Unterlassungen, mithin ein unternehmerischer Prozess, sanktioniert werden soll. Nicht kongruente Sanktionssysteme würden unter diesen Umständen zu einer mehrfachen Sanktionierung der natürlichen Person und der Unternehmung für den gleichen Lebenssachverhalt und letztlich zu völlig unhaltbaren Resultaten führen. Darüber hinaus ist die Androhung strafrechtlicher Sanktionen – erst Recht persönlicher strafrechtlicher Sanktionen – unverhältnismässig und in hohem Masse kontraproduktiv. Ganz besonders stossend ist dabei die Strafbarkeit von fahrlässigen DSG-Verstössen. Aber auch der Bussenrahmen für Mitarbeitende von bis zu CHF 500‘000 ist weit überschiessend – umso mehr als er selbst bei Fahrlässigkeit bis zu CHF 250‘000 reicht. Hinzu kommt, dass viele der sanktionierten DSG-Bestimmungen – zu Recht – weniger regel- und eher prinzipienbasiert konzipiert sind. Prinzipienbasierte Normen eignen sich jedoch nicht dafür, mit strafrechtlichen Sanktionen verknüpft zu werden, da für die Rechtsunterworfenen unter strafrechtlichen Gesichtspunkten zu wenig klar bzw. zu wenig eingegrenzt ist, welches Verhalten mit Strafe bedroht ist (nulla poena sine lege certa).

  Persönliche strafrechtliche Sanktionen würden die unternehmensinternen Entscheidungsprozesse lähmen und ein Klima schaffen, in welchem innerbetrieblich niemand mehr bereit wäre, abschliessend Verantwortung für den Datenschutz zu übernehmen. Durch die Schaffung eines persönlichen Strafbarkeitsrisikos würde ganz besonders auch die Funktion des/der betrieblichen Datenschutzverantwortlichen untergraben (anstatt dass diese gestärkt würde). In der Konsequenz würden einerseits betriebsintern keine

Entscheide mehr ohne externe Absicherung getroffen und andererseits aus Sicherheitsgründen Selbstbeschränkungen vorgenommen, welche als Innovationshemmer wirken würden. Damit wiederum würde im Datenschutz der Ausgleich zwischen den Interessen des Datenbearbeiters/des Verantwortlichen und denjenigen der betroffenen Person aus der Balance gebracht.

Wir beantragen daher, die Artikel 50 bis 55 VE-DSG zu streichen und auf neue Sanktionen zu verzichten. Dies umso mehr, als die Nichteinhaltung von Verfügungen des Beauftragten bereits heute via Art. 292 StGB sanktioniert werden kann.

Verzicht auf die Art. 50 bis 55 VE-DSG

Falls wider Erwarten dennoch an strafrechtlichen Sanktionen festgehalten werden sollte, wären ganz besonders die Tatbestände zu überdenken. Insbesondere die (hohen) Strafen für die Verletzung von Melde- oder Dokumentationspflichten und die Bestrafung von fahrlässigen Verletzungen sind in keiner Weise geeignet, den Schutz der Persönlichkeit der betroffenen Person zu stärken; gleichzeitig führen sie aber zu einer innovationshemmenden Angstkultur bei den Datenbearbeitern.

- Eventualanträge für den Fall, dass an strafrechtlichen Sanktionen festgehalten würde: Sollte entgegen dem vorstehenden Antrag an strafrechtlichen Sanktionen festgehalten werden, beantragen wir insbesondere folgende Anpassungen am Regime des VE-DSG:

- Überprüfung der Strafwürdigkeit einzelner Tatbestände, insbesondere der Unterlassungstatbestände wie z.B. Unterlassung der Vornahme einer Datenschutz-Folgenabschätzung (Art. 51 Abs. 1 lit. d. VE-DSG) oder Unterlassung betreffend Vorkehren „Privacy by Design“ (Art. 51 Abs. 1 lit. e. VE-DSG). Äusserst fragwürdig ist – unter dem Blickwinkel von „nemo tenetur“ – auch die Sanktionierung der Verletzung von Mitwirkungspflichten (Art. 50 Abs. 2 lit. c. VE DSG).
- Beachtung des Bestimmtheitsgebots: Nur Tatbestände, welche genügend klar umschrieben sind, können strafbewehrt werden.
- Die fahrlässige Tatbegehung darf nicht strafbar sein.
- Der heutige Art. 35 DSG (Verletzung der beruflichen Schweigepflicht) ist beizubehalten (anstelle Art. 52 VE-DSG): Es ist unverhältnismässig und nicht praktikabel, die Verletzung der beruflichen Schweigepflicht auf alle Personendaten auszudehnen (korrekterweise sind aktuell nur besonders schützenswerte Personendaten und Persönlichkeitsprofile erfasst) und mit einer Freiheitsstrafe von bis zu 3 Jahren zu bedrohen (aktuell Busse). Dies umso mehr, als – im Gegensatz zum Berufsgeheimnis im StGB – vorliegend nicht einmal eine Befreiung vom Berufsgeheimnis durch eine Aufsichtsbehörde vorgesehen ist und auch eine fahrlässige Tatbegehung strafbar wäre. Schliesslich müsste als Voraussetzung im Minimum eine berufliche Schweigepflicht unabhängig von Art. 52 VE-DSG bestehen (z.B. vertraglich), ansonsten so gut wie jeder Berufstätige eine strafrechtlich sanktionierte Schweigepflicht auferlegt bekäme.
- Keine Ausweitung von Art. 179novies StGB (bisher ist nur der Diebstahl von qualifizierten Daten sanktioniert).
- Keine Verlängerung der Verfolgungsverjährung gegenüber der allgemeinen Regel im StGB: Art. 55 VE-DSG will die Verfolgungsverjährung für Übertretungen auf fünf Jahren ausdehnen, obschon Art. 109 StGB drei Jahre vorsieht.

Wir danken Ihnen für die Prüfung unserer Ausführungen sowie für die Berücksichtigung unserer Überlegungen und Anliegen. Bei allfälligen Rückfragen stehen wir Ihnen gerne zur Verfügung. Wir werden uns zudem erlauben, Sie im Nachgang zur Eingabe der vorliegenden Stellungnahme zu kontaktieren und Sie um einen Besprechungstermin zu bitten, an welchem wir gerne unsere Kernanliegen zur DSG-Revision näher erläutern und Fragen Ihrerseits beantworten würden.

Freundliche Grüsse

Swiss Payment Association

Stefan Bolt
Präsident

Dr. Thomas Hodel
Geschäftsführer

Madame la Conseillère fédérale
Simmonetta Sommaruga
Département fédéral de justice et police

Envoi électronique à:
jonas.amstutz@bj.admin.ch

swissuniversities

Comité

Martina Weiss
Secrétaire générale
T +41 31 355 07 40
martina.weiss@
swissuniversities.ch

swissuniversities
Effingerstrasse 15, Case Postale
3001 Berne
www.swissuniversities.ch

3001 Berne, le 30 mars 2017

Prise de position de swissuniversities sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Madame la Conseillère fédérale,

swissuniversities, la Conférence des recteurs des hautes écoles suisses, saisit l'occasion d'exprimer sa position en vue de la révision totale de la loi sur la protection des données. Du point de vue des hautes écoles suisses, ce texte de loi s'adresse principalement au domaine des EPF. Néanmoins, en cas d'adaptation des législations cantonales, cette thématique s'étendrait par conséquent au reste des hautes écoles suisses, ce qui aurait une portée toute aussi importante. De manière générale, les adaptations permettant de s'aligner sur la législation de l'UE ainsi que sur les avancées technologiques sont saluées.

L'ensemble du texte de l'avant-projet avance la terminologie de « *données* », alors que la définition mentionnée dans l'art. 3 let. a et c est celle de « *données personnelles* ». Afin de garantir une cohérence, l'utilisation du terme de « données personnelles » dans tout le texte serait souhaitable, ceci afin de les distinguer des données de la recherche par exemple.

De plus, dans le cadre de cette révision swissuniversities souhaite rappeler l'importance d'éviter autant que possible les surcharges administratives, tant pour les personnes dont les données personnelles sont traitées que pour les personnes chargées du traitement des données personnelles. Elle invite le Conseil fédéral à tenir compte de ces considérations notamment dans l'élaboration de l'ordonnance d'application.

Cela étant, swissuniversities prend position sur les dispositions suivantes comme suit:

Art. 4 al. 6 Principes
La disposition introduite à l'art. 34 al. 4 concernant le fait que «la rectification, l'effacement ou la destruction de données personnelles ne peuvent être exigée des bibliothèques, établissements d'enseignement…» mériterait également de figurer dans le présent article par souci de cohérence.

swissuniversities

Art. 5, 6 Communication de données personnelles à l'étranger
Il est important qu'un niveau de protection adéquat en matière de protection des données soit garanti avec les pays étrangers. Ceci est particulièrement important pour les hautes écoles dans le cadre d'échanges ou de collaborations de chercheurs.

Art. 8, 9 Recommandations de bonnes pratiques
Les hautes écoles saluent l'introduction de l'outil des bonnes pratiques qui permet un lien avec le terrain et l'élaboration de recommandations utiles au plus grand nombre.

Art 12 Données d'une personne décédée
L'introduction de cette disposition qui permet une réglementation du traitement des données personnelles pour les personnes décédées est également saluée par swissuniversities.

Art. 24 al. 2 let. e Motifs justificatifs, Art. 32 Traitement à des fins de recherches, de planification et de statistique
Les hautes écoles prennent note que, selon leur analyse, l'intention de ces deux articles n'est pas modifiée et que le privilège des chercheurs est ainsi maintenu. Nous relevons cependant l'ajout à l'art. 24 al. 2 let. e d'une disposition visant l'anonymisation des données pour le traitement par des personnes privées dans le cadre de la recherche, de la planification ou de la statistique. Des précisions concernant les implications de cette disposition pour les activités de recherche seraient bienvenue dans l'ordonnance.

Art. 34 al. 4 Prétentions et procédures
L'introduction de cette exception permettant de ne pas exiger l'effacement, la destruction ou la rectification des données personnelles pour les fonds gérés par les bibliothèques, les établissements d'enseignement et d'autres institutions patrimoniales publiques est très bénéfique pour les hautes écoles. Cependant, afin de couvrir ce domaine de manière complète le terme « d'établissements de recherche » est également à inclure (et pas seulement les établissements d'enseignement).

Art. 50 et 51 Violation (devoir de renseigner et devoir de diligence)
Nous notons les dispositions pénales en cas de violation par ex. des devoirs de diligence par un responsable du traitement des données et son éventuel sous-traitant situation non couverte par le code pénal et estimons que la notion de « personne privée » en rapport avec la violation n'est pas suffisamment claire. Le rapport de l'avant-projet ne précise pas si l'auteur de la violation doit être compris comme la « personne privée » elle-même en tant que personne physique indépendamment de son lien de subordination avec l'organe responsable du traitement. Il serait utile de préciser le statut de la personne en ce sens.

Par ailleurs, du point de vue des hautes écoles, la thématique du *Big Data* n'est pas suffisamment présente dans l'avant-projet si ce n'est par rapport aux dispositions concernant le profilage. Au vu des avancées technologiques, cette question mériterait d'être traitée de manière plus approfondie afin de garantir une sécurité du droit à cet égard.

En vous remerciant de bien vouloir prendre connaissance de notre position, je vous prie d'agréer, Madame la Conseillère fédérale, l'expression de mes cordiales salutations.

Prof. Dr. Michael O. Hengartner
Président

Amstutz Jonas BJ

Von: Eicher, Lionel <Lionel.Eicher@tcs.ch>
Gesendet: Dienstag, 4. April 2017 10:33
An: Amstutz Jonas BJ
Betreff: Avant-projet de révision LPD
Anlagen: TCS - AP-LPD Prise de position TCS - 04.04.2017.doc; 5279-tcs-voiture-connectee.pdf

Monsieur,

Veuillez trouver en annexe la prise de position du Touring Club Suisse relative à l'avant-projet de révision totale de la loi sur la protection des données, ainsi qu'une annexe.

En vous souhaitant bonne réception, je reste à disposition pour toute question ou complément.

Avec mes salutations les meilleures

Lionel Eicher
Avocat

Touring Club Suisse
Corporate Center
Legal & Compliance
Chemin de Blandonnet 4
CP 820
1214 Vernier
Tel +41 58 827 27 74
Fax +41 58 827 51 37
lionel.eicher@tcs.ch
www.tcs.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Touring Club Suisse

Abkürzung der Firma / Organisation : TCS

Adresse : Chemin de Blandonnet 4

Kontaktperson : Lionel Eicher

Telefon : 058/827.27.74

E-Mail : lionel.eicher@tcs.ch

Datum : 4 avril 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
TCS	**A.** Le TCS ne figure pas sur la liste des destinataires de la consultation. Mais nos près de 1,5 million de membres sont particulièrement concernés par le traitement et la protection des données. En effet, un grand nombre d'acteurs sont intéressés par les données des « consommateurs mobiles », et notamment lorsque ces consommateurs sont sur la route avec leur véhicule. Nous traitons nous-même des données. Nous nous sentons donc légitimés à prendre position.
TCS	**B.** Le TCS salue les grands axes du projet de révision, et notamment : • l'augmentation de la transparence (meilleure information des personnes concernées, quel que soit le type de données collectées et traitées) ; • le renforcement des droits de contrôle des personnes concernées sur leurs données ; • la responsabilisation accrue des responsables du traitement (obligation de mener des analyses d'impact ; protection des données dès la conception et – surtout - par défaut) ; • le maintien du caractère technologiquement neutre de la loi ; • la favorisation de l'autorégulation et la possibilité pour le Préposé d'édicter des bonnes pratiques, qui permettent de mieux cerner les enjeux spécifiques à certains marchés ou types de traitement et de le réguler de manière spécifique. Il est primordial que le droit suisse de la protection des données soit en phase avec les évolutions technologiques et compatible avec le niveau de protection du droit européen, sans nécessairement aller au-delà.

TCS	**C.** D'expérience, le TCS sait que le traitement et la transmission automatique de données par des véhicules peuvent s'avérer extrêmement positifs et dans l'intérêt des usagers. Par exemple en cas de panne, où la transmission de données permet une réaction plus rapide et plus efficace. Selon les circonstances, le conducteur est averti à l'avance de problèmes potentiels et se voit proposer un soutien rapide en cas de dysfonctionnement. En raison de l'introduction du système d'appel d'urgence „eCall", qui devra obligatoirement équiper tous les véhicules neufs dès 2018, les voitures actuellement commercialisées sont quasiment toutes équipées de modules de téléphonie/télématique. Comme le TCS l'a déjà mis en évidence (cf. annexe « Voiture connectée – elle en sait beaucoup sur vous ! »), les constructeurs utilisent ces modules pour collecter et transmettre en grandes quantités les données les plus diverses. Les données collectées sont en principe reliées ou reliables facilement par le constructeur au numéro de châssis du véhicule (VIN Vehicle Indentification Number), et constituent une forme d'historique du véhicule qui peut s'avérer décisif en cas de problème technique ultérieur avec celui-ci. Mais vu la nature et le nombre des données traitées actuellement par certains constructeurs, il serait possible de dresser de véritables profils de conduite, de déplacement voire de personnalité des utilisateurs de véhicules, qui pourraient intéresser quantités d'acteurs (assurances, prestataires de service, autorités, etc.). A partir du VIN : - les constructeurs peuvent relier le véhicule à son détenteur s'il figure dans leurs fichiers clients ; - les autorités peuvent facilement retrouver le détenteur du véhicule (registre MOFIS des véhicules et détenteurs de véhicules). Le potentiel de dommages et effets collatéraux indésirables de ces traitements de données massifs – en partie à l'insu des utilisateurs - est donc réel en terme d'atteinte à la personnalité des conducteurs. Raison pour laquelle le TCS exige que les constructeurs communiquent en toute transparence et publient une liste détaillée des données collectées et traitées par modèle de véhicule, ainsi que les finalités des traitements. Les contrats d'achats des véhicules neufs contiennent en principe des clauses qui autorisent la transmission de l'intégralité des données au constructeur et à son réseau, sans toutefois détailler suffisamment les données traitées et les finalités. S'ils n'acceptent pas ces clauses, les acheteurs risquent de ne pas avoir accès aux services proposés. Le même risque existe si par la suite le propriétaire du véhicule souhaite refuser un développement des services proposés impliquant une extension du traitement des données.

TCS	**D.** Les constructeurs ont la maîtrise totale du flux de données, qu'ils contrôlent électroniquement. Ils peuvent orienter le conducteur vers un prestataire en particulier pour des travaux d'entretien et de réparation. Les conducteurs peuvent se voir proposer des prestations de service dont ils ne veulent pas. Les conséquences sont certes moins graves qu'en cas de violation de la personnalité ou des droits fondamentaux au sens étroit. Mais elles ne sont pas anodines et viennent limiter excessivement la liberté de choix des consommateurs, notamment si le système est programmé pour qu'il contacte systématiquement et exclusivement les prestataires privilégiés du constructeur ou de l'importateur, sans proposer d'alternative. Depuis des années, le TCS exige et se bat pour que les détenteurs de véhicules puissent choisir librement les prestataires auxquels ils souhaitent recourir pour les travaux d'entretien et de réparation, ainsi qu'en cas de panne. Cette demande revêt à notre avis non seulement un aspect de libre concurrence, mais également un aspect de protection des données, voire de protection de la personnalité du consommateur au travers de la maîtrise des données. En effet, même si le conducteur peut faire appel directement (grâce à un téléphone ou à une application) à un prestataire tiers, ce dernier sera confronté à un grave désavantage concurrentiel, car il ne pourra pas avoir accès – ou dans le meilleur des cas n'aura qu'un accès limité et tardif - aux données liées au véhicule, y compris l'historique et les codes de panne ou de réparation. Sous prétexte de sécurité et protection contre les vols, les constructeurs tentent de limiter toujours plus largement l'accès aux données des véhicules. Ce faisant, ils gardent la mainmise sur les données générées par les véhicules et rendent les clients plus dépendants voire captifs de leurs services et prestations.
TCS	**E.** Finalement, la collecte de données et le consentement de l'acheteur peuvent aisément se faire de manière propre et transparente lors de l'achat d'un véhicule neuf. La situation est plus délicate en cas de revente d'un véhicule. Les données collectées constituent une forme d'historique du véhicule qui peut s'avérer décisif en cas de problème ultérieur avec celui-ci. L'acheteur d'un véhicule d'occasion doit pouvoir exiger le transfert des données et de l'historique du véhicule à un autre prestataire.

TCS	**F.** Pour les différents motifs exposés ci-dessus, le TCS estime : ➢ que le projet de loi devrait reprendre le droit à la portabilité des données, tel que prévu dans la législation européenne (art. 20 R UE 2016/679 ; cf. également Article 29 Data Protection Working Party – lignes directrices du 13.12.2016). Sur ce point, l'argumentaire du rapport (ch. 1.6.4) ne convainc pas. En particulier, il est paradoxal d'une part de plaider le renforcement de la compétitivité des entreprises suisses (donc l'accès pour les entreprises suisses au marché européen/aux clients européens dans une logique de libre concurrence) pour justifier l'alignement du droit suisse aux règles européennes (rapport, condensé et ch. 1.3), et d'autre part de se distancer de ces principes dès qu'il s'agit de donner aux consommateurs un outil qui leur permet concrètement de faire jouer cette concurrence. La seule introduction de ce principe dans la loi pourrait également contribuer à limiter le volume des données collectées et traitées. ➢ que l'élaboration de recommandations de bonnes pratiques dans le domaine automobile est indispensable.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
TCS	LPD	4	2		Compte tenu du développement du Big Data et du niveau de connectivité croissant, il pourrait être opportun d'ancrer les principes d'évitement des données (Datenvermeidung) et de minimisation des données (Datensparsamkeit) dans la loi. S'ils découlent du principe de proportionnalité, les mentionner („notamment") permettrait d'insister sur deux des aspects essentiels de celui-ci.
TCS	LPD	4	6		Il conviendrait à notre avis de mentionner clairement dans la loi que le consentement peut être révoqué en tout temps. Il s'agit-là d'un droit considéré comme fondamental, reconnu par la pratique et la doctrine.
TCS	LPD	13			Le devoir d'information étendu, indépendamment du type de données personnelles, est une amélioration qui est à saluer. Elle est indispensable pour assurer la transparence nécessaire et voulue pour le consommateur.
TCS	LPD	13	1		Compte tenu de la multitude des situations couvertes, il ne serait pas opportun de prévoir dans la loi une forme particulière pour le devoir d'informer. Il conviendra par contre de préciser les bonnes pratiques au moyen de recommandations. Notamment, compte tenu du développement du commerce électronique, il conviendra d'exiger, en cas de conclusion de commandes/contrats sur internet, que les informations relatives aux données soient facilement téléchargeables ou imprimables.
TCS	LPD	59		a	La formulation de la lettre a (et la formulation du chiffre 8.1.10.3 du rapport, différente en allemand et en français) est ambiguë. On ne comprend pas si le responsable doit seulement être en mesure de faire une analyse d'impact (sur les processus existants ?) dans les 2 ans qui suivent l'entrée en vigueur, ou s'il doit l'avoir faite dans ce délai.
TCS	CPC	113s			La suppression des frais de justice est nécessaire pour ne pas dissuader les consommateurs de faire valoir leurs droits.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
TCS	1.6.4	Le droit à la portabilité est de l'avis du TCS un instrument important de la maîtrise de leurs données par les consommateurs. Il devrait être implémenté. Voir remarque générale F.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
	----	----

Données des véhicules

Voiture connectée – elle en sait beaucoup sur vous !

Aujourd'hui, une multitude de systèmes électroniques équipent les voitures modernes que l'on appelle aussi «voitures connectées». Une énorme quantité de données sur le véhicule et sur l'automobiliste sont collectées par celles-ci à chaque déplacement. Cependant, personne ne sait quel usage est réellement fait de ces informations. La question est de savoir à qui appartiennent ces données qui renseignent sur le véhicule et l'automobiliste dans ses moindres détails. Le TCS, en collaboration avec la FIA (Fédération Internationale de l'Automobile) a voulu faire toute la lumière sur cette épineuse question.

La voiture connectée sera capable d'empêcher des accidents.

Lors de la conception d'un nouveau véhicule, la sécurité et le confort sont au cœur de toutes les recherches: ABS, GPS et internet font partie depuis longtemps des standards de l'équipement. L'ordinateur de bord et une pléthore de capteurs et de caméras aident certes à la conduite et à la maniabilité, ils peuvent cependant aussi surveiller en permanence la voiture et son conducteur. Différents systèmes se contrôlent réciproquement ainsi que tout le fonctionnement du véhicule. Ils communiquent directement avec le conducteur et aussi de façon autonome avec le monde extérieur. C'est le cas du dispositif d'appel d'urgence «eCall» qui sera obligatoire dans l'Union européenne sur tous les véhicules neufs dès avril 2018. En cas d'accident, un module de téléphonie mobile organise automatiquement une liaison avec le numéro d'appel d'urgence en transmettant un certain nombre de données qui informent sur le lieu de l'accident, la direction sur l'autoroute et également des informations sur le véhicule comme le nombre de passagers. L'appel d'urgence peut aussi être déclenché manuellement par un bouton dans le véhicule.

Déclencher manuellement un appel d'urgence via un bouton.

Fonctionnant sur le même principe, d'autres services peuvent être actionnés comme le «bCall», un dispositif d'appel pour le dépannage ou pour demander des services tels réservations d'hôtels, de restaurants, etc. Essayer d'échapper à cette technologie est de plus en plus difficile, car les actuelles fonctionnalités en ligne se développent constamment et sont d'un essor sans précédent. De futurs systèmes d'assistance et des fonctions de conduite autonomes ne sont toutefois réalisables qu'avec un réseau de grande ampleur. On rencontrera ainsi des voitures qui aideront le conducteur à trouver une place de stationnement grâce à des capteurs à ultrasons qui enregistrent les places de stationnement potentiellement libres et qui les transmettent à la collectivité via un serveur.

Des affaires en tout genre

Les voitures contemporaines enregistrent, stockent et transmettent un nombre gigantesque de données. Hormis l'industrie automobile, personne ne sait exactement ce qu'il advient de ces informations. Certes, améliorer la sécurité et poser un diagnostic à temps est primordial. Or, contrairement à l'utilisation du smartphone, les automobilistes ne savent pas que le serveur du constructeur automobile est secrètement alimenté par le générateur de données de la voiture, communiquant les profils et les habitudes d'utilisation de l'automobiliste. Dans une «voiture connectée», le conducteur profite de la navigation en temps réel, de messages automatiques sur les accidents et de protection antivol. Techniquement, tout est faisable et enregistrable: la vitesse, les différents régimes moteur, les températures du moteur, le nombre de fois où l'ESP ou le prétensionneur de ceinture se sont déclenchés, le nombre de passagers transportés, le nombre de réglages du siège, le temps d'utilisation de l'éclairage, et bien plus encore. Ce qui suppose une infinité d'exploitation possible. Outre l'industrie automobile, les compagnies d'assurances, les sociétés de leasing ou les gestionnaires de flottes l'ont bien compris. Par exemple: les constructeurs peuvent diriger «leurs» véhicules pour l'entretien dans leurs garages concessionnaires. Les assurances peuvent à l'aide de boîtes noires installées volontairement offrir des primes sur mesure, ou bien, sur la base du nombre de fois où la pédale de frein ou des gaz a été actionnée, diminuer les prestations après un accident. L'assuré qui roule (trop) souvent à des régimes moteur élevés peut être considéré comme un conducteur à risques ou bien, en cas de sinistre, l'assurance peut contester les garanties.

Sous la loupe

Le TCS, en collaboration avec la Fédération Internationale de l'Automobile (FIA), a analysé les données qui étaient relevées dans le bloc électronique de deux BMW, une 320d et une i3, tout en sachant que l'analyse

d'autres modèles de voiture de marques différentes donnerait selon toute vraisemblance le même résultat. Où, pendant combien de temps et dans quel but toutes ces informations sont-elles stockées ? Sont-elles transmises à l'extérieur et sont-elles consultables pour le propriétaire de la voiture (par ex. le diagnostic effectué par le garage) ? A l'aide du logiciel de diagnostic de BMW, on a d'abord réalisé une vue d'ensemble des boîtiers électroniques et étudié quelles données pouvaient être vues par l'atelier de réparation. En effet, réaliser une analyse détaillée de tous les boîtiers électroniques aurait demandé, selon l'actuelle estimation, plusieurs années-homme de travail. Ainsi, seule une petite partie des informations a pu être consultée, ce qui, pour la 320d, donne déjà une bonne vue d'ensemble.

Nombre de données qui sont affichées durant le trajet sont des données d'ordre technique. Ainsi, le boîtier électronique de la 320d stocke les éventuelles erreurs de divers composants: on y trouve entre autres le kilométrage, la vitesse, le régime ou la température du moteur. Toutes ces données sont utiles à l'atelier pour la réparation et sont ensuite normalement effacées. Le contenu de la mémoire des erreurs est aussi transmis au constructeur automobile dans le but d'assurer le diagnostic à distance via le service BMW en ligne «Connected Drive». De même, les informations affichées et stockées par le Check-Control avec le kilométrage servent non seulement au garage mais aussi au constructeur pour le suivi des problèmes. Cependant, avec cette pléthore d'informations, on ne peut théoriquement empêcher une interprétation erronée du véhicule, comme en cas de température ou de régime du moteur trop élevés. La clé de la voiture stocke elle aussi des données comme le numéro de châssis, le kilométrage ou le contenu du réservoir de carburant. A l'aide d'un appareil lecteur approprié, le garage peut déjà effectuer un premier suivi du véhicule. Dans le cadre de la transmission des données FASTA, diverses informations (numéros d'identification, versions de logiciels, mémoire des erreurs, données d'usure et d'utilisation) sont directement transmises au serveur de BMW quand le véhicule est branché dans le garage sur l'appareil de diagnostic. Ceci est avant tout utile pour assurer la qualité et détecter aussi les fraudes (par ex. le chip-tuning).

Données «apparentes» ?

Les modèles BMW 320d et BMW i3 stockent de nombreuses données de «l'utilisateur» qui renseignent sur le style de conduite du conducteur et sur le profil de l'utilisation du véhicule. Sur la 320d, ce qui reste dans un premier temps stocké dans la voiture, est, sur la i3, transmis en partie par téléphonie mobile au constructeur par le «Last State Call», à savoir automatiquement chaque fois après avoir coupé le moteur et verrouillé la voiture.

Une BMW 320d stocke outre les erreurs de fonctionnement du véhicule, diverses informations sur le propriétaire, comme:

- régime maximal du moteur avec à chaque fois le kilométrage (déductions sur le style de conduite);
- trajets jusqu'à 5, 20, 100 km et plus de 100 km (déductions sur le profil d'utilisation);
- durée d'utilisation des différents mode de conduite (déductions sur le style de conduite);
- durée d'utilisation de chaque source d'éclairage;
- nombre d'ajustements du siège conducteur (déductions sur le nombre de conducteurs);
- nombre d'utilisation du CD/DVD;
- nombre de fois où les ceintures de sécurité se sont bloquées (par ex. freinage brusque) (déductions sur le style de conduite);
- branchement d'un portable sur bluetooth (selon le modèle de téléphone);
- les destinations introduites dans le système de navigation;
- accélération, vitesse, position des pédales de gaz et de frein avant le déclenchement de l'airbag.

Sur la BMW i3, voci un florilège des renseignements récoltés sur le propriétaire:

- données détaillées de la batterie (comme l'état de charge, température des cellules, etc.);
- lieux où le moyen de transport a été changé;
- mode de conduite sélectionné (Eco, Eco plus, sport);
- données du range extender (REX);
- le nombre de fois où le chargeur a été utilisé;
- comment et où la batterie a été chargée, quel était son niveau de décharge;
- le kilométrage après chaque processus, comme charger la batterie;
- position des 16 dernières stations de recharge;
- les 100 dernières positions d'arrêt du véhicule.

Pourquoi BMW mémorise-t-elle de telles données ? Personne ne le sait exactement, cependant il est facile de deviner ce que de telles informations peuvent générer. Ce qui soulève nombre de questions, dans l'intérêt du consommateur.

Toutes marques confondues

Les données ont été étudiées non seulement sur les modèles BMW 320d et i3 mais aussi sur la Mercedes-Benz classe B dotée du système me-connect et sur la Renault Zoe. Les résultats de la BMW 320d et de la Mercedes-Benz classe B sont pratiquement identiques, les légères divergences étant dues au niveau d'équipement différent. Cependant, étant donné que l'étendue de l'analyse n'était pas la même pour les quatre véhicules, les résultats ne peuvent être comparés entre eux.

Voici les données relevées sur la Mercedes-Benz classe B:

- toutes les deux minutes, la position GPS de la voiture et des données (le kilométrage, la consommation, le contenu du réservoir, la pression des pneus et aussi le niveau des liquides du réfrigérant, de lave-glace ou de frein) sont transmises au constructeur;
- le nombre de fois où le prétensionneur de la ceinture de sécurité a été activé (déductions sur le style de conduite);
- les informations de la mémoire d'erreurs sur le régime moteur trop élevé (déductions sur le style de conduite);
- les kilomètres parcourus sur autoroute, hors agglomération et en ville (déductions sur le profil d'utilisation);
- le nombre de fois où le système d'éclairage a été utilisé;

- les derniers 100 cycles de recharge et décharge de la batterie, avec heure, date et kilométrage.

Voici les informations sur la Renault Zoe:
- Renault peut à tout moment empêcher la recharge de la batterie via la téléphonie mobile (par ex. en cas de non-paiement de la facture de leasing);
- Renault a accès aux informations du bus de données CAN via la téléphonie mobile. Ce diagnostic à distance est mis hors service par défaut, mais peut être à tout moment activé par le constructeur;
- à chaque trajet, des données sont envoyées toutes les 30 minutes à Renault (numéro de châssis, divers numéros de série, date, heure, position GPS, température, charge et tension de la batterie à haut voltage). Le constructeur peut accéder aux informations à tout moment;
- outre les fonctions programmées entre le serveur Renault et la Renault Zoe, d'autres fonctions peuvent être demandées à volonté via la téléphonie mobile.

Transparence
Afin de ne pas perdre la confiance de leurs clients, les constructeurs automobiles doivent miser sur plus de transparence. Ainsi, pour chaque modèle de voiture, une liste de toutes les données collectées, traitées, stockées et transmises doit être publiée et mise à la disposition du consommateur. Pour les nouveaux modèles, une instance neutre doit être en mesure de vérifier que les dispositions relatives à la protection des données sont respectées. Actuellement, seul le constructeur automobile a connaissance de ces données et peut y accéder. Le détenteur de la voiture ne peut aucunement agir: lors de l'achat du véhicule, des clauses à ce sujet sont le plus souvent incluses dans le contrat qu'il doit signer. Selon plusieurs sondages, la majorité des consommateurs ne s'oppose pas à un enregistrement et à une transmission des données, seulement selon des conditions fixées et souhaitées par eux. La FIA est du même avis: les données sont la propriété du détenteur du véhicule. Celui-ci doit avoir la possibilité de désactiver la collecte et la transmission des données qui ne sont pas absolument nécessaires au fonctionnement du véhicule en toute sécurité. Il doit aussi pouvoir décider quel usage peut être fait de ses données, sans que la qualité des services attendus en soit entravée. Aujourd'hui, des services en ligne sont à la disposition de l'automobiliste soit totalement, soit pas du tout. Ainsi, si l'on souhaite seulement des informations sur les embouteillages en temps réel, il faut consentir à communiquer toutes ses données. Cette problématique pourrait à l'avenir s'aggraver. En plus de l'industrie automobile, les géants de l'informatique comme Apple ou Google s'intéressent aussi de près aux données du véhicule, car ils ont bien senti que c'est un futur marché lourd de plusieurs milliards. La question de la protection des données se pose à chaque enregistrement de données. En Suisse, la loi autorise par exemple la pose dans la voiture d'un appareil enregistreur de données (enregistreur de données d'accident). Les données collectées ne doivent toutefois être destinées que pour le but initialement défini. Mais il n'existe aucune autorisation juridique quant à l'utilisation des données collectées en dehors de ces buts d'application. Au sens strict, même les dispositifs d'appel d'urgence (eCall) des constructeurs automobiles sont illégaux si la géolocalisation d'un signal du téléphone mobile (le système est basé dessus) est effectuée sans l'accord exprès de l'utilisateur.

BMW Vehicular CrowdCell: les cellules mobiles femt pour tous. Ces cellules contribuent à l'amélioration du réseau du portable. De nombreuses petites cellules de radios mobiles et relais sont activées aux stations de base déjà existantes et peuvent élargir la capacité et la zone de couverture des réseaux.

Les propriétaires de la nouvelle Apple-Watch profitent de la collaboration du géant informatique californien avec BMW. Le BMW Remote App pour appareils IOS permet de porter les données importantes de sa voiture au poignet. BMW travaille par ailleurs aussi avec les constructeurs du système Android.

Exigences du TCS
Le TCS exige la plus grande transparence, le libre accès aux données, la sécurité des données et le contrôle des données par le détenteur du véhicule.
- Les constructeurs automobiles doivent établir une liste, accessible au public, détaillant toutes les données des véhicules qui sont collectées, traitées, stockées et transmises à l'extérieur.
- Cette liste doit pouvoir être consultée et être compréhensible pour les consommateurs, au garage ou sur internet.
- Lors du lancement de nouveaux modèles, la liste des données doit être contrôlée par une autorité neutre pour vérifier le respect des dispositions légales sur la protection des données.
- Des contrôles aléatoires doivent permettre de vérifier que le constructeur automobile a publié une liste complète des données.
- Tant le propriétaire du véhicule que les garages indépendants et les dépanneurs doivent pouvoir consulter librement toutes les données du véhicule. Les procédures d'enregistrement doivent être adéquatement sécurisées.
- Les constructeurs automobiles doivent être contraints de respecter les prescriptions sur la protection des données;
- Hormis les données prescrites par le législateur (comme le contrôle antipollution ou eCall), le propriétaire du véhicule doit avoir la possibilité de désactiver facilement le traitement et la transmission des données, pour autant que celles-ci ne soient pas absolument indispensables au fonctionnement du véhicule en toute sécurité.

Campagne FIA «My Car My Data»
Lors d'un sondage réalisé à l'échelle européenne, il ressort que 95% des personnes interrogées, soit 12'000, souhaitent un encadrement juridique protégeant leurs droits et les données collectées par les véhicules. L'enquête a été menée sur l'initiative de la FIA, association faîtière internationale des automobilistes, qui représente 111 clubs automobiles avec 38 millions d'adhérents. La campagne «My Car My Data» (http://mycarmydata.fr) également lancée par la FIA, a pour but de sensibiliser le public sur les données des véhicules. Elle exige la libre décision de l'automobiliste pour l'échange des données et le libre choix de fournisseurs de services.

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Engelberg, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DDSG)

Sehr geehrte Frau Bundesrätin

Sie haben am 21. Dezember 2016 interessierte Kreise eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nimmt Tele Alpin AG gerne wahr.

Die Tele Alpin AG ist ein Anbieter von Telekommunikationsnetzinfrastrukturen und -dienstleistungen. Wir leisten damit einen grossen Beitrag an die digitale Vernetzung der Schweiz und deren Bevölkerung. Unser Kerngeschäft ist die Datenverarbeitung. Diese Daten erfüllen zunehmend und überwiegend die Voraussetzungen von Personendaten bzw. Daten, die zu einer Identifikation einer Person führen könnten. Datenschutz und Datensicherheit, sowie die entsprechenden Regulierungen sind daher für uns eine der wichtigsten Geschäftsgrundlagen. Entsprechend besteht eine hohe Betroffenheit, wenn diesbezüglich neue Regulierungen zur Diskussion stehen.

Gerne nehmen wir wie folgt Stellung, wobei wir zunächst auf einige grundsätzliche Punkte eingehen, ehe wir – wie verlangt – zu den einzelnen Bestimmungen des VE-DSG Stellung beziehen und Anträge stellen:

A. Grundsätzliche Bemerkungen

1. Chancen der Digitalisierung und damit auch Chancen der Datenbearbeitung

Die Digitalisierung bietet für die Zukunft ein enormes Entwicklungspotential und sollte durch unterstützende Rahmenbedingungen – gerade im Bereich Datenbearbeitung – gefördert werden. Die Schweiz sollte ein Wirtschaftsstandort für digitale Geschäftsmodelle sein und grösstmögliche Freiräume für die Datenbearbeitung zulassen. Grundsätzlich sollte jede Form von Datenbearbeitung zulässig sein und die informelle Selbstbestimmung sollte über Auskunfts- und Kontrollrechte realisiert werden. Ein Regulierungskonzept darf nicht der Vorstellung folgen, eine „Datenbearbeitung"

durch Unternehmen sei *per se* anrüchig. Ein modernes Datenschutzgesetz ist weiter auch kein spezielles Konsumentenschutzrecht.

Die im Vorentwurf vorherrschende „Verbots- und Bestrafungskultur" sollte deshalb so nicht umgesetzt werden. Die Datenschutzgesetzgebung ist bisher – und gemäss VE-DSG noch mehr – als Konsumentenschutzgesetzgebung stark von gesetzlichen Einschränkungen für Unternehmen geprägt, die jedoch in der Praxis durch Einwilligungserklärungen der Datensubjekte übersteuert werden können. Dies führt heute gesamthaft nicht zu mehr Datenschutz, sondern nur zu aufwendigeren Einwilligungsverfahren und damit höheren Transaktionskosten bei der Geschäftsabwicklung.

Wir begrüssen eine Stärkung des Rechts auf informelle Selbstbestimmung, lehnen jedoch die Stossrichtung ab, dass zukünftig einzelfallbezogene Zustimmungserklärungen eingeholt werden müssen. Für eine wirtschaftliche Geschäftsabwicklung muss es möglich sein, in einem Vertragsverhältnis eine pauschale Einwilligung über allgemeine Geschäftsbedingungen abzuschliessen. Die Grundlagen dazu genügen im UWG.

2. Gleichwertigkeit des Datenschutzes in der CH und in der EU

Datenschutzregulierung ist heute kein nationales Thema mehr. Die modernen Kommunikationsnetze und die technologischen Entwicklungen machen den Datenverkehr zu einem globalen Thema. Ein freier Datenverkehr ist aus unserer Sicht unbedingt zu erreichen, insbesondere durch eine gegenseitige institutionelle Anerkennung eines gleichwertigen Datenschutzes mit möglichst vielen Ländern. Allen voran natürlich mit der Europäischen Union und den USA. Damit können für Unternehmen hohe administrative Hürden und Kosten vermieden werden. Dabei sind die notwendigen Bestimmungen für eine Gleichwertigkeit im Datenschutz umzusetzen.

2.1 Unnötiger „Swiss Finish"

Ein Grund für die Revision des DSG ist gemäss Erläuterungsbericht des EJPD/BJ die Entwicklung des Datenschutzes im europäischen Raum. Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) EuDSGVO in Kraft. Zudem gilt die EU-Richtlinie 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen. Die DSG-Revision soll die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Die Annäherung würde zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür bilden, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht (obschon unserer Ansicht nach dies auch das bestehende DSG weiterhin tun würde). Die Revision des Schweizer DSG geht aber in mehreren Fällen über das Schutzniveau der EU hinaus, was nicht nachvollziehbar ist. Beispiele für diesen Swiss Finish sind:

a) Art. 13 Abs. 3 und 4 VE-DSG sehen eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister) sowie bei der Weitergabe von jeglichen Personendaten vor. Für den Adressaten solcher Informationen führt dies in einer zunehmend über digitale Geschäftsprozesse gesteuerten Gesellschaft zu einer Informationsflut. Nicht einmal die EU-Richtlinie 680/2016 vom 27. April 2016 sieht diesen Detaillierungsgrad vor.

b) Art. 16 Abs. 3 VE-DSG sieht eine Informationspflicht des Datenschutzbeauftragten über die Datenschutz-Folgeabschätzungen in jedem Fall vor. Die EU-Richtlinie 680/2016 hingegen fordert dies in Art. 27 und 28 nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen.

c) Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung (Art. 25). Diese besagt lediglich, dass gewisse Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen.

d) Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EuDSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell.

e) Auch der Ansatz des VE-DSG betreffend Profiling geht über die Bestimmungen der EuDSGVO und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der EuDSGVO noch der Konvention. Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren. Die Bedingung einer vorgängigen ausdrücklichen Einwilligung bei jeder Art von Profiling schiesst über das Ziel hinaus. Profiling soll nicht bereits bei dessen Erstellung schutzrelevant werden.

f) Überschiessende Informationspflichten (z.B. Art. 6 Abs. 2 oder Art. 13 Abs. 5 VE-DSG), die Geschäftsgeheimnisse betreffen können (gemäss Art. 6 Abs. 2 VE-DSG informiert der EDÖB über heikle Verfahren und Geschäftsgeheimnisse, ohne dass ein datenschutzrechtlicher Tatbestand dazu vorliegen müsste). Diese Pflicht ist dem EU Recht (inkl. E-SEV 108) fremd.

Wir lehnen Bestimmungen ab, die über das Mass der europäischen Regelungen hinausgehen. Es besteht keine Notwendigkeit für einen «Swiss Finish». Entsprechende Vorschläge sind ersatzlos zu streichen oder auf ein supranationales Mass zurückzunehmen.

2.2 Keine Doppelspurigkeiten bei der Aufsicht

Da viele Schweizer Unternehmen eine Tätigkeit in der Europäischen Union ausüben, werden diese auf der Grundlage von Art. 3 DSGVO i.V.m. Art. 55 Abs. 1 DSGVO auch der Aufsicht der nationalen Datenschutzbehörden unterstehen. Diese Doppelaufsicht bringt einerseits zahlreiche Rechtsunsicherheiten mit sich und andererseits verursacht sie eine massive administrative Zusatzbelastung der Schweizer Unternehmen. Es ist mit der Europäischen Union eine Gleichbehandlung auszuhandeln, damit die Schweizer Datenschutzaufsicht gegenseitig in das Konzept des „One-Stop-

Shop" nach Art. 56 DSGVO einbezogen werden kann. Heute steht diese für Unternehmen ausserhalb der EU nicht zur Verfügung.

3. Fehlende verfassungskonforme Regulierungskosten Folgeabschätzung (RFA)

Die Bundesverfassung verpflichtet in Art. 170 die Bundesversammlung, die Massnahmen des Bundes auf ihre Wirksamkeit zu prüfen („Die Bundesversammlung sorgt dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden."). Nach Art. 141 Abs. 2 Bst. f) ParlG müssen in der Botschaft an das Parlament eine Kosten-Nutzen Abschätzung sowie nach Bst. g) die Folgen für die Wirtschaft und die Gesellschaft erläutert werden.

Auf Seite 23 des Erläuterungsberichts zum VE-DSG werden die Regulierungskosten als unbedeutend eingestuft. **Diese Einschätzung ist falsch**. Alle Unternehmen bearbeiten heute in zunehmendem und komplexem Mass Personendaten bzw. Rohdaten für Persönlichkeitsprofile und sind damit von den Bestimmungen direkt betroffen. **Die Regulierungskosten sind für alle Unternehmen massiv höher als beschrieben!**

3.1 Mangelhafte Durchführung der Regulierungsfolgeabschätzung

Wir stellen die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG grundsätzlich in Frage. Die Unternehmensbefragung basiert auf einer völlig ungenügenden Nettostichprobe von lediglich 95 (!) Fragebogen, wovon keines der Unternehmen den Fragebogen vollständig beantwortet hat. Insbesondere wurden die spezifischen Daten zu den Folgen nur von wenigen Unternehmen beantwortet. Keines der angefragten Unternehmen machte bei einer Interviewerhebung mit.[1] Die Studienverfasser – immerhin eine renommierte Revisionsgesellschaft – erklären dazu ohne jeden Interpretationsspielraum selbst:

> „Die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten waren sowohl in Bezug auf Quantität als auch Qualität unzureichend; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands."[2]

> „Die Quantität und die Qualität des Rücklaufs aus der Unternehmensbefragung ermöglichte es nicht, in repräsentativer Weise eine Hochrechnung zur Schätzung der finanziellen Auswirkungen zu erstellen."[3]

Eine korrekte Aussage ist daher aufgrund dieser Angaben nicht möglich und es ist erstaunlich, dass das EJPD in ihrem Erläuterungsbericht zum Ergebnis kommt, die zu erwartenden Regulierungskostenfolgen seien unbedeutend. Im Bericht wird lediglich angegeben, dass die fehlenden statistischen Erhebungen durch Gespräche mit Fachpersonen ausgeglichen worden sind. Auch das ist falsch: Die angeblichen Gespräche sind ein dreistündiges Gespräch vom 4. Mai 2016 mit neun Fachpersonen, wo auch der Geschäftsführer von SUISSEDIGITAL anwesend war. Die anwesenden Vertreter haben bei der mündlichen Erörterung der Fragen wiederholt darauf hingewiesen, dass eine verbindliche Beurteilung der „statistischen" Ergebnisse aufgrund der unzureichen-

---

1 Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

2 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 8.

3 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

den Quantität und Qualität der Umfrageergebnisse absolut unmöglich sei. Wir finden die sehr kritischen Aussagen der angeblich befragten Fachpersonen im Bericht heute mit keinem Wort erwähnt. In der Studie wird lediglich vermerkt, dass diese Aussagen nicht repräsentativ sind.[4] Über den Verlauf der Sitzung vom 4. Mai 2016 wurde durch den Geschäftsführer von SUISSEDIGITAL ein internes Protokoll erstellt; dort ist auch die – für die desaströse Datenqualität – von einem Berater des Bundes vorgebrachte Begründung vermerkt, für die Untersuchung wären halt lediglich CHF 80'000.- Budget zur Verfügung gestellt worden.

Wir sind der Meinung, dass damit die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt wurde. Das ist für einen Vorentwurf von derartiger wirtschaftlicher Tragweite nicht akzeptabel und wir behalten uns diesbezüglich alle rechtlichen Massnahmen ausdrücklich vor, sollte dieser Umstand im Zuge der Abwicklung des weiteren Gesetzesprojekts keine Beachtung finden.

3.2 Methodisch fehlerhafte Durchführung der Regulierungsfolgeabschätzung

Die Einteilung der Unternehmen in drei Kategorien scheint völlig willkürlich und basiert nicht auf der tatsächlichen Betroffenheit. So werden zum Beispiel die Mehrheit der gewerblichen KMU-Betriebe (wie Metzgerei, Schreinerei, Papeterie, Spenglerei, Elektriker, lokale Transporteure, Baubetriebe, Bauernbetriebe, Velomechaniker, Coiffeur etc.) in das Segment A als Unternehmen mit geringer datenschutzrechtlicher Exponierung und keinem oder geringem Einsatz von Web-IT-Technologien eingeteilt.

Dabei wird verkannt, dass heute – und vor allem in Zukunft – jedes Unternehmen moderne Informatikmittel einsetzt, eine Internetseite und Social Media-Profile betreibt und damit Personendaten bearbeitet. Gerade kleine Unternehmen nutzen überdurchschnittlich viel cloudbasierte Internetapplikationen oder beziehen ihre gesamte Geschäftssoftware aus der Cloud. Als Beispiel deinen Cloud-Angebote wie „Microsoft 365" für kleinere und mittlere Unternehmen mit einer Datenspeicherung im Ausland, u.a. auch in den USA. Damit müssen diese 335'000 (55.1%) Unternehmen korrekterweise dem Segment B als Unternehmen mit mittlerer bis grosser datenschutzrechtlicher Exponierung (innerhalb der Schweiz und weltweit tätige Unternehmen und/oder Einsatz von Web-IT-Technologien wie Webseiten für Marketing oder Nutzung von Cloud Services) zugeordnet werden.[5]

3.3 Falsche Angaben zur Regulierungsfolgeabschätzung im VE-DSG

Die Folgekosten für die Wirtschaft werden überhaupt nicht quantifiziert. Vielmehr wird behauptet:

> „Die Analyseergebnisse zeigen, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen generell nur geringfügig betroffen sind. Die Auswirkungen der Revision auf dieses Segment sind somit verhältnismässig gering. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im VE vorgesehenen Massnahmen stärker betroffen als Grossunternehmen, da

[4] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 25.

[5] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 5.

sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei."[6]

Nur schon durch das Zusammenziehen der in der Studie vorhandenen – ungenügenden – Schätzungen, wird der massive Umsetzungsaufwand sichtbar, entsprechend unerklärlich es ist, dass dies im Erläuterungsbericht mit keinem Wort erwähnt wird:[7]

Handlungspflichten nach VE-DSG	**Einmalig**	**Wiederkehrend**	**Kosten CHF**
Informationspflichten			
Pflicht zur Information der betroffenen Person	60 – 100 Stunden	30 Stunden	3000 – 40'000
Auskunft über Aufbau der Datenbearbeitung	4- 12 Stunden	1.6 h – 3 Tage pro Fall	Keine Angabe
Informationspflicht Automatisierte Entscheidungen	30 – 50 Stunden	3 Stunden pro Fall	10'000
Meldung Data Breach	5 – 20 Stunden	2 – 5 Stunden pro Fall	5'000 – 10'000
Datenherrschaft			
Mitteilung, Löschung, Beschränkung	14 – 20 Stunden	3 Stunden pro Fall	100 – 5'000
Pflichten auf Datenübertragbarkeit	12 Stunden	2 Stunden pro Fall	7'500
Unternehmensinterne Datenschutzorganisation			
Datenschutz-Folgeabschätzung[8]		20 – 160 h pro Fall	5'000 – 30'000
Privacy by Default	1 – 40 Stunden		500 – 5'000
Betriebliche Datenschutzbeauftragter		500 – 2'000 h pro Jahr	
Grenzüberschreitender Datenverkehr			
Genehmigung Standard Datentransfervereinbarung	50 Stunden		5'000

Auch wenn man nur die Aufgaben einbezieht, die alle Unternehmen beachten müssen, und als Basis Minimalschätzungen als Grundlage für eine Hochrechnung annimmt, ergeben sich Umsetzungskosten für die Schweizer Wirtschaft von über CHF 1'532'160'000, resp. im Durchschnitt von CHF 2'520 pro Unternehmen.[9] In der Praxis dürften diese noch wesentlich höher liegen.

Es muss heute nämlich davon ausgegangen werden, dass alle Unternehmen von diesen vorgeschlagenen Bestimmungen betroffen sind, insbesondere da auch alle ohne jede *de minimis*-Schwelle den exzessiven Strafbestimmungen unterliegen. Selbst die Studienverfasser gehen von einer vergleichsweise hohen Belastung der Unternehmen aus:

> „Gleichsam haben mehrere Fachpersonen im Rahmen der Fachgespräche vorgebracht, dass bei gleicher Datenbearbeitungstätigkeit KMU stärker von der Revision oder generell von den datenschutz-rechtlichen Verpflichtungen betroffen sind als grosse Unternehmen, da ihnen die notwendige Compliance-Infrastruktur fehle resp. sie im Verhältnis teurer sei. In Bezug auf die

---

6 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetze und Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 23.

7 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 27 ff.

8 In einer Studie der Europäischen Union zur Datenschutz-Folgeabschätzung (Privat Impact Analysis) wurden die Kosten pro Durchführung auf € 14'000 – 149'000 geschätzt. Quelle: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, Seite 70.

9 608'000 Unternehmen mit einem Aufwand von 84 Stunden zu einem Stundenkostensatz von CHF 30.

> Unternehmen der Segmente B und C ist demgegenüber von einer vergleichsweise hohen Belastung durch die Revision des Datenschutzgesetzes auszugehen."[10]

Aufgrund der methodischen Fehlbeurteilung wird in Verbindung mit der ungenügenden Datenerhebung bei den Unternehmen sichtbar, dass einerseits die Regulierungsfolgenabschätzung nicht korrekt durchgeführt wurde und andererseits die Regulierung für die gesamte Wirtschaft massiv höhere Kosten zur Folge hat.

Bislang wurde die korrekte Durchführung eines Vernehmlassungsverfahrens oder sogar die Vorlage einer Botschaft an das Parlament ohne solche Regulierungskostenfolgenabschätzung nie durch die Judikative überprüft. Wir und mit uns die gesamte Schweizer KMU-Wirtschaft müssen darauf vertrauen, dass dieses Manko vor einer Parlamentsvorlage unbedingt und professionell korrigiert wird. Andernfalls muss diese Korrektur spätestens vom Parlament bzw. den entsprechenden Rechtskommissionen vorgenommen werden. Sollte diese nicht gelingen, würden die neuen Regulierungen spätestens beim Vollzug einer auf den VE-DSG gestützten Verordnung über die akzessorische Normenkontrolle Fälle für Gerichte.

B. Forderungen

Wir stellen weiter folgende Forderungen grundsätzlicher Natur an das revidierte Datenschutzgesetz:

a) Eine klare Regelung der Einwilligung und eine gesetzliche Vermutung der Einwilligung bei definierten Vorgängen, wie zum Beispiel einem Vertragsverhältnis würden den Unternehmen wesentlich mehr Rechtssicherheit und weniger administrativen Aufwand bringen. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten.

b) Auf die unüberschaubare Menge von Informations- und Dokumentationspflichten der Unternehmen sowie der rein administrativen Meldungen an den Beauftragten ist grundsätzlich zu verzichten. Hingegen sollten Unternehmen vom Beauftragten innerhalb von 30 Tagen eine verbindliche Beurteilung einer Datenbearbeitung verlangen können (Negativattest, *Comfort Letter* oder dergleichen).

c) Auf eine Ausweitung des Strafenkatalogs ist zu verzichten. Insbesondere sind nur materielle Datenschutzverletzungen zu sanktionieren und keinesfalls Verletzungen von Dokumentations- oder Meldepflichten an den Beauftragten. Es bestehen heute genügend Möglichkeiten bei tatsächlichen Verstössen, Sanktionen gegen fehlbare Unternehmen zu verhängen. Der Verweis auf das Persönlichkeitsrecht für Ansprüche von betroffenen Personen hat sich ebenfalls bewährt und muss nicht geändert werden.

C. Stellungnahme zu den einzelnen Artikeln

Im Übrigen finden Sie unsere Anträge und Bemerkungen zu den einzelnen Artikeln wie verlangt in der nachfolgenden tabellarischen Übersicht:

---

[10] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 53.

VE-DSG	Anträge und Bemerkungen
1. Abschnitt: Zweck, Geltungsbereich und Begriffe	
Art. 1 Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.	**Antrag zu Art. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. Wenn nicht im Gesetzestext (Art. 1 oder Art. 2 Abs. 1 VE-DSG) selbst, so ist diese Klarstellung spätestens in der Botschaft unmissverständlich anzubringen.
Art. 2 Geltungsbereich [1] Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen durch: a. private Personen; b. Bundesorgane. [2] Es ist nicht anwendbar auf: a. Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden; b. Personendaten, die durch die Eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden; c. Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden; d. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007, die in der Schweiz Immunität geniessen, wie das Internationale Komitee vom Roten Kreuz. [3] Dieses Gesetz ist nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Für die Bearbeitung der übrigen Daten sind sie von	**Antrag zu Art. 2 Abs. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. **Antrag zu Art. 2 Abs. 2 lit. c)**: Beibehaltung des geltenden Wortlauts. Der VE will neu nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung nicht mehr gelten. Das ist weder sachgerecht, noch nachvollziehbar, und führt zu schwerwiegenden Konsequenzen im Zusammenhang mit der Führung von Gerichtsverfahren (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).

VE-DSG	Anträge und Bemerkungen
der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ausgenommen. [4] Die Bundesversammlung und der Bundesrat sind von der Aufsicht durch den Beauftragten ausgenommen.	**Antrag zu Art. 2 Abs. 5 (neu)**: Der im Erläuterungsbericht erwähnte Allgemeincharakter des VE (*Lex Generalis*) ist in einem neuen Abs. 5 ausdrücklich vorzusehen. Es ist festzustellen, dass datenschutz- bzw. datenbearbeitungsrelevante Regelungen in kantonalen und anderen Erlassen des Bundes dem allgemeinen DSG vorgehen (*Lex Specialis*). Damit können entsprechende Einzelhinweise im VE gestrichen werden. Solche Einzelerwähnungen sind nicht sinnvoll und gefährlich, weil diese das im Erläuterungsbericht erwähnte, selbstverständliche Wirkungsprinzip „*Lex Specialis derogat Lex Generalis*" grundsätzlich in Frage stellen. Diese generelle Klarstellung ist aber vor allem deshalb wichtig, weil das Prinzip beim Anspruch auf Information über bearbeitet Personendaten schon nach geltendem Recht immer wieder in Frage gestellt worden (Beispiel: Ein Teil der allgemeinen Datenschutz-Lehre meint unzutreffend, dass Art. 8 DSG auch im Bereich von fernmelderechtlich geschützten Personendaten anwendbar bleibt, ergo die spezifischen fernmelderechtlichen Datenschutzbestimmungen in Art. 43 bis 46 FMG und 9. Kapitel „Fernmeldegeheimnis und Datenschutz", Art. 80 ff. FDV, den Datenschutz bei der Datenherausgabe im Zusammenhang mit der Erbringung von Fernmeldediensten nicht als „Lex Specialis" abschliessend regelt.)
2. Abschnitt: Allgemeine Datenschutzbestimmungen	
Art. 3 Begriffe Die folgenden Ausdrücke bedeuten: a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; b. *betroffene Person:* natürliche Person, über die Daten bearbeitet werden; c. *besonders schützenswerte Personendaten:* 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,	**Antrag zu Art. 3 lit. c Ziff. 4**: Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Der im Erläuterungsbericht enthaltene Hinweis, wann auch Fotos als biometrische Personendaten gelten, ist unverständlich. Es ist klarzustellen, wann Fotos als Personendaten gelten; dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biometrische Daten gelten.

VE-DSG	Anträge und Bemerkungen
5. Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe; d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten; e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten; f. *Profiling:* jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;	**Bemerkung zu Art. 3 lit. c Ziff. 5**: Die Bestimmung ist in dieser allgemeinen Form problematisch; etwa wenn Vermögensdelikte zur Diskussion stehen, von welchen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste. **Antrag zu Art. 3 lit. f)**: Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes „Daten". Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um „Personendaten". Andere Daten werden gemäss Erläuterungsbericht durch den Begriff „Personendaten" konsumiert. Der Begriff des „Profiling" ist zu unbestimmt und gefährdet damit die Rechtssicherheit mit nicht ermittelbaren Kostenfolgen für die gesamtschweizerische Wirtschaft. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem „Persönlichkeitsprofil" des geltenden Rechts abzulehnen. **Generelle Bemerkung zu Art. 3 lit. f)**: Die nicht reflektierte Übernahme von Begriffen des ausländischen Rechts führt dazu, dass sich die Anwendung und Auslegung von Schweizer Recht zukünftig primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und hier vor allem deshalb nicht sachgerecht. weil der Begriff des „Profiling" gegenüber dem EU-Recht sogar nicht mit einem „Swiss Finish" versehen und inhaltlich ausgeweitet wird. Die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich schädlich, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als „Voraussage" eines späteren Verhaltens interpretiert werden könnten. Die Revision schiesst hier

VE-DSG	Anträge und Bemerkungen
	weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen, ohne alle erheblichen Verpflichtungen einzuhalten, die der VE mit dem „Profiling" verknüpft. Es gäbe zahlreiche Beispiele von sicherlich nicht beabsichtigten und unbedachten Konsequenzen in längst etablierten und von Konsumenten akzeptierten digitalisierten Wirtschaftsprozessen: Man denke nur an die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind. So etwas Selbstverständliches würde plötzlich problematisch.
g. *Bundesorgan:* Behörde und Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist; h. *Verantwortlicher*: Bundesorgan oder private Person, das oder die – alleine oder zusammen mit anderen – über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet;	**Antrag zu Art. 3 lit. h und i**: Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), *eventualiter* zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu einer unklaren – teilweise unsinnigen – Aufteilung der Verantwortung und zu Doppelspurigkeiten. Zudem wird übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen *kann*. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für wen?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den Verantwortlichen?) geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den Verantwortlichen?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht, ergo auch hier nicht einmal das Generalargumente der Bundesverwaltung zieht, man müsse etwas so regeln, weil es ausländisches Recht so vorgebe und man andernfalls auf eine „Blacklist" gesetzt werde. Dass „Arbeitnehmer mit einem Arbeitsvertrag" (gibt es auch Arbeitnehmer ohne Arbeitsvertrag?) nicht unter den Begriff des "Auftragsbearbeiters" fallen, steht zwar im Erläuterungsbericht. In Anbetracht der merkwürdigen Formulierung „Arbeitnehmer mit Arbeitsvertrag" wäre es aber dringend nötig, dies klar und deutlich im Gesetzestext zu normieren (Simpler Vorschlag: „Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter").
i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	

VE-DSG	Anträge und Bemerkungen
Art. 4 Grundsätze [1] Personendaten müssen rechtmässig bearbeitet werden. [2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.	**Antrag zu Art. 4 Abs. 2**: In Absatz 2 ist zu ergänzen, dass nicht nur die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und verhältnismässig zu sein hat, sondern auch die Ausübung anderer Rechte und Pflichten gemäss diesem Gesetz.
[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.	**Antrag I zu Art. 4 Abs. 3**: Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Der Erläuterungsbericht argumentiert, es sei mit der redaktionellen keine materielle Änderung beabsichtigt (das steht im Übrigen – beschwichtigend – an zahlreichen anderen Stellen des Erläuterungsberichts). Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann in der Praxis eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. **Antrag II zu Art. 4 Abs. 3**: Im Erläuterungsbericht wird beim Beispielkatalog von nicht erkennbaren Datenbearbeitungen die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch Privatunternehmen erwähnt. Es wird dazu auf den sog. Logistep-Entscheid (BGE 136 II 508 E.4) verwiesen. Dieser Verweis und dieses Beispiel ist deplatziert, zumal das Bundesgericht in diesem Entscheid ausdrücklich festgehalten hat, seine Begründung beziehe sich auf geltendes Recht, welches durch den Gesetzgeber im Lichte der mit der Sammlung solcher IP-Adressen zusammenhängenden vertretbaren Absicht allenfalls zu korrigieren sei. Es ist unverständlich, weshalb nun gerade dieses Beispiel als „Nicht-Erkennbarkeit einer Bearbeitung von Personendaten" aufgeführt ist. Vielmehr wäre gerade vorzusehen, dass die Beschaffung von IP-Adressen zum Zwecke der Strafverfolgung von diesem Grundsatz ausdrücklich nicht erfasst wird.
[4] Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.	**Antrag zu Art. 4 Abs. 4**: Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.
[5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten. [6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von	**Antrag zu Art. 4 Abs. 5**: Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Erläuterungsberichts sind auch hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten. *Eventualiter* ist Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind" zu beschränken (Streichung des Rests). Bekanntlich fängt die "Bearbeitung" schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE).

VE-DSG	Anträge und Bemerkungen
besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.	Eine fortdauernde Verpflichtung zur Nachführung ist nicht erfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Selbst wenn so etwas möglich wäre, ist dieses Konzept nicht finanzierbar. **Antrag zu Art. 4 Abs. 6**: Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f) vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (vgl. dazu auch die Bemerkungen zu Art. 3 lit. f VE). Die im Erläuterungsbericht vertretene Ansicht, mit der vorgeschlagenen Redaktion von Abs. 6 möge die in der Lehre ausgetragene Kontroverse über die „Ausdrücklichkeit" einer Einwilligung beendet sein, ist die blosse Äusserung einer Hoffnung. Das Gegenteil wird der Fall sein und die Kontroverse verstärkt werden: Es lassen sich über die Begriffe „freiwillig", „freiwillig und eindeutig", „ausdrücklich" und die Abgrenzung zur blossen „Einwilligung" (vgl. z.B. Art. 6 Abs. 1 lit. a VE) vorzügliche juristische Publikationen schreiben.
Art. 5 Bekanntgabe ins Ausland [1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. [2] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz gewährleistet. [3] Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch: a. einen völkerrechtlichen Vertrag; b. spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde; c. standardisierte Garantien, insbesondere durch Vertrag: 1. welche der Beauftragte vorgängig genehmigt hat, oder 2. welche der Beauftragte ausgestellt oder anerkannt hat; d. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig genehmigt wurden: 1. durch den Beauftragten, oder 2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet. [4] Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 Buchstabe b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien informieren. [5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c	**Antrag zu Art. 5 Abs. 3 lit. d)**: Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG. **Antrag zu Art. 5 Abs. 4 bis 6**: Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt – wie aus dem Wort ersichtlich – nach den Weisungen des Verantwortlichen, dem – wiederum entsprechend seiner Bezeichnung – die Verantwortung für die Information des Beauftragten obliegt.

VE-DSG	Anträge und Bemerkungen
Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht. [6] Der Verantwortliche oder der Auftragsbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit. [7] Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.	**Antrag zu Art. 5 Abs. 7**: Es ist zu ergänzen, dass der Bundesrat die Liste quartalsweise aktualisieren muss und dazu ein ständiges Staaten-Monitoring etabliert. Heute ist die Liste von Staaten mit der Gewährleistung von angemessenem Schutz des EDÖB gut etabliert und ausreichend dynamisch. Wenn nun die Kompetenz zum Bundesrat hinaufgereicht wird, ist sicherzustellen, dass der Bundesrat diese sehr operative Rolle auch bedarfsgerecht wahrnehmen muss.
Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: a. die betroffene Person im Einzelfall eingewilligt hat; b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt; c. die Bekanntgabe im Einzelfall unerlässlich ist für: 1. die Wahrung eines überwiegenden öffentlichen Interesses, oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde; d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; e. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; f. die Daten aus einem gesetzlich vorgesehenen Register stammen, das zugänglich ist für die Öffentlichkeit oder für Personen mit einem schutzwürdigen Interesse, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. [2] Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.	**Antrag zu Art. 6 Abs. 1 lit. a)**: Es ist zu präzisieren, wie sich die hier ohne die Zusätze „freiwillig", „eindeutig" oder „ausdrücklich" auskommende Einwilligung gestalten lässt. **Antrag zu Art. 6 Abs. 2**: Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1 lit. b, c oder d ins Ausland bekanntgegeben wird. Das gilt erst recht, wenn neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Es ist mit dieser Doppelnennung nicht klar, wer am Ende für die Erfüllung der Meldepflicht verantwortlich ist. Die Folge davon

VE-DSG	Anträge und Bemerkungen
	wird sein, dass sowohl der Verantwortliche, als auch der Auftragsbearbeiter Meldung erstatten müssen, um sich nicht einer Strafverfolgung auszusetzen. Die Bestimmung ist weiter auch deshalb heikel, weil solche Meldungen z.T. sensible Geschäftsinformationen betreffen (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetzen auch für Dritte einsehbar werden. Auch hier wurde offenbar in keiner Weise an den berechtigten Schutz von Geschäftsgeheimnissen gedacht.
Art. 7 Auftragsdatenbearbeitung [1] Die Bearbeitung von Personendaten kann durch Vereinbarung oder Gesetz einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. [2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters. [3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. [4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.	s **Antrag zu Art. 7 Abs. 2**: Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Die Pflichten des Auftragsbearbeiters ergeben sich aus den Pflichten des Verantwortlichen und des zwischen diesem und dem Auftragsbearbeiter abgeschlossenen Vertrags. **Antrag zu Art. 7 Abs. 3**: Schaffung der Möglichkeit einer generellen Einwilligung.
Art. 8 Empfehlungen der guten Praxis [1] Der Beauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen. [2] Der Verantwortliche sowie interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie. [3] Er veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.	**Antrag zu Art. 8**: Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der von diesem vordefinierten "interessierten Kreise" – erfahrungsgemäss ist die Zusammenstellung von solchen *Round Tables* „interessierter Kreise" völlig willkürlich und intransparent – ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. Es ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen *tel quel* als Ermessensindikator zugrunde legen werden. Der Beauftragte wird damit im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich faktisch gemäss seinen Eindrücken Recht setzen. Dies wiegt umso schwerer, als der Beauftragte nicht einmal Jurist oder Anwalt sein oder über Erfahrungen in der Unternehmensjurisprudenz verfügen muss.
Art. 9 Einhaltung der Empfehlungen der guten Praxis [1] Befolgt der Verantwortliche die Empfehlungen der guten Praxis, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren. [2] Die Datenschutzvorschriften können auch auf andere Weise eingehalten werden, als in Empfehlungen der guten Praxis vorgesehen.	**Antrag zu Art. 9**: Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zu Lasten des Datenbearbeiters führen.

VE-DSG	Anträge und Bemerkungen
Art. 10 Zertifizierung [1] Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen. [2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.	Keine Bemerkungen
Art. 11 Sicherheit von Personendaten [1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden. [2] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.	Keine Bemerkungen
Art. 12 Daten einer verstorbenen Person [1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und: a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder b. keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen. [2] Ein schutzwürdiges Interesse wird bei Personen vermutet, die mit der verstorbenen Person in gerader Linie verwandt sind oder mit ihr bis zum Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten. [3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.	**Antrag I zu Art. 12**: Die Bestimmung ist aus dem VE zu entfernen und die Thematik in die aktuell laufende Revision des Erbrechts zu integrieren. Derart weitreichende, thematisch in einem allgemeinen Datenschutzgesetz nicht zu erwartende Regularien als Folge des Todes gehören dorthin, wo der Tod und dessen Folgen abgewickelt werden. Das ist das allgemeine Erbrecht. Die dort zu erlassenden datenschutzrechtlichen Bestimmungen sind *lex specialis* zum DSG. Weiter ist die gesamte Bestimmung voll von schwerwiegenden Unklarheiten: Wer urteilt über das Vorliegen überwiegender Interessen der verstorbenen Person? Wer über die überwiegenden Interessen Dritter? Wie verhält sich das schutzwürdige Interesse zum überwiegenden Interesse Dritter? Weiter ist die Verknüpfung des schutzwürdigen Interesses mit Verwandtschaftsgraden unbegründet und willkürlich. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären. Es gäbe unzählige weitere Beispiele. Art. 4 Abs. 1 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen. **Antrag II zu Art. 12 Abs. 3**: Die Bestimmung ist gerade umzukehren. Sie ist abzuändern, dass im Zusammenhang mit dem Vollzug dieser Bestimmung Amts- und Berufsgeheimnisse von Geheimnisträgern jederzeit geltend gemacht werden können. Alles andere wäre absurd: Es gäbe zahlreiche Beispiele, die dramatische Konsequenzen zur Folge hätten. Man denke nur an den Fall, in

VE-DSG	Anträge und Bemerkungen
	welchem ein Mitglied einer zerstrittenen Erbengemeinschaft den Vertrauensanwalt des Verstorbenen nötigen würde, ihm Einsicht in die Personendaten zu geben, die er dann auch noch auf Geheiss vernichten müsste.
[4] Jeder Erbe kann verlangen, dass der Verantwortliche Personendaten des Erblassers kostenlos löscht oder vernichtet, ausser: a. der Erblasser hat dies zu Lebzeiten ausdrücklich untersagt; oder b. der Löschung oder Vernichtung stehen überwiegende Interessen des Erblassers oder von Dritten entgegen.	**Antrag zu Art. 12 Abs. 4**: Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und Löschungsrecht völlig ausreichen.
[5] Vorbehalten bleiben spezielle Bestimmungen anderer Bundesgesetze.	**Bemerkung zu Art. 12 Abs. 5**: Es ist bezeichnend, dass genau bei dieser Bestimmung noch einmal explizit betont wird, was gemäss Art. 2 VE ohnehin generell gilt. Diese Bestimmung steht mit zahlreichen spezialgesetzlichen Regelungen komplett im Widerspruch. Insofern ist der Sinn einer solchen allgemeinen Datenschutzklausel im Zusammenhang mit Verstorbenen nicht ersichtlich.
3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters	**Vorbemerkungen**: - Es fehlt an Übergangsbestimmungen, welche regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar und führt über Jahre hinweg zu grossen Unsicherheiten in der Praxis. - Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention – und nicht die DSGVO – den Massstab für die Angemessenheit des Datenschutzes zu liefern haben.
Art. 13 Informationspflicht bei der Beschaffung von Personendaten [1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. [2] Er teilt der betroffenen Person spätestens bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten; c. den Zweck der Bearbeitung.	**Antrag zu Art. 13 Abs. 1 und 2:** Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird zwar festgehalten, es genüge eine solche "allgemeine Information". Das ist allerdings im Wortlaut der Bestimmung nicht ersichtlich. In der vorliegenden Form ist die Bestimmung nicht praktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. In der Telekommunikationsbranche ist dies selbst mit solchen Massenschreiben nicht möglich, weil regelmässig Personendaten bearbeitet werden, mit welchen ein Dienstanbieter nie in einem direkten Kontakt

VE-DSG	Anträge und Bemerkungen
	steht. Die Bestimmung ist schlicht nicht umsetzbar und schiesst über das Ziel hinaus: Selbst die insgesamt absolut ungenügende Analyse der Regulierungskostenfolgeabschätzung von PWC hält dies so fest.
[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.	**Antrag zu Art. 13 Abs. 3** Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist nicht akzeptierbar. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, in welchen persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger jeder Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen.
[4] Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die er bearbeitet, mit.	**Antrag zu Art. 13 Abs. 4**: Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
[5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden; werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.	**Antrag zu Art. 13 Abs. 5**: Ersatzlos streichen. *Eventualiter* ist die aktive Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten zu beschränken. Die vorgesehene uferlose Informationspflicht ist schlicht nicht umsetzbar und – selbst wenn diese umsetzbar wäre – völlig unverhältnismässig. Hinzu kommt, dass die Bestimmung sogar noch weiter geht als die DSGVO, die immerhin noch einen Monat Frist gewährt. Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird. Weiter muss man sich bei diesem Konzept auch die Auswirkungen auf Konsumentenseite vor Augen führen: Da in Zukunft praktisch kein Wirtschaftszweig mehr ohne die Beschaffung und Bearbeitung von Personendaten auskommen wird, wird der Konsument mit solchen Informationen regelrecht zugespamt werden. Die einzelne Information versinkt im Informationsmeer. Der Adressat wird abgestumpft und negiert die diesem Informationswahn zu Grunde gelegten Absichten, den Adressaten vor „bösen" Datenbearbeitern zu schützen.
Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen [1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt.	**Bemerkung**: Wurde unnötigerweise enger als die SEV 108 gefasst. **Antrag zu Art. 14 Abs. 1:** Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung),

VE-DSG	Anträge und Bemerkungen
[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn: a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.	in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist. **Antrag zu Art. 14 Abs. 2**: 1. Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der VE für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
[3] Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn: a. ein Gesetz im formellen Sinn dies vorsieht; oder b. dies aufgrund überwiegender Interessen Dritter erforderlich ist.	
[4] Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten: a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt; b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls eine der folgenden Voraussetzungen erfüllt ist: 1. es ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich; oder 2. die Übermittlung der Information stellt den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage.	**Antrag zu Art. 14 Abs. 4 lit. a**: Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns (der als Dritter gilt) unnötig erschwert.
II. [5] Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	
Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung [1] Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.	**Antrag zu Art. 15 Abs. 1**: Streichen. *Eventualiter* ist die Bestimmung um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a DSGVO EU (2016/679) zu ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als untauglicher Versuch, Konsumenten vor jeder Art automatisiert getroffener Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche" Auswirkung ist, dürfte letztlich von der Sensibilität des Be-

VE-DSG	Anträge und Bemerkungen
	troffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte. Die saloppe Begründung im Erläuterungsbericht „denn solche Entscheidungen sind in allen Wirtschaftsbereichen immer häufiger und werden teilweise auf der Grundlage falscher Daten getroffen" reicht jedenfalls nicht aus, einer solchen weitreichenden Bestimmung ein öffentliches Interesse mitzugeben. Art. 22 DSGVO nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor. Eine von der DSGVO abweichende Regelung wäre demnach zweifellos auch für die Schweiz zulässig. Es ist nicht nachvollziehbar, weshalb hier ein „Swiss Finish" erfolgt. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung seit der Gründung des Bundesstaates frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Das hat nichts damit zu tun, ob die Grundlage für einen solchen Entscheid aus Papier, aus Menschen oder aus Algorithmen stammt.
[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.	**Antrag zu Art. 15 Abs. 2**: Streichen. Wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand für die gesamte Schweizer Wirtschaft. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens.
[3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.	**Antrag zu Art. 15 Abs. 3**: Streichen. Es ist nicht nachvollziehbar, weshalb gerade der Staat automatisierte Entscheidungen ohne Informations- und Anhörungspflicht durchführen darf. Das Handeln des Staates ist an die Einhaltung von Grundrechten geknüpft. Diese Bestimmung zeugt von einem sehr gefährlichen Grundverständnis der Gesetzesredaktoren: Hier der gute Staat, dort die böse Wirtschaft. Es ist daran zu erinnern, dass solche Ausnahmen für staatliches Handeln vor allem Mittel totalitärer Staaten sind, sich für nichts rechtfertigen zu müssen.
Art. 16 Datenschutz-Folgenabschätzung [1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen. [2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern.	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschätzungen bei jeder beliebigen Datenbearbeitung vornehmen zu müssen; abgesehen davon muss die Abschätzung ohnehin durchgeführt werden, um herauszufinden, ob die Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit führt. Die Kosten sind angefallen, selbst wenn man zum Schluss käme, dass gar keine Risiken bestehen. Hier wird ein bürokratisches Monstrum freigesetzt,

VE-DSG	Anträge und Bemerkungen
[3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen. [4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit.	das in der Privatwirtschaft im Ergebnis nichts ausser gigantischen Kosten bringen wird. Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier, Zeit und Geld dafür aufwenden müssen. Denn anders als der Bund, der – wie im vorliegenden Fall – meint, mit wenig Geld eine verfassungskonforme Regulierungskostenfolgenabschätzung machen zu können, hat der private Datenbearbeiter mit seiner Existenz gerade zu stehen, wenn er einer solchen Verpflichtung nicht im Sinne des Gesetzes nachkommen sollte. **Antrag zu Art. 16 Abs. 3 und 4**: Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist ist weiter viel zu lang und zeugt nicht von einem Verständnis wirtschaftlicher Prozesse. Wenn es bei solchen Folgeabschätzungen Beanstandungen gibt, dann hat der Beauftragte Einwände innert 7 Tagen zu adressieren, ansonsten Geschäftsprozesse während Monaten blockiert bleiben müssen. Wir weisen dazu auch darauf hin, dass allein die Überprüfung der zu erwartenden Schwemme solcher Meldungen, ein Herr von neuen Beamten erforderlich machen wird, die nichts anderes tun, als solche Folgeabschätzungen zu prüfen.
Art. 17 Meldung von Verletzungen des Datenschutzes [1] Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.	**Antrag zu Art. 17**: Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien unseres Rechtsstaates. Es ist nicht zu rechtfertigen, dass diese Garantie gerade im Datenschutzrecht nicht mehr gewährleistet werden soll; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer Flut von Selbstanzeigen zu rechnen, die erneut nur den Apparat des Beauftragten übermässig aufblähen würde. Diese aus den USA bekannten Regulierungsmechanismen sollten in der Schweiz nicht angefasst werden. Der Druck auf die Verantwortlichen wäre enorm und würde ein pragmatisches und/oder vernunftgetriebenes Handeln von vornherein ausschliessen. Die Selbstanzeige ist in einem solchen System immer die sicherste Art, sich prophylaktisch „compliant" zu verhalten.

VE-DSG	Anträge und Bemerkungen
[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. [3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. [4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung.	**Antrag zu Art. 17 Abs. 2**: Streichung; In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen. **Bemerkung zu Art. 17 Abs. 4**: Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen [1] Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. [2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.	**Antrag zu Art. 18**: Streichung. Die Bestimmung ist redundant. Der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Art. 19 Weitere Pflichten Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie dokumentieren ihre Datenbearbeitung; b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.	**Antrag zu Art. 19**: Streichung; Die Bestimmung ist nicht nur überflüssig, sondern teilweise nicht umsetzbar. Die stipulierte Dokumentationspflicht würde insbesondere für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b ist von vornherein nicht umsetzbar. Teilweise lassen sich dagegen auch absurde Beispiele vorbringen: Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine allfällige Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gemäss Art. 25 machen zu müssen. Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Auch hier gilt es, sich auch in die Situation der Informationsadressaten zu versetzen. Dass Millionen unnützer Mitteilungen versandt werden ist das eine; dass aber jeder Einzelne tausende solcher Informationen von allen Datenbearbeitern erhält, das andere. Diese Informationen sind die neuen „Spam Waves" und werden bei den Adressaten keinerlei Wirkung erzielen, geschweige denn, diese in ihren Persönlichkeiten schützen.
4. Abschnitt: Rechte der betroffenen Person	
Art. 20 Auskunftsrecht	

VE-DSG	Anträge und Bemerkungen
[1] Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. [2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten; c. der Zweck der Bearbeitung; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; e. das Vorliegen einer automatisierten Einzelentscheidung;	**Antrag zu Art. 20 Abs. 2 lit e)**: Streichen; in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich(vgl. auch den Antrag zu Art. 15).
f. die verfügbaren Angaben über die Herkunft der Personendaten;	**Antrag zu Art. 20 Abs. 2 lit. f)**: Streichen; die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntgeben zu müssen, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen.
g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4. [3] Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.	**Antrag zu Art. 20 Abs. 3**: Streichen; *eventualiter* ist Abs. 3 auf die Pflicht zu beschränken, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt: Entweder wird ein Vertrag geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, eine Begründungspflicht für den Nicht-Abschluss von Verträgen über das Datenschutzrecht einzuführen. Das kann nicht das Ziel des Datenschutzes sein. Die Verweigerung von Geschäftsbeziehungen ist ausschliesslich ein wettbewerbs- und lauterkeitsrechtlicher Tatbestand. Es ist lebensfremd, wenn man heute meint, allein durch eine modernere Datenbearbeitung würden Fehler bei der Einschätzung von geschäftlichen Tätigkeiten verursacht. Die Frage, ob zwei Personen miteinander kontrahieren, basierte seit jeher auf der Einschätzung von „Personendaten“ und „Persönlichkeitsprofilen“. Es kam bislang niemand auf die Idee, im allgemeinen oder im besonderen Teil des OR eine Begründungspflicht für den Nicht-Abschluss eines Vertrages zu fordern. Vielfach wird gerade deshalb kein Vertrag geschlossen, weil die persönliche Chemie nicht stimmt. In den seltenen Fällen wird dies der anderen Seite so direkt mitgeteilt. Wieso es weiter für den Schutz der Persönlichkeit erforderlich sein soll, dem Betroffenen die Auswirkungen eines Nicht-Entscheids zu erläutern, ist völlig unerfindlich, wenn

VE-DSG	Anträge und Bemerkungen
[4] Personendaten über die Gesundheit können der betroffenen Person durch einen von ihr bezeichneten Arzt mitgeteilt werden. [5] Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat. [6] Niemand kann im Voraus auf das Auskunftsrecht verzichten.	nicht gleichzeitig eine Rechtsmittelmöglichkeit besteht, die am Ende in einen Vertragszwang münden könnte. Beides wird zum Glück und konsequenterweise (jedoch im Kontext aller anderen Ideen fast schon überraschend) nicht gefordert.
Art. 21 Einschränkung des Auskunftsrechts [1] Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. [2] Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.	Keine Bemerkungen
Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende [1] Werden Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben: a. Die Daten geben Aufschluss über die Informationsquellen; b. Es müsste dafür Einsicht in Entwürfe für Publikationen gewährt werden; c. Die freie Meinungsbildung des Publikums würde gefährdet. [2] Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.	Keine Bemerkungen
5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen	
Art. 23 Persönlichkeitsverletzungen [1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. [2] Eine Persönlichkeitsverletzung liegt insbesondere vor: a. wenn Personendaten entgegen den Grundsätzen nach den Artikeln 4-6 und 11 bearbeitet werden; b. wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden; c. wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden; d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.	**Antrag zu Art. 23 Abs. 2 lit d)**: Streichung; zum Profiling vgl. Bemerkungen zu Art. 3 lit. f VE.

VE-DSG	Anträge und Bemerkungen
[3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	**Bemerkung zu Art. 23 Abs. 3**: Streichung des zweiten Teils „und eine Bearbeitung nicht ausdrücklich untersagt hat". Was einmal allgemein zugänglich gemacht worden ist, kann später nicht mehr widerrufen werden.
Art. 24 Rechtfertigungsgründe [1] Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. [2] Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere: a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet; b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben; c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn: 1. es sich dabei nicht um besonders schützenswerte Personendaten handelt, 2. Dritten nur Daten bekanntgegeben werden, welche diese für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen, 3. die betroffene Person volljährig ist; d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet; e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet, soweit: 1. die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt, 2. Dritten besonders schützenswerte Personendaten so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind, 3. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind; f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.	**Antrag I zu Art. 24 Abs. 2, erster Satz**: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit. **Antrag II zu Art. 24 Abs. 2. lit a)**: Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft Abgrenzungsfragen auf, für welche der VE keine Antworten liefert. **Antrag zu Art. 24 Abs. 2 lit. c) Ziff. 3**: Streichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar (Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft). Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit Sicherheit bestimmbar.
Art. 25 Rechtsansprüche [1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs. Die klagende Partei kann insbesondere verlangen, dass:	

VE-DSG	Anträge und Bemerkungen
a. die Datenbearbeitung verboten wird; b. die Bekanntgabe von Personendaten an Dritte untersagt wird; c. Personendaten berichtigt, gelöscht oder vernichtet werden. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die klagende Partei verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird. Sie kann darüber hinaus verlangen, dass die Bearbeitung der bestrittenen Daten eingeschränkt wird. [3] Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.	**Antrag Art. 25 lit. a) bis c)**: Es müsste klargestellt werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. Ansonsten kann die Bestimmung nicht umgesetzt werden. **Antrag Art. 25 Ziff. 2**: Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", *eventualiter* Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis schiefe Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat. **Antrag Art. 25 Ziff. 3**: Ziff. 3. streichen. Lit. a) bis c) reichen völlig, um die Interessen der Betroffenen zu wahren. Auch die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor.
6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane	
Art. 26 Verantwortliches Organ und Kontrolle [1] Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt. [2] Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.	Keine Bemerkungen
Art. 27 Rechtsgrundlagen [1] Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. [2] Für die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Eine Grundlage in einem Gesetz im materiellen Sinn ist ausreichend, wenn die folgenden Voraussetzungen erfüllt sind: a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn klar festgelegte Aufgabe unentbehrlich; und b. Die Bearbeitung birgt für die Persönlichkeit und die Grundrechte der betroffenen Person keine besonderen Risiken. [3] In Abweichung von den Absätzen 1 und 2 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Der Bundesrat bewilligt die Bearbeitung, sofern die Rechte der betroffenen Person nicht gefährdet sind; b. Die betroffene Person hat in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt;	**Antrag zu Art. 15 Abs. 2**: Streichen „oder den Erlass einer automatisierten Einzelfallentscheidungen nach Artikel Art. 15 Absatz 1" (vgl. dazu den Kommentar zu Art. 15 Abs. 2): Damit würde jede Prozessautomatisierung und -optimierung in der Verwaltung massiv erschwert. Es stellt sich grundsätzlich auch die Frage, ob als Grundlage für die Datenbearbeitung nicht auch Regelungen auf Verordnungsstufe ausreichen sollten.

VE-DSG	Anträge und Bemerkungen
c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.	
Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen [1] Der Bundesrat kann vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling bewilligen, wenn: a. die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz im formellen Sinn geregelt sind; b. ausreichende Massnahmen getroffen werden, um eine Verletzung der Grundrechte der betroffenen Person zu verhindern; und c. eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, zwingend erforderlich ist. [2] Er holt vorgängig die Stellungnahme des Beauftragten ein. [3] Das zuständige Bundesorgan legt dem Bundesrat spätestens innerhalb von zwei Jahren nach Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor. [4] Die automatisierte Datenbearbeitung oder das Profiling müssen in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage umfasst.	**Antrag zu Art. 28 Abs. 1 und 2**: Die Bestimmung ist entweder zu streichen, oder die entsprechenden Möglichkeiten ist auch Privaten zu eröffnen.
Art. 29 Bekanntgabe von Personendaten [1] Bundesorgane dürfen Personendaten bekannt geben, wenn eine Rechtsgrundlage im Sinne von Artikel 27 Absätze 1 und 2 dies vorsieht. [2] In Abweichung von Absatz 1 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten bekannt geben, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich; b. Die betroffene Person hat in die Bekanntgabe eingewilligt; c. Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; d. Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt; e. Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben, wenn: a. die betreffenden Daten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen; und b. an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. [4] Name, Vorname, Adresse und Geburtsdatum einer Person dürfen Bundesorgane auf Anfrage auch bekannt geben, wenn die Voraussetzungen von Absatz 1 oder 2 nicht erfüllt sind. [5] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 3 bekannt geben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst gelöscht. [6] Sie lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn: a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.	
Art. 30 Widerspruch gegen die Bekanntgabe von Personendaten [1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen. [2] Das Bundesorgan weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist: a. es besteht eine Rechtspflicht zur Bekanntgabe; b. die Erfüllung seiner Aufgabe wäre sonst gefährdet. [3] Artikel 29 Absatz 3 bleibt vorbehalten.	Keine Bemerkungen
Art. 31 Angebot von Unterlagen an das Bundesarchiv [1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998 bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen. [2] Sie vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese: a. anonymisiert sind; b. zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.	Keine Bemerkungen
Art. 32 Datenbearbeitung für Forschung, Planung und Statistik [1] Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn: a. die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt;	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
b. das Bundesorgan privaten Personen besonders schützenswerte Personendaten so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind; c. die Empfängerin oder der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und d. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. [2] Die Artikel 4 Absatz 3, 27 Absätze 1 und 2 sowie Artikel 29 Absatz 1 sind nicht anwendbar.	
Art. 33 Privatrechtliche Tätigkeit von Bundesorganen [1] Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen. [2] Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.	Keine Bemerkungen
Art. 34 Ansprüche und Verfahren [1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es: a. die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt; b. die Folgen einer widerrechtlichen Bearbeitung beseitigt; c. die Widerrechtlichkeit der Bearbeitung feststellt. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so muss das Bundesorgan bei den Daten einen Bestreitungsvermerk anbringen und deren Bearbeitung einschränken. [3] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan: a. die betreffenden Personendaten berichtigt, löscht oder vernichtet; b. seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, das Verbot der Bearbeitung, den Widerspruch gegen die Bekanntgabe nach Artikel 30 oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht. [4] Die Berichtigung, Löschung oder Vernichtung von Personendaten kann nicht verlangt werden in Bezug auf die Bestände öffentlich zugänglicher Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderer öffentlicher Gedächtnisinstitutionen. Wenn die Gesuchstellerin oder der Gesuchsteller ein überwiegendes Interesse nachweisen kann, kann sie oder er jedoch verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt. [5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.	Keine Bemerkungen
Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Öffentlichkeitsgesetzes hängig, so kann die betroffene Person im Rahmen dieses Verfahrens diejenigen Rechte geltend machen, die ihr nach Artikel 34 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.	Keine Bemerkungen
Art. 36 Register [1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [2] Der Beauftragte führt ein Register der Datenbearbeitungstätigkeiten. Das Register ist öffentlich.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.	
7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte	
Art. 37 Ernennung und Stellung [1] Die oder der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen. [2] Das Arbeitsverhältnis der oder des Beauftragten richtet sich, soweit dieses Gesetz nichts anderes vorsieht, nach dem Bundespersonalgesetz vom 24. März 2000 (BPG). [3] Die oder der Beauftragte übt ihre bzw. seine Funktion unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder zu erhalten. Sie oder er ist administrativ der Bundeskanzlei zugeordnet. [4] Sie oder er verfügt über ein ständiges Sekretariat und ein eigenes Budget. Sie oder er stellt sein Personal an. [5] Die oder der Beauftragte unterstehen nicht dem Beurteilungssystem nach Artikel 4 Absatz 3 BPG.	**Antrag zu Art. 37 Abs. 1**: Dem Bundesrat soll ein Vorschlagsrecht zukommen und die Wahl soll durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Amtsdauer von 4 Jahren gewählt". Was die blosse Genehmigung einer Wahl bringen soll, ist nicht ersichtlich. Die Person des Beauftragten soll über grosse Kompetenzen und einen Wirkungsgrad mit erheblichen finanziellen Auswirkungen auf die Schweizer Wirtschaft verfügen. In Anbetracht des zukünftigen, angedachten Gewichts dieses Posten, ist eine Wahl durch das Parlament gerechtfertigt. **Antrag zu Art. 37 Abs. 4**: Das Budget wird durch das Parlament genehmigt.
Art. 38 Wiederwahl und Beendigung der Amtsdauer [1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden. [2] Verfügt der Bundesrat nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl, so ist der oder die Beauftragte für eine neue Amtsdauer wiedergewählt. [3] Die oder der Beauftragte kann den Bundesrat unter Einhaltung einer Frist von sechs Monaten um Entlassung auf ein Monatsende ersuchen. [4] Der Bundesrat kann die Beauftragte oder den Beauftragten vor Ablauf der Amtsdauer des Amtes entheben, wenn diese oder dieser: a. vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder b. die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.	**Antrag zu Art. 38 Abs. 2**: Der oder die Beauftragte ist für jede Amtsperiode neu zu wählen. Das Verfahren über eine Verfügung kommt einem Kündigungsverfahren gleich, das in der Praxis nur aus wichtigen Gründen möglich ist. Das Wahlorgan soll in seiner Wahl wirklich frei sein.
Art. 39 Nebenbeschäftigung [1] Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, der Verwaltung, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein. [2] Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1 auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.	**Antrag zu Art. 39 Abs. 2**: Solche Bewilligungen von Nebenbeschäftigung sind offenzulegen. Für die Vermeidung von Interessenkonflikten ist absolute Transparenz unabdingbar.
Art. 40 Aufsicht	Keine Bemerkungen.

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte überwacht die Einhaltung der Datenschutzvorschriften des Bundes. [2] Bundesverwaltungsbehörden, die nach einem anderen Bundesgesetz Private oder Organisationen ausserhalb der Bundesverwaltung beaufsichtigen, laden den Beauftragten zur Stellungnahme ein, bevor sie eine Verfügung treffen, die Fragen des Datenschutzes berührt. [3] Führt der Beauftragte gegen die gleiche Partei ein eigenes Verfahren, so haben die beiden Behörden ihre Verfahren zu koordinieren.	
Art. 41 Untersuchung [1] Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.	
[2] Das Bundesorgan oder die private Person erteilt dem Beauftragten die von ihm verlangten Auskünfte und stellen ihm alle für die Untersuchung notwendigen Unterlagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes.	**Antrag zu Art. 41 Abs. 2**: Hier ist zu ergänzen, dass bei Untersuchungen gegen Private alle Untersuchungsakten nicht dem Öffentlichkeitsgesetz unterliegen, da ansonsten über diesen Umweg Betriebsgeheimnisse an Dritte gelangen könnten. Wenn Unternehmen verpflichtet sind, dem Beauftragten alle notwendigen Unterlagen zur Verfügung zu stellen, muss es die Garantie haben, dass diese nicht veröffentlicht werden. Der Beauftragte veröffentlicht bei Untersuchungen gegen private Personen nur die Empfehlung.
[3] Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte vergeblich versucht, Auskünfte und Unterlagen einzuholen, so kann der Beauftragte im Rahmen einer Untersuchung: a. ohne Vorankündigung Räumlichkeiten inspizieren; b. Zugang zu allen notwendigen Daten und Informationen verlangen.	**Antrag zur Art. 41 Abs. 3**: Diese Bestimmung ist nur akzeptabel, wenn das Unternehmen Rechtsmittel gegen die Auskunftsverfügung hat. Eine unbestimmte Verletzung von Mitwirkungspflichten darf nicht zu Strafsanktionen oder publizitätswirksamen Aktionen des Beauftragten gegen Unternehmen führen. Bevor solche Massnahmen ergriffen werden, muss eine Editionsverfügung des Beauftragten einer gerichtlichen Überprüfung zugänglich sein.
[4] Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten.	**Antrag zu Art. 41 Abs. 4**: Streichen „private Personen". Ein Tätigwerden des Beauftragten gegenüber Privaten ohne Anzeige einer Datenschutzverletzung ist strikt abzulehnen. Wenn Anhaltspunkte vorliegen, kann der Beauftragte nach Art. 41 Abs. 1 formell vorgehen. Es dürfen hier keine mehrgleisigen Verfahren ohne Rechtsschutz für die betroffenen Parteien eingefügt werden. Im Gegenteil, es müsste für Unternehmen möglich sein, Sachverhalte rechtsverbindlich durch den Beauftragten überprüfen und mittels Attest der Datenrechtskonformität genehmigen zu lassen.
[5] Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung.	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Parteistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte Abs. 5 auch gestrichen werden.
Art. 42 Vorsorgliche Massnahmen	

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern. [2] Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.	**Antrag zu Art. 42 Abs. 1**: Ändern: Der Beauftragte kann beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen. Vorsorgliche Massnahmen sind – auch im Persönlichkeitsschutz – immer Sache der Gerichte. Hier ist die bisherige Regelung mit dem Antrag beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts beizubehalten. Es sollte hier nicht von den bewährten rechtsstaatlichen Prozessen abgewichen werden. Jedenfalls gibt es dazu keine ausreichenden Rechtfertigungsgründe.
Art. 43 Verwaltungsmassnahmen [1] Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden. [2] Der Beauftragte kann zudem die Bekanntgabe ins Ausland aufschieben oder untersagen, wenn sie gegen die Voraussetzungen nach Artikel 5 oder 6 oder gegen spezifische Bestimmungen betreffend die Bekanntgabe von Personendaten ins Ausland in anderen Bundesgesetzen, verstösst.	**Antrag zu Art 43 Abs. 1**: Ändern: Anstelle der Empfehlung und des nachfolgenden Gerichtswegs wie im heutigen Recht wird hier auch die Klage- und Beweislast umgekehrt. Das ist abzulehnen. Der Beauftragte hat in der Verfügung die Rechtsverletzung nachzuweisen. Eine Verfügung sollte nur nach der Durchführung einer Untersuchung zulässig sein, in welchem dem betroffenen Datenbearbeiter selbstverständlich auch das rechtliche Gehör gewährt wurde. Eine Datenvernichtung darf nicht durch den Beauftragten angeordnet werden können, da dies nicht wieder gutzumachende Folgen hat (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 41 reicht zum Schutz Betroffener völlig aus.
Art. 44 Verfahren [1] Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz. [2] Partei sind lediglich das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wurde. [3] Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt keine aufschiebende Wirkung zu.	**Antrag zu Art. 44 Abs. 2**: Drittpersonen haben keine Parteistellung und kein Akteneinsichtsrecht, was zu begrüssen ist. Zu ergänzen ist weiter, dass Untersuchungsunterlagen nicht dem Öffentlichkeitsgesetz unterliegen dürfen. **Antrag zu Art. 44 Abs. 3**: Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Vielmehr wäre vorzusehen, dass die aufschiebende

VE-DSG	Anträge und Bemerkungen
[4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.	Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt nicht praktikable Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Art. 45 Anzeigepflicht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.	**Antrag zu Art. 45**: Streichen. Ein Recht zur Anzeige würde völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE).
Art. 46 Amtshilfe zwischen schweizerischen Behörden [1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses Gesetzes erforderlich sind. [2] Der Beauftragte gibt den folgenden Behörden die Informationen und Personendaten bekannt, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind: a. den für den Datenschutz zuständigen kantonalen Behörden; b. den zuständigen Strafverfolgungsbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 45 geht; c. den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss Artikel 41 Absatz 3, 42 und 43.	**Antrag zu Art. 46 Abs. 2**: Hier ist zu ergänzen, dass Informationen die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen.
Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden [1] Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen: a. die Identität des Verantwortlichen, des Auftragsbearbeiters oder anderer beteiligter Dritter; b. Kategorien von betroffenen Personen; c. die Identität der betroffenen Personen, falls: 1. die betroffenen Personen eingewilligt haben, oder 2. die Mitteilung der Identität der betroffenen Personen unumgänglich ist, um die gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde zu erfüllen; d. bearbeitete Personendaten oder Kategorien von bearbeiteten Personendaten; e. den Zweck der Datenbearbeitung; f. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern; g. technische und organisatorische Massnahmen. [2] Der Beauftragte kann der ausländischen Behörde Amtshilfe gewähren und ihr die Informationen gemäss Absatz 1 zur Verfügung stellen, wenn sie folgende Voraussetzungen erfüllt: a. Sie verpflichtet sich, die zur Verfügung gestellten Informationen und Personendaten, nicht für andere Zwecke zu verwenden, als im Amtshilfegesuch angegeben; b. Sie verpflichtet sich, ähnlichen Amtshilfegesuchen der Schweiz Folge zu leisten;	**Antrag zu Art. 47 Abs. 1**: Auch hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen, insbesondere auch für Informationen, die in der Schweiz dem Berufsgeheimnis unterliegen. Die Herausgabe vertraulicher Unternehmensdaten darf nicht im Ermessen des Beauftragten liegen, sondern – wenn überhaupt – nur mit Zustimmung des betroffenen Unternehmens zulässig sein.

VE-DSG	Anträge und Bemerkungen
c. Sie verpflichtet sich zur Wahrung des Amts- und Berufsgeheimnisses; d. Sie verpflichtet sich, die erhaltenen Informationen und Personendaten nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln; e. Sie verpflichtet sich, die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten.	
Art. 48 Information [1] Der Beauftragte erstattet der Bundesversammlung periodisch sowie bei Bedarf Bericht. Er übermittelt den Bericht gleichzeitig dem Bundesrat. Die periodischen Berichte werden veröffentlicht. [2] In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über seine Feststellungen und Verfügungen.	**Antrag zu Art. 48 Abs. 2**: Streichen des Begriffs „seine Feststellungen und Verfügungen" und ersetzen mit „seine Untersuchungen". Damit der Beauftragte die Persönlichkeitsrechte wahrt, soll er nur über die Tatsache einer Untersuchung informieren. Es ist nicht ersichtlich, weshalb der Beauftragte zur Profilierung von Amt und Person ein öffentliches Prangerrecht haben soll.
Art. 49 Weitere Aufgaben Der Beauftragte nimmt darüber hinaus insbesondere folgende Aufgaben wahr: a. Er informiert und berät die Organe des Bundes und der Kantone sowie private Personen bei Fragen des Datenschutzes. b. Er arbeitet mit schweizerischen und ausländischen Behörden, die für den Datenschutz zuständig sind, zusammen. c. Er sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz. d. Er erteilt der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann. e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen. f. Er nimmt die ihm durch das Öffentlichkeitsgesetz übertragenen Aufgaben wahr.	**Antrag zu Art. 49 lit. d**: Streichen. Wenn der Datenschutzbeauftragte eine Aufsichtsfunktion hat, kann er nicht gleichzeitig auch eine Konsumentenschutzaufgabe erfüllen dürfen.
8. Abschnitt: Strafbestimmungen	**Antrag zum 8. Abschnitt (Art. 50ff)**: Das gesamte Sanktionssystem ist zu überarbeiten. Es führt zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden und Unternehmen. Unverständlich ist zudem, dass gerade die Verwaltung von den Strafsanktionen ausgenommen werden soll. Es wird komplett vergessen und ausgeblendet, dass vor noch nicht langer Zeit, die Gefahr im Umgang mit Daten nicht von Privaten und nicht von Unternehmen, sondern vom Staat selbst ausgegangen ist (Stichwort: Fichen-Affäre). Es wäre naiv zu glauben, dass sich diese Bedrohung in den letzten 20 Jahren komplett verflüchtigt hätte. Mit einer zunehmend

VE-DSG	Anträge und Bemerkungen
	hohen Verwaltungsquote von gegen 40% wäre ein sehr hoher Anteil der Berufstätigen vom Sanktionssystem ausgenommen. Das ist höchst zweifelhaft und politisch nicht zu rechtfertigen. Alternative: Der Beauftragte soll als Aufsichtsbehörde untersuchen und verfügen können. Unternehmen sollen sich in diesem verwaltungsrechtlichen Verfahren wehren können. Erst wenn rechtskräftige Entscheide nicht umgesetzt worden sind, sollten Strafsanktionen greifen. Es besteht kein Rechtfertigungsgrund, von diesem in anderen Belangen des Bundesrechts verankerten Prinzip abzuweichen.
Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten [1] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft: a. die ihre Pflichten nach den Artikeln 13, 15 und 20 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;	**Antrag zu Art. 50**: Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen. Der Bussenrahmen ist auf eine maximale Höhe von CHF 5'000.- bzw. – im Wiederholungsfall – auf maximal CHF 10'000.- zu begrenzen. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen anzusetzen, sicher nicht Beträge bis CHF 500'000.-. Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.- für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Grössenordnungen. Bussenbeträge über CHF 100'000.- sind bislang in der Schweiz nicht bekannt. Die Erhöhung des Strafrahmens auf CHF 500'000.- ist daher völlig überrissen und nicht nachvollziehbar.
b. die es vorsätzlich unterlassen: 1. die betroffene Person nach Artikel 13 Absätze 1 und 5, 15 und 17 Absatz 2 die betroffene Person zu informieren; oder 2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2, 3 und 4 zu liefern.	**Antrag zu Art. 50 Abs. 1 lit. b)**: Ändern. Art 13 ist vollständig von der Sanktionierung auszunehmen.
c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3).	**Antrag zu Art. 50 Abs. 1 lit. c)**: Streichen. Ist vollständig von der Sanktionierung auszunehmen.
[2] Mit Busse bis zu 500 000 Franken werden private Personen bestraft, wer vorsätzlich: a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b und Absatz 6 zu informieren; b. die es unterlassen, dem Beauftragten die standardisierten Garantien oder die verbindlichen unternehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d Ziff. 1);	**Antrag zu Art. 50 Abs. 2, lit. a) und b)**: Streichen. Da die Meldepflicht sowieso massiv reduziert werden müssen, ist auch diese Bestimmung zu streichen.

VE-DSG	Anträge und Bemerkungen
c. dem Beauftragten bei der Untersuchung (Art. 41 Abs. 2) falsche Auskünfte erteilen oder die Mitwirkung verweigern; e. es unterlassen, dem Beauftragten Verletzungen des Datenschutzes nach Artikel 17 Absatz 1 zu melden; f. einer Verfügung des Beauftragten nicht Folge leistet. [3] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft, die es vorsätzlich unterlassen: a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren; b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 zu informieren. [4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**Antrag zu Art. 50 Abs. 2, lit. e)**: Ändern. Diese Bestimmung ist auf Vorfälle zu beschränken, die schwerwiegend sind und mehr als 1'000 Personen betreffen. **Antrag zu Art. 50 Abs. 2, lit. f**: Streichen. Hier genügt die bestehende Strafbestimmung im StGB. **Antrag zu Art. 50 Abs. 3, lit. a)**: Streichen. Die dem Bst. a) zugrundeliegende Bestimmung ist Art. 19 Bst. b) ist in der Praxis gar nicht umsetzbar. Daher ist auch die Strafbestimmung zu streichen. **Antrag zu Art. 50 Abs. 4**: Streichen. Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen.
Art. 51 Verletzung der Sorgfaltspflichten [1] Mit Busse bis zu 500'000 Franken werden private Personen auf **Antrag** bestraft, die vorsätzlich: a. unter Verstoss gegen Artikel 5 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln; b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 7 Absätze 1 und 2 erfüllt sind; c. es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder Verlust zu schützen (Art. 11); d. es unterlassen, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16); e. es unterlassen, die Vorkehren nach Artikel 18 zu treffen; f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert.	**Antrag zu Art. 51 Abs. 1**: Bei Vorsatz sind Bussen bis CHF 10'000.- angemessen. **Antrag zu Art. 51 Abs. 1 lit. a)**: Die Meldepflicht von Art. 6 Abs. 2 ist von der Busse auszunehmen, da ansonsten tausende von KMU unwissentlich kriminalisiert werden. **Antrag zu Art. 51 Abs. 1 lit. d)**: Streichen; erst die Folgeabschätzung kann ja zeigen, ob eine Folgeabschätzung notwendig wäre. Die Strafdrohung führt dazu, dass dieses Verfahren für jede Datenbearbeitung durchgeführt werden muss. In der Rechtsfolgeabschätzung werden Kosten von CHF 5'000 – 30'000.- pro Durchführung veranschlagt, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU führen würde. **Antrag zu Art. 51 Abs. 1 lit. e)**: Streichen; Hier handelt es sich um eine unbestimmte Handlungsdefinition, die dadurch kaum eine Strafbarkeit auslösen kann. **Antrag zu Art. 51 Abs. 1 lit. f)**: Streichen; die Strafdrohung führt dazu, dass alle Prozesse für die Datenbearbeitung vorsorglich dokumentiert werden müs-

VE-DSG	Anträge und Bemerkungen
[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	sen, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU, führen würde. In der RFA wurden diese Kosten nicht erhoben. **Antrag zu Art. 51 Abs. 2**: Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen.
Art. 52 Verletzung der beruflichen Schweigepflicht [1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf **Antrag** bestraft, wer vorsätzlich geheime Personendaten bekannt gibt: a. von denen er im Rahmen seiner beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat; b. welche er selbst zu kommerziellen Zwecken bearbeitet hat. [2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er bei der Tätigkeit für einen Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat. [3] Das Bekanntgeben geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.	**Antrag zu Art. 52**: Streichen; der bisherige Art. 35 DSG hat die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten geregelt. Die Ausweitung auf den unbestimmten Begriff „geheime Personendaten" wird abgelehnt. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Damit würde jeder Bearbeiter von Personendaten einer strafbewehrten Schweigepflicht unterworfen. Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist völlig unverhältnismässig. *Eventualiter* wäre es sinnvoller, die Strafbarkeit in dieser Bestimmung auf Auftragsbearbeiter und Beauftragte zu beschränken.
Art. 53 Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.	**Antrag zu Art. 53**: Streichen; die bestehenden Regelungen im Verwaltungsstrafrecht und im Strafrecht sind ausreichend.
Art. 54 Anwendbares Recht und Verfahren Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.	**Antrag zu Art. 54**: Streichen; die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet werden und ist somit vom Bund zu führen.
Art. 55 Verfolgungsverjährung für Übertretungen Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.	**Antrag zu Art 55**: Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109) und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
9. Abschnitt: Abschluss von Staatsverträgen	
Art. 56 Der Bundesrat kann Staatsverträge abschliessen betreffend: a. die internationale Zusammenarbeit zwischen Datenschutzbehörden; b. die gegenseitige Anerkennung eines angemessenen Schutzes für die Bekanntgabe von Personendaten ins Ausland.	Titel fehlt zum Artikel fehlt.
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unterstehen den Artikeln 1-22, 26, 27, 29 bis 32, 34 Absätze 1-3 und 36 dieses Gesetzes, soweit sie nicht kantonalen Datenschutzvorschriften unterstehen, die einen angemessenen Schutz der Daten gewährleisten. [2] Die Kantone bestimmen ein Organ, das die Einhaltung der Datenschutzvorschriften überwacht. Die Artikel 41-43, 48 und 49 gelten sinngemäss.	
Art. 58 Aufhebung und Änderung anderer Erlasse Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.	Keine Bemerkungen
Art. 59 Übergangsbestimmung Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die für Verantwortlichen sowie der Auftragsbearbeiter in der Lage sein: a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen; b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.	**Antrag zu Art. 59**: Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, die nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken ist.
Art. 60 Referendum und Inkrafttreten [1] Dieses Gesetz untersteht dem fakultativen Referendum. [2] Der Bundesrat bestimmt das Inkrafttreten.	Keine Bemerkungen

Sammlung Änderungsvorschläge: Aufhebung und Änderung anderer Erlasse

VE-DSG	Anträge und Bemerkungen
11. Zivilprozessordnung *Art. 20 Bst. d* Für die folgenden Klagen und Begehren ist das Gericht am Wohnsitz oder Sitz einer der Parteien zuständig: d. Klagen und Begehren nach dem Datenschutzgesetz vom … *Art. 99 Abs. 3 Bst. d* [3] Keine Sicherheit ist zu leisten: d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom…. *Art. 113 Abs. 2 Bst. g* [2] Keine Gerichtskosten werden gesprochen in Streitigkeiten:	**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Da in Datenschutzfragen der Beauftragte eine Aufsichtsfunktion ausübt, kann er bei Verstössen aktiv werden. Es braucht hier keine weitere soziale Gerichtsbarkeit. Für zivilrechtliche Verfahren genügen die bestehenden Regeln. Das kostenlose Prozessieren könnte hier eine Flut – auch von mutwilligen – Klagen auslösen. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll – wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist – seine Kostenrisiken abwägen müssen, ehe Gerichte bemüht werden.

VE-DSG	Anträge und Bemerkungen
g. nach dem Datenschutzgesetz vom …… *Art. 114 Bst. f* Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom …… *Art. 243 Abs. 2 Bst. d* [2] Es gilt ohne Rücksicht auf den Streitwert für Streitigkeiten: d. zur Durchsetzung der Ansprüche nach den Artikeln 12 und 20 des Datenschutzgesetzes vom …	

VE-DSG	Anträge und Bemerkungen
13. Strafgesetzbuch *Art. 179novies* Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. *Art. 179decies* Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.	**Antrag zu Art. 179novies**: Die Strafbarkeit der Beschaffung ist zu beschränken auf Daten die einem Berufsgeheimnis unterliegen sowie auf besonders schützenswerte Personendaten. Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe zu bestrafen ist unverhältnismässig. Hier reicht eine Geldstrafe.
37. Fernmeldegesetz vom 30. April 1997 *Art. 13a Abs. 1 erster Satz* 1 Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, bearbeiten, sofern dies für die Erfüllung der ihnen durch die Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. ... *Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz* 1 ... Zu diesen Daten gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten. 2 Unter Vorbehalt anders lautender internationaler Vereinbarungen dürfen die Kommission und das Bundesamt ausländischen Aufsichtsbehörden im Fernmeldebereich Daten, einschliesslich in Verwaltungs- oder Verwaltungsstrafverfahren beschaffter besonders schützenswerter Personendaten, nur übermitteln, sofern diese Behörden: 4 Schweizerische Behörden geben der Kommission und dem Bundesamt kostenlos diejenigen Daten weiter, die für die Durchsetzung der Fernmeldegesetzgebung von Bedeutung sein können, einschliesslich besonders schützenswerter Personendaten. ...	**Bemerkung zu datenschutzrechtlichen Regulierungen im Fernmeldegesetz**: Es ist klarzustellen, dass datenschutzrechtliche Regulierungen im Fernmeldegesetz und in dessen Ausführungsbestimmungen als *lex specialis* den allgemeinen Datenschutzbestimmungen des DSG und dessen Ausführungsbestimmungen vorgehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

von Holzen Philipp
Technischer Leiter

von Holzen René
Adimistrativer Leiter

Amstutz Jonas BJ

Von: Cornelia Aschmann <info@aschmann.com> im Auftrag von Cornelia Aschmann - Geschäftsstelle Textverband <kontakt@textverband.ch>
Gesendet: Donnerstag, 30. März 2017 11:08
An: Amstutz Jonas BJ
Betreff: Stellungnahme des Textverbands zum Vorentwurf für das total revidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Der Textverband ist der Berufsverband der Texterinnen und Texter in der Schweiz. Fast hundert Mitglieder zählt der bereits 1982 gegründete Verband, der dem zentralen Dachverband KS/CS Kommunikation Schweiz angeschlossen ist.

Der Verband engagiert sich für seine Mitglieder, die wertvolle Textarbeit liefern für die gesamte Schweizer Wirtschaft, und fördert die qualitativ und fachlich hochstehende, von hoher Berufsethik geprägte wirtschaftliche Tätigkeit seiner Mitglieder.

Wir befürchten, die Auflagen, die in diesem Gesetz geregelt werden, verklompiziere die zukünftige Verbandsarbeit unnötig. Insbesondere was das Führen von Datenbanken mit Adressen und der damit einhergehenden neuen Verantwortlichkeit anbelangt.

Auch das Strafenszenario dünkt uns wenig förderlich, das zumeist ehrenamtliche Übernehmen von Engagements in Vereinen und Verbänden weiter zu fördern. Das betrifft alle Vereine, nicht nur den Textverband.

Vereine und Verbände sind der Kitt des schweizerischen Wirtschafts- und Sozialgefüges. Diese Verbindungsfunktion sehen wir durch das total revidierte Datenschutzgesetz für die Zukunft gefährdet. Wir danken Ihnen, wenn Sie bei der Totalrevision des Datenschutzgesetzes Verbände, insbesondere von solchen der Werbewirtschaft, und deren Anliegen speziell berücksichtigen.

Freundliche Grüsse

Präsidentin und Geschäftsführerin Textverband

Odile Nerfin Cornelia Aschmann

TEXTVERBAND

Berufsverband der Texterinnen und Texter in der Schweiz
Geschäftsstelle Bachtobelstrasse 53 8045 Zürich
kontakt@textverband.ch http://textverband.ch

TvT Services SA

p.a. SIE SA
Chemin de la Gottrause 11
Case postale 71
CH 1023 Crissier

Tél. 021 631 51 20
Fax 021 634 77 47
info@tvtservices.ch
www.tvtservices.ch

CHE-105.144.658
IBAN CH27 0900 0000 1000 8057 4

Département Fédéral de Justice et Police
Madame la Conseillère fédérale
Simonetta Sommaruga
Bundesrain 20
3003 Berne

Votre référence :
Notre référence : AY/chc
Affaire traitée par : J.-D. Ayer
Téléphone direct : 021 631 55 19

Crissier, le 3 avril 2017

Prise de position sur l'avant-projet de loi au sujet de la révision totale de la loi sur la protection des données (AP-LPD)

Madame la Conseillère fédérale,

Nous vous remercions de nous avoir associé à la consultation citée en titre.

Pour notre société, active dans le déploiement d'infrastructures de télécommunication et de services associés, les enjeux liés à ce sujet sont très importants. Pour cette raison, nous y répondons comme suit :

TvT Services SA est en tout point du même avis que celui exprimé par notre association faîtière SUISSEDIGITAL, association des réseaux de communication, Kramgasse 5, CP 515, 3000 Berne 8, à votre attention, sur ce même objet.

En vous remerciant de l'attention que vous porterez à la présente, nous vous adressons, Madame la Conseillère fédérale, l'expression de nos sentiments distingués.

TvT Services SA

J.- D. Ayer

Th. Huguenin

Amstutz Jonas BJ

Von: thomas.bischof@ubs.com
Gesendet: Dienstag, 4. April 2017 19:22
An: Amstutz Jonas BJ
Cc: juerg.schaer@ubs.com; thomas.bischof@ubs.com
Betreff: 20170404 Totalrevision-des-Datenschutzgesetzes_UBS-Stellungnahme_FINAL
Anlagen: 20170404 Totalrevision-des-Datenschutzgesetzes_UBS-Stellungnahme_FINAL.doc; Legal Disclaimer.txt

Sehr geehrter Herr Amstutz

Wir beziehen uns auf die **Vernehmlassung zum VE-DSG** und lassen Ihnen anbei die Stellungnahme der UBS zukommen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Beste Grüsse
Thomas Bischof & Jürg Schär

UBS AG
Head Legislative & Regulatory Initiatives CH
Talacker 30, P.O. Box, CH-8098 Zurich, Switzerland

Tel. +41-44-234 20 76
Fax. +41-44-234 32 45
E-mail thomas.bischof@ubs.com

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : UBS AG

Abkürzung der Firma / Organisation : -

Adresse : Postfach, 8098 Zürich

Kontaktperson : Dr. Thomas Bischof und Jürg Schär

Telefon : +41-44-234 20 76/+41-44-234 87 61

E-Mail : thomas.bischof@ubs.com/juerg.schaer@ubs.com

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
UBS AG	Datenschutz spielt im Wirtschaftsleben mittlerweile eine zentrale Rolle. Die geltenden gesetzlichen Grundlagen werden sodann den aktuellen Gegebenheiten und auch den internationalen Anforderungen an ein adäquates Datenschutzrecht nicht mehr gerecht. Eine Modernisierung des schweizerischen Datenschutzes auch unter Berücksichtigung der internationalen Vorgaben erscheint uns daher angezeigt. In diesem Sinne **unterstützen wir eine massvolle Revision** des schweizerischen Datenschutzgesetzes (DSG).
UBS AG	Wichtig erscheint es uns, dass die richtige Balance zwischen dem Schutz der betroffenen Person und der Wettbewerbsfähigkeit des Wirtschaftsstandortes gefunden wird. Das bedeutet, dass das DSG so revidiert werden soll, dass es einem Äquivalenztest gegenüber der EU Datenschutzgrundverordnung standhält, aber nicht über diesen Standard hinausgeht. **Einen sog. "Swiss Finish" gegenüber der EU lehnen wir ab**. Zusätzliche oder darüber hinausgehende Anforderungen an die Datenbearbeitung gegenüber der EU Regelung wäre nicht verhältnismässig, weil damit die Datenbearbeiter (Verantwortliche, wie auch Auftragsbearbeiter) in der Schweiz ohne sachlichen Grund einem Wettbewerbsnachteil ausgesetzt würden.
UBS AG	Im Gegenteil, wo immer möglich, **sollte zusätzliche Bürokratie verhindert werden**, wie dies teilweise im EU Regelwerk vorgesehen ist. Dabei gilt es den Schutzzweck des DSG ins Zentrum zu stellen und nur dort, wo die Persönlichkeitsrechte der betroffenen Person berührt sind, zu regulieren. Es ist z.B. nicht zielführend, wenn die betroffene Person mit möglichst vielen und umfassenden Informationen versorgt wird. Dies führt nur dazu, dass sie in der allgemeinen Informationsflut die für sie tatsächlich relevanten Informationen nicht mehr erkennen kann. Stattdessen gilt es, die betroffene Person mit gezielten Informationen in die Lage zu versetzen, sich ein angemessenes Bild über die vorgenommene Datenbearbeitung und deren Auswirkung auf ihre Persönlichkeitsrechte machen zu können.
UBS AG	Dasselbe gilt im Verhältnis zwischen dem Datenbearbeiter/dem Datenverantwortlichen und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Es ist nicht sinnvoll und nicht mehr verhältnismässig, wenn für jeden denkbaren Fall eine Meldepflicht vorgesehen wird. Auch in Anbetracht der Ressourcen des EDÖB ist fraglich, wie er mit einer solchen Flut von Daten und Informationen umgehen soll. Er könnte seine Funktion wohl kaum mehr wahrnehmen und das Regulierungsziel würde damit ernsthaft gefährdet. Vielmehr erscheint es angebracht, die **Meldepflichten auf wirklich bedeutende Fälle zu beschränken**, in welchen ein Einschreiten des EDÖB angezeigt sein kann.
UBS AG	Der Gesetzesentwurf (Vorentwurf DSG, "VE DSG") sieht demgegenüber sehr viele Informations- und Meldepflichten vor, die teilweise über den

	Standard der EU Datenschutzgrundverordnung ("DSGVO") hinausgehen. Wir plädieren deshalb im Sinne der effektiven Umsetzung des Schutzzweckes des DSG für pragmatische Lösungen, welche den betroffenen Personen einen effektiven Schutz bieten und praxistauglich sind.
UBS AG	Es ist zu verhindern, dass unter dem Titel Datenschutz **Hürden für neue Technologien** errichtet werden. Die Regelung im Datenschutzgesetz soll in diesem Sinne technologieneutral erfolgen. Solche Hürden wären gerade bei Vorschriften über das **Profiling** zu befürchten. Meist sind es die betroffenen Personen in ihrer Eigenschaft als Kunden, welche solche neuen Dienstleistungen nachfragen und davon auch profitieren. Die Wettbewerbsfähigkeit des Wirtschafts- und Technologiestandortes Schweiz gilt es auch im Bereich des Datenschutzes zu sichern und zu fördern.
UBS AG	Wir lehnen die neuen, zusätzlichen **Strafbestimmungen ab**. Mit der vorgeschlagenen Lösung geraten insbesondere die Mitarbeiter von Datenbearbeitern in den Fokus der Strafverfolgung und zwar für Taten, deren Unrechtsgehalt eine strafrechtliche Sanktion in keiner Weise rechtfertigt. Es ist völlig unverhältnismässig, wenn bei Normalen, alltäglichen beruflichen Tätigkeiten schon eine kleine Nachlässigkeit mit strafrechtlichen Konsequenzen versehen wird. In Fällen, in denen die Persönlichkeit in strafwürdiger Weise verletzt wird, bestehen bereits Strafbestimmungen (z.B. Berufsgeheimnispflichten, Ehrverletzungsdelikte etc.). Völlig unverhältnismässig erachten wir die Strafbarkeit von Mitarbeitern bei fahrlässiger Begehung. Damit wird jeglicher Umgang mit Personendaten potentiell strafrechtlich relevant, was auch normale Arbeitsprozesse im Arbeitsalltag massiv erschweren würde. Das Parlament hat dies schon länger erkannt und in jüngsten Gesetzesvorschlägen fahrlässige Strafrechtstatbestände gestrichen und der "Verstrafrechtlichung" des heute normalen und üblichen Geschäftsalltags klare Grenzen gesetzt. Soweit unter dem Gesichtspunkt der Äquivalenz mit der EU der Datenschutzgesetzgebung in der EU ein Sanktionensystem erforderlich wäre, könnte anstelle der vorgeschlagenen Strafsanktionen ein System von Verwaltungssanktionen vorgesehen werden.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
UBS AG	VE-DSG	1			**Begründung** Die Bearbeitung von Personendaten ist eine elementare Voraussetzung für eine erfolgreiche Digitalisierung der schweizerischen Wirtschaft und Gesellschaft. Es ist deshalb zentral, dass das revidierte Schweizerische Datenschutzgesetz auch gesamtwirtschaftliche und gesellschaftliche Interessen bei der Bearbeitung von Personendaten berücksichtigt und dies im Zweckartikel zum Ausdruck kommt. Die diesem zusätzlichen Ziel entsprechende Berücksichtigung gesamtwirtschaftlicher Interessen stünde auch im Einklang mit der Strategie des Bundesrates für eine digitale Schweiz. Danach soll die Schweiz „Chancen der Digitalisierung in allen Lebensbereichen konsequent nutzen“, von der „zunehmenden Digitalisierung profitieren“, sich „als innovative Volkswirtschaft noch dynamischer entwickeln“ und die „Wirtschaft soll sich im digitalen Raum möglichst frei entfalten können“ (vgl. Medienmitteilung vom 20.04.2016 zur Strategie des Bundesrates für eine digitale Schweiz). Wir erachten es auch nicht unbedingt als zutreffend, in diesem Zusammenhang vom Schutz „der Grundrechte“ von natürlichen Personen zu sprechen. Das mag zwar der Regelung in der DSGVO entsprechen. Das europäische Recht kennt eine direkte Drittwirkung der Grundrechte, die dem schweizerischen Recht in dieser Form jedoch fremd ist. Es ist nicht Aufgabe privater Datenbearbeiter, die Grundrechte betroffener Personen zu schützen, soweit diese Grundrechte nicht in den einzelnen Anforderungen des DSG Ausdruck gefunden haben. **Formulierungsvorschlag** Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden und die Förderung der Rahmenbedingungen der digitalen Wirtschaft.

UBS AG	VE-DSG	2	2	a	**Begründung** Es soll klargestellt werden, dass die Ausnahme des Privat- bzw. Familienbereichs am Zweck der Datenbearbeitung und nicht an der Art oder dem Umfang der Bearbeitung anknüpft. Insbesondere kann es nicht darauf ankommen, ob die Daten in physischer Form oder elektronischer Form erstellt und aufbewahrt werden. Auch sollte in der Botschaft klargestellt werden, dass die Ausnahme technologieneutral zu verstehen ist und sich an der privaten Zwecksetzung nichts ändert, wenn beispielsweise Cloud-Lösungen verwendet oder Daten ausserhalb eines eng verstandenen persönlichen Bereichs gespeichert werden (z.B. im „privaten / persönlichen" Ordner im Netzwerk eines Arbeitgebers). Deshalb ist die Anknüpfung des Ausschlussgrundes am Merkmal der Bearbeitung (Zugriffe) durch Aussenstehende nicht mehr sachgerecht. Richtigerweise muss sich dieser am Willen des Erstellers orientieren. Legt ein Mitarbeiter eine persönliche Notiz in seinem „privaten/persönlichen" Ordner im Netzwerk seines Arbeitgebers ab, müsste diese von der Anwendung des Datenschutzgesetzes ausgeschlossen werden, auch wenn bspw. der technische Support oder ein Arbeitskollege die **Möglichkeit** hätte, darauf zuzugreifen. Diese Auffassung sollte in der Botschaft zum Ausdruck kommen. **Formulierungsvorschlag** [2] Es ist nicht anwendbar auf: a. Personendaten, die durch eine natürliche Person ausschliesslich zum Zweck des persönlichen Gebrauchs bearbeitet werden;
UBS AG	VE-DSG	2	2	e	**Begründung** Sobald Gerichtsverfahren anhängig sind, stellen die anwendbaren Verfahrensregeln sicher, dass die Persönlichkeitsrechte der Parteien gewahrt werden. Die Ausweitung der Anwendbarkeit des Datenschutzgesetzes auf hängige Gerichtsverfahren für Parteien (nicht jedoch für Gerichte) ist **unnötig und unverhältnismässig**. Das hätte zur Folge, dass während hängiger Verfahren das Auskunftsrecht zur (datenschutzrechtlich nicht vorgesehenen) Beweisbeschaffung zweckentfremdet werden könnte: einerseits ist es kostenlos, andererseits können die (hohen) Hürden der ZPO (bspw. für Editionsbegehren) umgangen werden. Damit würde dem **Missbrauch des Auskunftsgesuchs** Tür und Tor geöffnet. Es bedarf daher

					einer Anpassung (vgl. Kommentar zu Art. 20). Sollte diese bisher in Art. 2 Abs. 2 lit. c vorgesehene Nichtanwendbarkeit des DSG entgegen unserer Anregung nicht beibehalten werden, so sind mögliche Konflikte mit den relevanten Prozessordnungen (ZPO, StPO und auch – insbesondere für Kartellverfahren relevant – VwVG) durch entsprechende Ausnahmebestimmungen im neuen DSG zu lösen. Das Auskunftsrecht Dritter darf den an Zivilprozessen oder Verwaltungs-, Kartell- oder Strafverfahren beteiligten Unternehmen nicht zum Nachteil reichen. Gerade auch aufgrund solcher übergeordneter Interessen sollte beim Auskunftsrecht klargestellt werden, dass neu tatsächlich keine Ausdrucke bzw. Kopien ausgehändigt werden und zudem eine Verwendungsbeschränkung auf die Geltendmachung von Ansprüchen aus Datenschutzrecht gelten soll (vgl. Kommentar zu Art. 20). **Formulierungsvorschlag** [2] Es ist nicht anwendbar auf: *e.* hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren;
UBS AG	VE-DSG	3	1	c	**Begründung** Der Wortlaut des Gesetzes widerspricht den Erläuterungen im Begleitbericht. Gemäss Wortlaut wäre jedes Gesichtsfoto ein besonders schützenswertes Personendatum. Bilder in der Zeitung, auf welchen Personen erkennbar sind, wären damit besonders schützenswerte Personendaten. Dies ist abzulehnen. Der erläuternde Bericht sieht hingegen vor, dass nur diejenigen biometrischen Daten als besonders schützenswerte Personendaten qualifiziert werden sollen, die (mit besonderen technischen Mitteln) *zum Zweck bearbeitet werden*, eine natürliche Person eindeutig zu identifizieren. Im Übrigen entspricht dies auch der Auffassung der Konvention 108. **Formulierungsvorschlag** 4. biometrische Daten, die mit besonderen technischen Mitteln zum Zweck der Personenidentifikation bearbeitet werden ~~, eine natürliche Person eindeutig identifizieren~~

UBS AG	VE-DSG	3		f	**Begründung** Die Definition von „**Profiling" ist zu breit** und geht weit über die Definition von „Profiling" in der DSGVO hinaus: Bereits eine „von Hand" bearbeitete Mitarbeiterbeurteilung würde als "Profiling" nach Art. 23 Abs. 2 Bst. d und damit per se als Persönlichkeitsverletzung gelten. Konsequenterweise müsste ein Verantwortlicher vor jeder Bearbeitung einen Rechtfertigungsgrund ausweisen können, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden wäre. Dies stellt einen Paradigmenwechsel im schweizerischen Datenschutzrecht dar, für den es keine Rechtfertigung gibt. Warum eine im Geschäftsverkehr übliche Auswertung von Personendaten spezielle Schutzanforderungen erfordern soll, ist unseres Erachtens nicht schlüssig dargelegt. Solange Transparenz über die Bearbeitung besteht, sollten keine weitergehenden Voraussetzungen an die Auswertung der Personendaten gestellt werden. Wir beantragen daher, den **Begriff des Profiling zu streichen** (vgl. auch unten Art. 4 Abs. 6). Die automatisierte Einzelentscheidung, welche im Wesentlichen dem Profiling der DSGVO entspricht, wird sodann bereits in Art. 15 geregelt. Auf jeden Fall, d.h. wenn am Begriff des Profilings festgehalten werden soll, sollte er sich aber auf die Bearbeitung von besonders schützenswerte Personendaten beschränken und nur die maschinelle Bewertung dieser Daten umfassen. **Formulierungsvorschlag** ~~Profiling: jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität~~
UBS AG	VE-DSG	4	5		**Begründung** Die vorgeschlagene Prüf- und Nachführungspflicht würde die Pflicht zu regelmässiger Aufdatierung der Daten führen, was in der Praxis gar nicht zu bewältigen wäre. Zudem kann es nicht sein, dass der Verantwortliche in jeder Situation die Daten auf ihre Richtigkeit überprüfen muss. Gerade wenn Daten z.B. von einem Kunden zur Verfügung gestellt werden, muss der Verantwortliche davon ausgehen können, dass diese richtig sind. Eine Prüfpflicht darüber hinaus wäre nicht verhältnismässig. Aus diesen Gründen ist der

					erste Satz von Art. 4 Abs. 5 zu streichen. **Formulierungsvorschlag** [5] ~~Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden.~~ Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten
UBS AG	VE-DSG	4	6		**Begründung** Im Erläuterungsbericht (S. 47) wird gefordert, die betroffene Person dürfe nicht gänzlich untätig bleiben, damit von einer „Einwilligung“ ausgegangen werden könne.. Damit würde de facto eine verkappte Formvorschrift eingeführt. Die Einwilligung mittels Allgemeiner Geschäftsbedingungen (AGB) spielt im heutigen Geschäftsleben und Massengeschäft in allen Branchen eine entscheidende Rolle. Die schlichte Bemerkung im Erläuterungsbericht könnte dies inskünftig verunmöglichen. In Anwendung der Regeln von Art. 6 OR vereinbaren die Vertragsparteien regelmässig, dass Stillschweigen (passives Verhalten) als Einwilligung für eine explizit dargelegte Datenbearbeitung gilt. Stillschweigen ist somit als ausdrückliche Einwilligung zu qualifizieren, sofern die betroffene Person nicht innert einer bestimmten Frist (i.d.R. 30 Tage) Widerspruch erhebt. Dies sollte nicht nur in der Botschaft klargestellt werden, sondern auch im Gesetzestext. Auch bei der Einwilligung im Datenschutzgesetz handelt es sich um eine gewöhnliche Willenserklärung im Sinne des Obligationenrechts handelt. Danach kann Stillschweigen als affirmatives Verhalten genügen kann, wenn die Parteien dies vorab gültig vereinbart haben (Art. 6 OR). Eine ausdrückliche Einwilligung (oder ein anderer Rechtfertigungsgrund) als Voraussetzung für die Bearbeitung von Personendaten ist auch im Rahmen von Profiling unverhältnismässig und ginge über das hinaus, was die DSGVO verlangt. Die DSGVO knüpft an das Profiling selber keine Rechtspflichten. Profiling wird nur im Zusammenhang mit automatisierten Einzelfallentscheidungen gemäss Art. 22 DSGVO genannt, die eben typischerweise auf der Basis von Profiling und entsprechender Algorithmen erfolgen. Der Teil "und das Profiling" ist daher ersatzlos zu streichen (vgl. weiter oben Kommentar zu Art. 3 lit. f).

					Formulierungsvorschlag [6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig ~~und eindeutig~~ erfolgt. Die Einwilligung kann auch stillschweigend erteilt werden. Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen. Dies kann in standardisierter Form erfolgen.
UBS AG	VE-DSG	5	3	d	**Begründung** Die Pflicht, verbindliche unternehmensinterne Datenschutzvorschriften durch den Beauftragten vorgängig genehmigen zu lassen, erscheint uns nicht sachgerecht, da diese bereits durch die externen Revisionsstellen der Unternehmen zu prüfen sind. Daher beantragen wir die ersatzlose Streichung des Art. 5 Abs. 3 lit. d VE-DSG. **Formulierungsvorschlag** streichen
UBS AG	VE-DSG	5	5 und 6		**Begründung** Der Wortlaut von Art. 5 Abs. 1 stellt im Umkehrschluss klar, dass ein Auslandtransfer grundsätzlich erlaubt ist. Nicht erlaubt ist ein Transfer ins Ausland nur dann, wenn dadurch dem Betroffenen schwerwiegende Persönlichkeitsverletzungen drohen. Angesichts problematischer Entwicklungen in der Rechtsprechung hin zur Auffassung, Art. 5 Abs. 1 (heute Art. 6 Abs. 1) sei eine Verbotsnorm, wäre eine Klarstellung des Gesetzgebers dringend nötig. Zumindest in der Botschaft sollte klargestellt werden, dass Art. 5 keine Verbotsnorm ist – dass also Auslandtransfers (auch in die USA) erlaubt sind, solange durch den Transfer nicht eine schwerwiegende Verletzung der Persönlichkeit der Betroffenen droht. Dabei müssen die Interessen der Betroffenen am Schutz ihrer Persönlichkeit und die Interessen der Unternehmen am Auslandtransfer gegeneinander abgewogen werden (vgl. nachstehend den Kommentar zu Art. 6). Absatz 3: Der guten Ordnung halber sollte auch im Gesetzestext klargestellt werden, dass die Buchstaben a-d alternativ zu verstehen sind. Dies sollte durch den Zusatz "oder" am Ende des Wortlauts von Buchstabe

					c erfolgen. Die Regelung, wonach Binding Corporate Rules (BCR) einer Genehmigungspflicht von sechs Monaten unterliegen sollen, ist weder sachgerecht noch praktikabel (Art. 5 Abs. 3 lit. d). Einerseits stellen die BCR eine „Unterkategorie" der „spezifischen Garantien" i.S.v. Art. 5 Abs. 3 lit. b dar – für letztere ist lediglich eine Informationspflicht vorgesehen (eine Genehmigung durch den EDÖB ist nicht erforderlich). Ferner ist eine Frist von sechs Monaten abzulehnen. Dasselbe gilt für die Möglichkeit des EDÖB, Informationen nachzuverlangen, was die sechsmonatige Frist erneuern würde. Eine solche Regelung würde jeden unternehmerischen Handlungsbedarf im Keim ersticken; BCR würden im Ergebnis nicht mehr verwendet. Abs. 5 ist damit ebenfalls zu streichen. Die pauschale Informationspflicht bei der Verwendung von Standardklauseln sollten ebenfalls ersatzlos gestrichen werden. Sie bietet weder der betroffenen Person noch dem EDÖB einen Mehrwert; die DSGVO kennt auch keine entsprechende Informationspflicht (Art. 5 Abs. 6). **Formulierungsvorschlag** [3] c. standardisierte Garantien…. 2. welche der Beauftragte ausgestellt oder anerkannt hat; oder … [5] ~~-~~streichen [6] ~~-~~streichen
UBS AG	VE-DSG	6	1		**Begründung** Art. 6 Abs. 1 lit. b sollte mit der Regelung der DSGVO in Übereinstimmung gebracht werden. Danach ist eine

					Bekanntgabe im Sinne eines Ausnahmefalls auch dann zulässig, wenn die betroffene Person nicht Vertragspartei ist, aber der fragliche Vertrag in ihrem Interesse oder zu ihren Gunsten abgeschlossen wurde. So tritt z.B. die Bank bei Wertschriftentransaktion in ausländischen Effekten und bei deren Verwahrung in eigenem Namen, aber im Interesse und auf Rechnung des Kunden auf. Andere Lösungen wären in Massengeschäften dieser Art gegenüber ausländischen Vertragspartnern der Bank nicht durchsetzbar. Um schwierige Abgrenzungsfragen im Voraus auszuschliessen, sollten in Art. 6 Abs. 1 lit. c Ziff. 2 die Begriffe „Gericht“ sowie „Verwaltungsbehörde“ ersatzlos gestrichen werden. Massgebend ist, dass die Datenbearbeitung zur „Feststellung, Ausübung, Durchsetzung oder Verteidigung von Rechtsansprüchen“ erfolgt. Die hierfür zuständigen ausländischen Behörden können unterschiedlich organisiert sein, verschiedene Bezeichnungen tragen und/oder sich nicht in eine der beiden Kategorien zuordnen lassen. Zum Beispiel besteht das U.S. Department of Justice (DOJ) unter anderem aus einer "Civil Division" und einer "Criminal Division". Es kann Verstösse also einerseits strafrechtlich und andererseits im Rahmen von Zivilprozessen oder Prozessen mit (nach Schweizer Verständnis) verwaltungsrechtlichem Charakter verfolgen. Eine betroffene Person könnte sich auf den Standpunkt stellen, es handle sich beim DOJ um eine Strafbehörde und nicht um eine "Verwaltungsbehörde" im Sinne von Art. 6 Abs. 1 lit. b. Nebst der Streichung von "vor einem Gericht oder einer Verwaltungsbehörde" schlagen wir vor, die möglichen Handlungen um die "Verteidigung" zu ergänzen. Beides entspricht der Regelung in Art. 49 Abs. 1 lit. e DSGVO. In der Botschaft muss sodann klargestellt werden, dass auch die Datenbekanntgabe im Rahmen vorprozessualer Beweiserhebungen wie z.B. US-Discovery-Verfahren sowie Verfahren, die auf den Abschluss einvernehmlicher Regelungen abzielen, von diesem Rechtfertigungsgrund erfasst sind. Andernfalls wären Schweizer Unternehmen im Nachteil, die ihre Rechte in Zivilprozessen in den USA durchsetzen wollen oder in Verwaltungs- oder Strafverfahren umfassenden Mitwirkungspflichten (einschliesslich Datenlieferung) nachkommen müssen (z.B. um eine einvernehmliche Regelung mit den Behörden überhaupt abschliessen zu können; vgl. Kommentar zu Art. 13). **<u>Formulierungsvorschlag</u>** [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:

					… b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt oder einer Person, zu deren Gunsten oder in deren Interesse der Vertrag abgeschlossen wird; c. die Bekanntgabe im Einzelfall ~~unerlässlich~~ erforderlich ist für: 1. … 2. die Feststellung, Ausübung, ~~oder~~ Durchsetzung oder Verteidigung von Rechtsansprüchen ~~vor einem Gericht oder einer Verwaltungsbehörde;~~
UBS AG	VE-DSG	6	2		**Begründung** Art. 6 Abs. 2 sollte ersatzlos gestrichen werden. Erstens ist eine Verpflichtung, den EDÖB trotz Ausnahmetatbestand zu informieren, unverhältnismässig. Zweitens würde diese bereits (für Verantwortliche und Auftragsdatenbearbeiter) geltende Pflicht zu einer regelrechten „Meldeflut“ führen, welche der EDÖB gar nicht wird bewältigen könnte. Die Meldungen wären damit zwecklos und würden auf einer "Datenhalde" beim EDÖB landen. Drittens würde der EDÖB über heikle Verfahren und (Geschäftsgeheimnisse informiert, ohne zwingenden datenschutzrechtlichen Grund und ohne Mehrwert für die betroffenen Personen. Dazu muss auch erwähnt werden, dass Dritte via Einsichtsrecht aus dem Öffentlichkeitsgesetz solche Unterlagen beim EDÖB u.U. einsehen könnten, womit die Öffentlichkeit ohne entsprechende öffentliche Interessen und ggf. auch Konkurrenten über sensitive Informationen und Geschäftsgeheimnisse informiert würden. **Formulierungsvorschlag** 2 ~~streichen~~
UBS AG	VE-DSG	7	2		**Begründung** Die rechtskonforme Bearbeitung von Personendaten ist Aufgabe des Verantwortlichen. Alternativ könnte eine Pflicht formuliert werden, wonach der Auftragsdatenbearbeiter gegenüber dem Verantwortlichen erforderliche Massnahmen unternimmt, damit letzterer die Rechte der betroffenen Personen wahren kann.

					Die in Art. 7 Abs. 2 vorgesehene „Kompetenzdelegation", wonach der Bundesrat „weitere Pflichten" des Auftragsdatenbearbeiters konkretisieren könne, ist unnötig und daher zu streichen. Die im Gesetzesentwurf formulierten Pflichten gehen bereits sehr weit und sollten nicht im Sinne einer Blankodelegation an den Verordnungsgeber ausgeweitet werden. **Formulierungsvorschlag** [2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. ~~Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters.~~
UBS AG	VE-DSG	7	3		**Begründung** Art. 7 Abs. 3 muss mindestens im Erläuterungsbericht präzisiert werden, um ein Überschiessen im Vergleich zur DSGVO zu verhindern. Darin sollte klar festgehalten werden, dass eine generelle Einwilligung zum Beizug von Sub-Auftragsdatenbearbeitern ausreicht, sofern der Verantwortliche im konkreten Fall (d.h. wenn ein konkreter Sub-Auftragsdatenbearbeiter beigezogen wird) informiert wird und ein Vetorecht ausüben kann. Das Erfordernis einer vorgängigen Zustimmung würde de-facto in einem Verbot der Unterakkordanz resultieren, weil eine solche vorgängige Zustimmung in der Praxis gar nicht eingeholt werden könnte. Ausserdem wäre zu präzisieren, dass dem Schriftlichkeitserfordernis genügend Rechnung getragen wird, wenn die Zustimmung dokumentiert wird (d.h. keine Schriftlichkeit im Sinne von Art. 13 OR). **Formulierungsvorschlag** [3] Der Auftragsbearbeiter darf die Bearbeitung nur mit ~~vorgängiger~~ ~~schriftlicher~~ Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. Die Bewilligung kann in genereller Art erteilt werden. Sie ist zu dokumentieren.
UBS AG	VE-DSG	8			**Begründung**

					Die Einführung von „good practices“ wird begrüsst. Für das Verfahren oder den Erlass an sich sind aber keine Rechtsschutzmechanismen vorgesehen. Dem EDÖB würde ein viel zu weiter Ermessensspielraum eingeräumt. Würde z.B. eine „falsche“ oder unverhältnismässige Empfehlung erlassen oder genehmigt, hätte dies aufgrund der Fiktion der Rechtmässigkeit gravierende Folgen für eine Vielzahl von Verantwortlichen, Auftragsdatenbearbeiter sowie betroffener Personen. Aus diesem Grund sollte der Beauftragte lediglich die Kompetenz erhalten, vorgelegte Richtlinien zu genehmigen. Dies würde weitgehend einer Selbstregulierung entsprechen und den Vorteil haben, dass die Richtlinien von Betroffenen verfasst werden, die mit der nötigen Expertise die möglichen Besonderheiten einer Branche sachgerecht erfassen können. Damit würde der EDÖB einerseits entlastet und anderseits verhilft dieser Mechanismus zu sachgerechten Lösungen. Dem EDÖB verbleibt die Möglichkeit der Genehmigung. **Formulierungsvorschlag** Der Beauftragte genehmigt ihm vorgelegte Empfehlungen der guten Praxis, welche ~~die~~ Datenschutzvorschriften konkretisieren~~.~~ ~~Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen.~~
UBS AG	VE-DSG	9	1		**Begründung** Art. 9 Abs. 1 sollte so ergänzt werden, dass auch der Auftragsdatenbearbeiter Datenschutzvorschriften einhalten muss, welche durch Empfehlungen der guten Praxis konkretisiert werden. **Formulierungsvorschlag** Befolgen ~~t~~ der Verantwortliche und Auftragsdatenbearbeiter die Empfehlungen der guten Praxis, ~~hält~~ halten sie ~~er~~ diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren.

UBS AG	VE-DSG	12			**Begründung** Die Legitimation der Erben und deren Auskunftsrechte werden durch das Erbrecht bereits geregelt. Eine besondere datenschutzgesetzliche Spezialregelung ist unnötig. Art. 12 beinhaltet zudem Spezialregeln, welche mit dem Erbrecht teilweise kollidieren und erhebliche Widersprüche schaffen. Beispiel: Gemäss Art. 12 Abs. 4 hätte ein Erbe gegenüber einem Verantwortlichen mehr Rechte als der Erblasser zu Lebzeiten. Ferner sind die vorgesehenen Nachweise der persönlichen Beziehungen (bspw. faktische Lebensgemeinschaft; vgl. Art. 12 Abs. 2) in der Praxis kaum zu erbringen. Wir schlagen daher die ersatzlose Streichung der Bestimmung vor. **Formulierungsvorschlag** streichen
UBS AG	VE-DSG	13	1 und 4		**Begründung** Abs. 1 soll gegenüber dem geltenden Recht verschärft werden. Dafür fehlt ein sachlicher Grund. Die vorgeschlagene Variante dehnt die Informationspflicht dermassen aus, dass daraus in der Praxis ein unverhältnismässig hoher Aufwand resultiert, falls dies überhaupt umgesetzt werden kann. Sinnvollerweise wird die Informationspflicht ausdrücklich auf besonders schützenswerte Daten und überdies auf Datenbearbeitungen ausserhalb des (objektivierten) Erkennbarkeitshorizonts i.S.v. Art. 4 DSG der betroffenen Person eingeschränkt. Dies folgt aus dem naheliegenden Grundsatz, dass alle anderen Daten entsprechend den Grundsätzen von Art. 4 für die betroffene Person erkennbar sind und demzufolge keiner (zusätzlichen) Information bedürfen. Wir bevorzugen die alte Fassung nach Art. 14, welche die Informationspflicht auf die Beschaffung von *besonders schützenswerten* Personendaten einschränkt. Sollte die Informationspflicht künftig dennoch für die Bearbeitung jeglicher Personendaten gelten, so ist es

					unabdingbar, in Art. 14 weitere Ausnahmen festzulegen. Bekanntlich erlaubt es Art. 23 DSGVO den EU-Mitgliedstaaten, gesetzliche Ausnahmen von der Informationspflicht (und vom Auskunftsrecht) festzulegen. Der Schweizer Gesetzgeber sollte seinen (als Nicht-EU-Mitgliedsstaat noch grösseren) Handlungsspielraum hier nutzen (vgl. Kommentar zu Art. 14). Gemäss der vorliegenden Bestimmung ist über die Identität und die Kontaktdaten der Auftragsbearbeiter und konsequenterweise auch aller Unterauftragsbearbeiter zu informieren. Dies geht sowohl über die Vorgaben der Konvention 108 als auch der DSGVO hinaus. Die Auslagerung von Dienstleistungen und der damit einhergehenden Datenbearbeitungen gehört zum täglichen Geschäftsbetrieb jedes Unternehmens. Auch das betroffene Datensubjekt weiss, dass nicht jeder Betrieb sämtliche Dienstleistungen selber erbringen kann. Dieser Informationspflicht nachzukommen, lässt sich für Unternehmen nur mit einem unverhältnismässigen Aufwand bewerkstelligen. Überdies ist gemäss Gesetzeswortlaut unklar, wann genau über was informiert werden muss. Aus Sicht des Persönlichkeitsschutzes ist entscheidend, dass die Datenbearbeitung nur unter Einhaltung der gesetzlichen Vorgaben erfolgen kann. Dies zu regeln ist Gegenstand von Art. 7. Eine darüberhinausgehende Informationspflicht birgt aus datenschutzrechtlicher Sicht keinerlei Mehrwert. Das würde beispielsweise dazu führen, dass ein Kundenberater, der seinem Kunden via Fleurop einen Blumenstrauss schicken möchte, dem Kunden vorgängig mitteilen muss, dass seine Adressdaten an Fleurop gehen. Wenn Fleurop einen weiteren lokalen Blumenladen damit beauftragt, muss Fleurop uns um Einwilligung bitten und es ist eine schriftliche Zustimmung notwendig. Dies schiesst somit offensichtlich über das Ziel hinaus und ist in der Praxis nicht umsetzbar. Zudem handelt es sich um einen Swiss Finish, der sachlich weder geboten noch gerechtfertigt ist. Wir beantragen daher die Streichung von Art. 13 Abs. 4 zu streichen. **Formulierungsvorschlag** [1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von besonders schützenswerten Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. [4] ~~streichen~~.

UBS AG	DSG	14	2	C (neu)	**Begründung** Die DSGVO sieht keine Informationspflicht vor, wenn die Daten einem Berufsgeheimnis unterliegen. Wir empfehlen deshalb, eine zusätzliche Bestimmung aufzunehmen, damit das Schweizer Amts- und Berufsgeheimnis gewahrt ist. So werden beispielsweise Banken von der FINMA angehalten, Hintergrundinformationen zu Vertragspartner, Kontrollinhaber und wirtschaftlich Berechtigten zu sammeln. Diese Information dürfen jedoch nur eingeschränkt an die betroffenen Personen weitergeleitet werden. **Formulierungsvorschlag:** die Daten dem [Amts- oder] Berufsgeheimnis unterliegen.
UBS AG	VE-DSG	14	4	a	**Begründung** Für die Einschränkung gemäss Art. 14 Abs. 4 lit. a gibt es aus datenschutzrechtlichen Überlegungen keinerlei Berechtigung. Zudem geht die Bestimmung unnötigerweise über die Regelung der europäischen DSGVO hinaus. Sollten die Interessen der betroffenen Personen durch die Bekanntgabe an einen Dritten tatsächlich beeinträchtigt sein, ist dies bereits im Rahmen der allgemeinen Interessenabwägung im nach Art. 24 berücksichtigt. Demgegenüber enthält Absatz 4 lit. a eine pauschal vorweggenommenen Interessenabwägung. Nebst mangelnder Rechtfertigung würde dies mitunter auch zu Rechtsungleichheit und absurden Resultaten führen: So dürfte ein Konzernunternehmen, welches Daten mit einem anderen Konzernunternehmen nicht ausschliesslich für die Zwecke der Auftragsdatenbearbeitung teilt, nicht auf ein überwiegendes eigenes Interesse abstellen während ein Unternehmen, das Daten innerhalb der gleichen juristischen Person ins Ausland liefert, dies nach wie vor könnte. Es wäre umgekehrt der Rechtssicherheit förderlich, wenn einige der überwiegenden Interessen des Verantwortlichen in Art. 14 Abs. 4 lit. a aufgeführt würden. Es gibt viele Situationen, in denen ein Unternehmen ein Interesse daran hat, betroffene Personen nicht schon bei der Beschaffung von Personendaten über die Beschaffung und die beabsichtigte Verarbeitung oder Bekanntgabe zu informieren. In vielen Fällen würde eine vorgängige Information sogar den eigentlichen Zweck der Bearbeitung vereiteln. Dies zeigt sich zum Beispiel im Zusammenhang mit der internen Beweiserhebung zur Vorbereitung von

					Gerichtsprozessen oder zur Erfüllung von Mitwirkungspflichten im Rahmen von Verwaltungs-, Aufsichts- oder Strafverfahren. Unternehmen haben ein legitimes Interesse, die Vorbereitung von Zivilprozessen, in denen das Unternehmen Kläger oder Beklagter ist, geheim zu halten und dabei auch Personendaten ihrer Mitarbeiter, Berater, Kunden oder Mitarbeiter der Kunden zu bearbeiten. Eine vorgängige Information der betroffenen Personen würde den eigentlichen Zweck der Bearbeitung vereiteln. Entsprechendes gilt für interne Untersuchungen und Whistleblowing-Verfahren: Damit der Zweck einer internen Untersuchung bzw. eines Whistleblowing-Verfahrens nicht vereitelt wird, können die betroffenen Mitarbeiter nicht vorgängig über die Datenbearbeitung informiert werden. Nicht zuletzt könnte das Unternehmen auch seinen Mitwirkungspflichten im Rahmen von inländischen oder ausländischen Verwaltungs- oder Strafverfahren (einschliesslich Kartellverfahren) nicht, nicht richtig oder nicht rechtzeitig nachkommen, wenn alle betroffenen Personen vorgängig über eine Datenbearbeitung (z.B. Erhebung und Lieferung von Beweisen, die Personendaten von Mitarbeitern enthalten) informiert werden müssten. Eine solche Information wäre den Unternehmen aufgrund bestehender Geheimhaltungs- oder Kooperationspflichten in den entsprechenden Verfahren gar nicht erlaubt. Sie würde den Zweck der behördlichen Untersuchung in Frage stellen und es dem Unternehmen in vielen Fällen sogar verunmöglichen, Rechte durzusetzen, Klagen abzuwehren oder sich in Strafverfahren rechtzeitig und adäquat zu verteidigen. Zum Beispiel ist es gemäss dem sog. Yates Memorandum absolut notwendig, dass Unternehmen bereits zu Beginn einer Untersuchung die Namen sämtlicher für den Verstoss verantwortlicher Mitarbeiter im Unternehmen nennt. Das Yates Memorandum bzw. die entsprechend dem Memorandum revidierten Grundsätze des U.S. Department of Justice sind Anweisungen an die Staatsanwälte, dass parallel zu Ermittlungen gegen ein Unternehmen von Anfang an auch gegen verantwortliche Mitarbeiter innerhalb des Unternehmens ermittelt werden soll. Zudem ist darin festgelegt, dass Unternehmen nur dann mit einer einvernehmlichen Regelung einschliesslich Kooperationskredit rechnen dürfen, wenn sie von Anfang an alle relevanten Tatsachen zu mutmasslich am Fehlverhalten beteiligten oder dafür verantwortlichen Mitarbeiter offen legen – einschliesslich der Namen der Mitarbeiter (Alles-oder-Nichts-Prinzip). Entsprechend ist Art. 14 Abs. 4 lit. a wie oben vorgeschlagen anzupassen. Klarstellend, diese zusätzlichen Ausnahmen in Abs. 4 müssten konsequenterweise auch als mögliche Gründe für die Einschränkung des Auskunftsrechts (so der Verweis in Art. 21 Abs. 1) und als Rechtfertigungsgrund für Verletzungen von

					Bearbeitungsgrundsätzen (vgl. Kommentar zu Art. 24) gelten. **Formulierungsvorschlag** a. Wenn es sich beim Verantwortlichen um eine private Person handelt, 1. falls überwiegende Interessen des Verantwortlichen dies erfordern 2. falls die Übermittlung der Information den Zweck der Bearbeitung, insbesondere die Feststellung, Ausübung, Durchsetzung oder Verteidigung von Rechtsansprüchen, in Frage stellen würde. ~~und er die Personendaten nicht Dritten bekannt gibt;~~
UBS AG	VE-DSG	14	5		**Begründung** Art. 14 Abs. 5 sollte ersatzlos gestrichen werden. Diese Pflicht hätte faktisch zur Folge, dass Unternehmen permanent überprüfen müssten, ob eine Interessenabwägung aktuell noch gleich ausfallen würde. Das ist in grossen, komplexen Organisationen schlichtweg nicht zu bewerkstelligen. Der Vorschlag ist in keiner Weise praxistauglich. Demgegenüber ist es für die betroffene Person zumutbar, dass sie ein Informationsgesuch gegebenenfalls wiederholt. **Formulierungsvorschlag** streichen
UBS AG	VE-DSG	15	2		**Begründung** Das in Art. 15 Abs. 2 vorgesehene Äusserungsrecht bzw. die Anhörungspflicht zu den bearbeiteten Personendaten ist unseres Erachtens ersatzlos zu streichen. Eine Datenbearbeitung mit ausschliesslich automatisierten Mitteln ist an und für sich kein schwererer Eingriff in Persönlichkeitsrechte als eine rein "menschliche" Bearbeitung. Im Gegenteil, eine Algorithmen basierte

					Datenbearbeitung, die den zwingenden Grundsätzen des Privacy by Default und Design folgt, bietet eine grössere Gewähr der Rechtskonformität; der Risikofaktor "Mensch" kann hier ausgeschlossen werden. Aus diesem Grund beinhaltet das fragliche Äusserungsrecht keinen Mehrwert für die betroffenen Personen; es ist ein sachlich nicht begründeter Ausdruck eines generellen Misstrauens gegenüber "der Maschine". Als solches ist es technologie- und innovationsfeindlich. Darüber hinaus ist ein solches Recht angesichts der ebenfalls neu eingeführten Pflicht, die betroffene Person darüber zu informieren, wenn eine automatisierte Einzelentscheidung gefällt wurde (Abs. 1), unnötig. Unabhängig davon quasi „auf Vorrat“ zu informieren, produziert demnach keine zusätzliche Transparenz, sondern generiert lediglich unnötigen zusätzlichen Administrativaufwand. Weder ERK 108 noch DSGVO sehen ein entsprechendes Äusserungsrecht vor. Die Regelung ist demzufolge ein unnötiger Swiss Finish. **Formulierungsvorschlag** [2] streichen
UBS AG	VE-DSG	15	3		**Begründung** Ferner sollte die Informationspflicht betreffend automatisierter Einzelentscheidungen wegfallen, wenn solche automatisierten Einzelentscheidungen gestützt auf eine Vereinbarung zwischen der betroffenen Person und dem Verantwortlichen gefällt werden und sie den erkennbaren Kern der Vereinbarung ausmachen. Dies kann z.B. bei einem Vertrag betreffend die automatisierte Verwaltung des Vermögens der betroffenen Person gegeben sein (z.B. RoboAdvice – hier möchte der Kunde gerade eine ausschliesslich automatisierte Einzelentscheidung). Diesfalls sind der betroffenen Person die zugrundeliegenden Parameter bekannt bzw. sie hat diese mit dem Verantwortlichen vereinbart. In diesem Rahmen kann sich die betroffene Person sogar zum gesamten Prozedere betreffend das Fällen von automatischen Einzelentscheidungen im Voraus äussern. Entsprechend sollte in Art. 15 Abs. 3 VE DSG festgehalten werden, dass die Informationspflicht nicht anwendbar ist, wenn eine Vereinbarung zwischen dem Verantwortlichen und der betroffenen Person die Abgabe (ev. einer Vielzahl) von automatisierten Einzelentscheidungen bezweckt und dies aus der Vereinbarung erkennbar ist (analog Ausnahme kraft Gesetz); die Schlechterstellung einer erkennbaren Datenbearbeitung im privaten Bereich ist ausserdem nicht gerechtfertigt.

					Allenfalls könnte auch die Möglichkeit eines Verzichtes auf die Informations- und Anhörungspflicht in Art. 15 DSG aufgenommen werden. **Formulierungsvorschlag** [3] Die Informations~~- und Anhörungs~~pflicht gilt nicht, wenn ein Gesetz oder ein Vertrag zwischen Verantwortlichem und betroffener Person eine automatisierte Einzelentscheidung vorsieht.
UBS AG	VE-DSG	16	1		**Begründung** ***a) Schwelle*** Die Schwelle zur Durchführung einer Datenschutzfolge-Abschätzung (DSFA) wurde zu tief angesetzt und mit vagen Kriterien umschrieben. Ein „voraussichtlich erhöhtes Risiko“ wird es bei jeder Datenbearbeitung geben; insbesondere bei einer grösseren Unternehmung, die Personendaten grenzübergreifend bearbeitet. Zudem ist unklar im Verhältnis zu was das Risiko „erhöht“ sein muss. Aus dem Erläuterungsbericht geht sinngemäss hervor, dass jede Übermittlung von Personendaten in die USA, jedes Profiling sowie jede Bearbeitung besonders schützenswerter Personendaten eine DSFA verlangen würde. Faktisch müssten also sämtliche Datenbearbeitungen einer aufwendigen DSFA unterzogen werden. Der hierfür benötigte Aufwand wäre **unverhältnismässig**, der Mehrwert für die betroffene Person dafür gering. Ferner liegt die erwähnte Schwelle des VE-DSG deutlich unter dem „**hohen“ Risiko**, welches gemäss Art. 36 Abs. 1 DSGVO verlangt wird. Im Interesse der Rechtssicherheit müssten Datenbearbeitungen mit hohem Risiko, auf Verordnungsstufe durch eine Aufzählung der Fälle abschliessend definiert werden. Schliesslich müsste klar festgehalten werden, dass eine Wiederholung (Update) einer DSFA nicht nötig sei, sofern und soweit sich die Logik der fraglichen Datenbearbeitung im Wesentlichen nicht ändert. Ferner müsste eine DSFA ausbleiben können, wenn ein Rechtfertigungsgrund gegeben ist oder die betroffenen Personen nach entsprechender Aufklärung über das hohe Risiko gem. Abs. 1 in die fragliche Datenbearbeitung rechtsgültig eingewilligt haben. Sobald eine Einwilligung vorliegt, besteht keine Notwendigkeit einer DSFA, da die Rechte der betroffenen Person auf diese Weise bereits berücksichtigt

					sind. ***b) Auftragsdatenbearbeiter*** Angesichts der Tatsache, dass nur der Verantwortliche über Zweck, Mittel sowie Umfang der Datenbearbeitung entscheidet, ist es nicht sachgerecht, dass auch der Auftragsdatenbearbeiter der Pflicht zur Durchführung einer DSFA unterliegt. Letzterer wird regelmässig nicht über die für eine DSFA notwendigen Angaben verfügen. **Formulierungsvorschlag** [1] Führt die vorgesehene Datenbearbeitung ~~voraussichtlich~~ zu einem ~~erhöhten~~ hohen Risiko für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen. Der Bundesrat definiert die Datenbearbeitungen mit hohem Risiko.
UBS AG	VE-DSG	16	2-5		**Begründung** Des Weiteren ist die pauschale Meldepflicht samt Einwendungsmöglichkeit des EDÖB nicht praktikabel, unverhältnismässig und ohne jeden Mehrwert für die betroffene Person. Der EDÖB wäre kaum in der Lage, die Flut an Anfragen innerhalb angemessener Frist zu bearbeiten. Auch in dieser Hinsicht liegt ein unnötiger Swiss Finish vor. Die DSGVO ist weniger streng: eine Meldepflicht besteht dort nur, wenn für die fragliche Datenbearbeitung trotz mitigierender Massnahmen ein hohes Risiko der Verletzung von Persönlichkeitsrechten der betroffenen Personen verbleibt. Entsprechend sollte eine aufgrund transparenter Information der betroffenen Person basierende Datenverarbeitung nicht auch noch zu einer DSFA führen. Ausserdem sieht Art. 16 Abs. 4 vor, dass der EDÖB seine Einwände innert drei Monaten geltend machen kann. Während dieser Zeit steht die fragliche Datenbearbeitung still; mit entsprechenden Auswirkungen auf z.B. zeitkritische Projekte. Zusätzlich kann der EDÖB diese Frist selber um jeweils weitere drei Monate verlängern, immer wenn er weitere Angaben für „erforderlich“ hält. Die DSGVO ist in dieser Hinsicht viel praxisnäher: sie sieht eine acht wöchige Frist vor; diese kann nur in besonderen Ausnahmefällen um sechs Wochen verlängert werden (vgl. Art. 36 Abs. 2 DSGVO). Wir würden anregen die Lösung der DSGVO entsprechend zu übernehmen. Für eine abweichende Regel gibt es keine Veranlassung.

					Wie oben ausgeführt, ist es falsch, von einem Schutz „der Grundrechte“ von natürlichen Personen zu sprechen. Das entspricht zwar mehr oder weniger der Regelung der DSGVO. Das europäische Recht kennt aber eine direkte Drittwirkung der Grundrechte, die dem schweizerischen Recht fremd ist. Es ist nicht Aufgabe privater Datenbearbeiter, die Grundrechte betroffener Personen zu schützen, soweit diese Grundrechte nicht in den einzelnen Anforderungen des DSG Ausdruck gefunden haben. Dazu kommt, dass völlig unklar ist, um welche Grundrechte es geht und welche Risiken dabei relevant wären. **Formulierungsvorschlag** 2 Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit ~~oder der Grundrechte~~ der betroffenen Person zu verringern. 3 Der Verantwortliche ~~oder der Auftragsbearbeiter~~ benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen**,** sofern die Datenbearbeitung trotz der vorgesehenen Massnahmen zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. 4 Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von ~~drei~~ zwei Monaten nach Erhalt der Benachrichtigung ~~aller erforderlichen Informationen~~ mit. 5bis Wurde die betroffene Person über das hohe Risiko nach Abs. 1 aufgeklärt und stimmt sie dennoch der Datenbearbeitung zu, kann von der Datenschutz-Folgeabschätzung abgesehen werden
UBS AG	VE-DSG	17			**Begründung** Der Anwendungsbereich von Art. 17 ist wesentlich weiter als jener der DSGVO. Im schweizerischen Recht soll faktisch jede „falsche“ Datenbearbeitung erfasst werden, während unter dem Regime der DSGVO eine getroffene Sicherheitsmassnahme verletzt werden muss, die zusätzlich zu einem Bruch bzw. Verlust des Gewahrsams an den betroffenen Personendaten geführt haben muss. Abs. 1 sollte deshalb entsprechend der DSGVO angepasst werden. Der Swiss Finish ist unbegründet. Ausserdem wäre der EDÖB mit einer

					Meldungsflut konfrontiert, die er nicht bewältigen, geschweige darauf reagieren könnte. Dies zeigen die Erfahrungen der Niederlande, wo seit einem Jahr auf nationaler Ebene eine entsprechende Meldepflicht besteht. Art. 17 führt zu einer Unternehmenskultur mit starker Überwachung und grossem Compliance Aufwand. Ein für den Datenschutz verantwortlicher Mitarbeiter wäre unter Strafdrohung verpflichtet, seine für einen Datenschutzverstoss verantwortlichen Kollegen beim EDÖB zu melden. Aufgrund der Anzeigepflicht des EDÖBs würden die Mitarbeiter, die für die entsprechende Verletzung der Sicherheit von Personendaten verantwortlich wären, der strafrechtlichen Verantwortung unterzogen (Art. 51 Abs. 1 lit. c). Dieser Mechanismus ist aber auch mit den Grundprinzipien des Strafrechts, insbesondere dem Prinzip des *Nemo tenetur,* nicht vereinbar. Befolgt der Verantwortliche die Meldepflicht nicht, wird er gleichwohl durch Nichteinhaltung derselben strafbar (Art. 50 Abs. 2 lit. e). Umso schlimmer ist diese Regelung, wenn man davon ausgeht, dass seriöse Datenbearbeiter der Meldepflicht nachkommen werden und gestützt darauf „als Dank“ für ihre Versäumnisse sanktioniert werden. Eine Meldung beim EDÖB müsste im Gegenteil den Schutz des Unternehmens und verantwortlicher Mitarbeiter vor (mindestens) strafrechtlichen Sanktionen zur Folge haben. Zudem sollte eine Meldung ohne Nennung der für den Data Breach verantwortlichen Person(en) möglich sein. Gemäss Wortlaut des Gesetzesvorschlags muss die Meldung "unverzüglich" erfolgen. Obschon hier nicht klar ist, ob sich der Gesetzgeber eine gemessen an den 72 Stunden der DSGVO - längere oder kürzere Frist vorstellt oder ob sich diese an irgendwelchen äusseren Umständen bemisst, suggeriert eine "unverzügliche" Meldung, dass das betroffene Unternehmen in der Praxis die Meldung übereilt absetzten muss, ohne dass der betroffenen IT-Abteilung die Zeit bleibt, den eigentlichen Fehler, der zu einer Verletzung geführt hat, vorab ausreichend zu untersuchen, zu analysieren und zu beheben. Auch Abs. 2 geht über die DSGVO hinaus. Jene erfordert eine Information nur, wenn ein hohes Risiko für eine Persönlichkeitsverletzung besteht. Es ist nicht ersichtlich, weshalb die Schweiz hier weitergehen sollte. Wir lehnen einen Swiss Finish auch hier ab und schlagen eine Angleichung an das EU Recht vor. Damit wäre auch sichergestellt, dass die betroffene Person nicht unnötig alarmiert wird, sondern nur dann, wenn eine tatsächliche Gefahr besteht. Damit hätten solche Benachrichtigungen auch eine grössere Wirkung, als wenn sie in grosser Zahl wegen Unbedeutendem abgesetzt werden müssen. Schliesslich ist der Mechanismus der Informationspflicht so zu organisieren, dass dies Primär Aufgabe des Verantwortlichen ist.

					Nur wenn dieser nicht informiert, soll der EDÖB eine Möglichkeit haben, das Nachholen anzuordnen, wenn er ein hohes Risiko einer Persönlichkeitsverletzung sieht. Im Übrigen bestehen berechtigte Interessen der Verantwortlichen, betroffene Personen nicht über einen Data Breach zu informieren. Hier werden einerseits die Ausnahmen gemäss Art. 14 Abs. 3 und 4 greifen (vgl. Kommentar dazu oben). Andererseits braucht es in Art. 17 klar geregelte Ausnahmen von der Meldung an betroffene Personen, wie sie auch in Art. 33 Abs. 3 DSGVO vorgesehen sind. Zum Beispiel wäre es unverhältnismässig und zum Schutz der Persönlichkeit und der Grundrechte betroffener Personen unnötig, Data Breaches zu melden, von denen nur verschlüsselte Daten betroffen waren. Wir empfehlen, diese und weitere in Art. 33 Abs. 3 DSGVO geregelten Ausnahmen in Art. 17 (wie oben vorgeschlagen) zu übernehmen. Dies würde den notwendigen Spielraum für eine einzelfallgerechte Abklärung ermöglichen und damit den effektiven Schutz der Persönlichkeitsrechte der betroffenen Personen sicherstellen. **Formulierungsvorschlag** 1 Der Verantwortliche meldet dem Beauftragten ~~unverzüglich~~ ~~Verzug~~ eine Verletzung der Sicherheit von Personendaten ~~unbefugte Datenbearbeitung oder den Verlust von Daten~~, es sei denn die Verletzung ~~des Datenschutzes~~ der Sicherheit von Personendaten führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person. Die gemeldete Verletzung wird strafrechtlich nicht verfolgt. 2 Der Verantwortliche informiert ausserdem die betroffene Person, wenn die Verletzung der Sicherheit von Personendaten voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen darstellt.~~es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt~~. er Beauftragte kann den Verantwortlichen auffordern, dies nachzuholen, falls er zum Schluss kommt, dass ein hohes Risiko vorliegt. 2ter Die Benachrichtigung der betroffenen Person gemäss Abs. 2 ist nicht erforderlich, wenn: a. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen Personendaten angewandt wurden, insbesondere solche, durch die die Personendaten für alle Personen, die nicht zum Zugang zu den Personendaten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

					b. der Verantwortliche durch nachfolgende Massnahmen sichergestellt hat, dass das hohe Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen gemäss Absatz 2 mit hoher Wahrscheinlichkeit nicht mehr besteht; oder c. dies mit einem unverhältnismässigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Massnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden. – [3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. [4] Der Auftragsbearbeiter informiert den Verantwortlichen ~~unverzüglich~~ über eine Verletzung gemäss Absatz 1 ~~unbefugte Datenbearbeitung.~~
UBS AG	VE-DSG	18	1		**Begründung** Die schweizerische Regulierung weitet in diesem Punkt den Adressatenkreis auf den Auftragsbearbeiter aus. Wir beantragen, die Vorschrift an die Regelung der DSGVO anzupassen. **Formulierungsvorschlag:** [1] Der Verantwortliche ~~und der Auftragsbearbeiter~~ sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit ~~oder der Grundrechte~~ verringern und solchen Verletzungen vorbeugen.
UBS AG	VE-DSG	18	2		**Begründung** Bei Art. 18 Abs. 2 geht es im Kern um „Privacy by default“ als Präzisierung des Verhältnismässigkeitsgrundsatzes im Sinne von Art. 4 Abs. 2. Danach soll diejenige Datenbearbeitung voreingestellt sein, welche am schonendsten ist und nur ein Minimum an Personendaten für die Bearbeitung umfasst. Der gewählte Wortlaut bringt dieses Anliegen jedoch nur ungenügend zum Ausdruck. Richtigerweise sollte diese Bestimmung nicht an der Art bzw. dem Umfang der Personendaten, sondern am standardmässig vorgesehenen Zweck anknüpfen.

					Formulierungsvorschlag [2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig ~~nur diejenigen~~ Personendaten nur derart bearbeitet werden, ~~die~~ wie es für den jeweiligen Verwendungszweck erforderlich ~~sind~~ ist.
UBS AG	VE-DSG	19			**Begründung** Umfang und Inhalt der Dokumentationspflicht gemäss Art. 19 lit. a sind unklar. Klar ist hier einzig, dass diese Regelung über die vergleichbare Bestimmung der DSGVO hinaus geht (vgl. Art. 30 DSGVO). Letztere verlangt nämlich nur ein Verzeichnis. Richtigerweise sollte Art. 19 lit. a mit „ein Verzeichnis für regelmässige Datenbearbeitungen“ angepasst werden. Andernfalls müsste jede E-Mail, jede Chatnachricht etc. dokumentiert werden, womit der Aufwand für die Dokumentation ungleich höher als das Verfassen einer E-Mail wäre. Alternativ könnte am bewährten Begriff der Datensammlung gemäss Art. 3 lit. g DSG festgehalten werden. Dieser würde eine bereits existierende und verlässliche Übersicht über die massgeblichen Datenbearbeitungen bieten. Art. 19 lit. b ist viel zu breit formuliert, erfasst auch nur unbedeutende Vorgänge und ist damit unverhältnismässig. Einerseits müssten Verantwortliche und Auftragsdatenbearbeiter über heikle oder sensible Datenschutzverletzungen eine Vielzahl Dritter informieren, was ein grober Eingriff in ihre Privatsphäre wäre. Andererseits wäre der Aufbau einer neuen Infrastruktur, welche zentralisiert sämtliche Empfänger von Personendaten über Jahrzehnte verwaltet im Vergleich zum Nutzen nicht verhältnismässig. Schliesslich müssten, wenn überhaupt, nicht die Empfänger, sondern die betroffenen Personen informiert werden, um ihre Persönlichkeitsrechte zu wahren. Alternativ wäre eine Nachinformation konkreter Empfänger auf Gesuch und bei berechtigten Interessen der betroffenen Personen denkbar. Wir beantragen die Streichung von lit. b. **Formulierungsvorschlag** Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet:

					a. Sie ~~dokumentieren ihre Datenbearbeitung~~ erstellen ein Verzeichnis für regelmässige Datenbearbeitungen; b. ~~Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.~~
UBS AG	VE-DSG	20	2 und 3		**Begründung** Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen sowie auf hängige Verfahren (vgl. Art. 2 Abs. 3) ist unverhältnismässig. Dies gilt umso mehr, als dass gemäss der in Schweiz geltenden Rechtsprechung kein Auskunftsersuchen je rechtsmissbräuchlich sein kann, weil selbst ein untergeordnetes Datenschutzinteresse ausreicht, um ein Auskunftsanspruch zu bejahen. Die Anknüpfung am bisher bewährten System der Datensammlung wäre sachgerechter und würde den betroffenen Personen ausreichenden Schutz bieten. Schliesslich ist dem zunehmenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke ein Riegel zu schieben. Die Vergangenheit hat gezeigt, dass einerseits datenschutzrechtliche Begründungen viel zu leicht vorgeschoben werden können, um eine kostenlose Beschaffung von Beweismitteln durchzusetzen. Andererseits hat die Anzahl querulatorischer, kosten- und ressourcenintensiver Fälle zu Schikanezwecken ebenfalls stark zugenommen. Aus diesen Gründen ist die pauschale Kostenlosigkeit der Auskunft zu relativieren und stattdessen ein angemessener Unkostenbeitrag vorzusehen. Alternativ wäre analog Art. 12 Abs. 5 lit. a DSGVO dem Bundesrat die Kompetenz einzuräumen, die Ausnahmen der Kostenlosigkeit auf Verordnungsstufe festzulegen. Der bisherige Abs. 5 von Art. 8 DSG, wonach die Auskunft in der Regel schriftlich in der Form eines Ausdrucks oder einer Fotokopie zu erteilen ist, wurde zurecht nicht in Art. 20 DSG übernommen. Gerade die Möglichkeit, eine Fotokopie von jeglichen Dokumenten zu erhalten, auf denen die Personendaten einer betroffenen Person genannt werden, hat in der Praxis zu Missbräuchen des Auskunftsrechts für datenschutzfremde Zwecke sowie zu exzessiven Auskunftsersuchen geführt. Auch hat dies dazu geführt, dass Unternehmen Personendaten über Drittpersonen oder der Geheimhaltung unterliegende Abschnitte

					der jeweiligen Dokumente zuvor in aufwendigen Verfahren abdecken bzw. schwärzen mussten. Will der Gesetzgeber – was unseres Erachtens im Interesse der Wirtschaft absolut notwendig ist – diesen Auswüchsen Einhalt gebieten, so muss er das klarstellen und Art. 20 Abs. 2 lit. b wie vorgeschlagen anpassen. Ferner erachten wir es als ausreichend, wenn die Herkunft der Personendaten dann angegeben werden muss, wenn die Daten nicht bei der betroffenen Person selbst erhoben wurden. Dies entspricht Art. 15 Abs. 1 lit. g DSGVO. Überdies ist es zur Vermeidung von Missbräuchen erforderlich, die oben (Abs. 5ter) vorgeschlagene Verwendungsbeschränkung festzulegen. Der zweite Halbsatz in Abs. 3 ist unseres Erachtens ersatzlos zu streichen. Eine derart weitgehende Begründungs- bzw. Rechtfertigungspflicht stellt einen Swiss Finish dar, der datenschutzrechtlich nicht gerechtfertigt werden kann. Er würde ausserdem zwangsläufig zu einer Offenlegung von Geschäftsgeheimnissen sowie internen Entscheid- und Ablaufverfahren führen. Alternativ wäre diese Regelung auf eine sehr generelle Darlegung der Funktionsweise automatisierter Einzelentscheide zu beschränken. **Formulierungsvorschlag** 2 Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die ~~bearbeiteten~~ Kategorien von Personendaten, die über die betroffene Person bearbeitet werden, nicht aber eine Kopie jeglicher über diese bearbeiteten Personendaten; c. der Zweck der Bearbeitung; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; e. das Vorliegen einer automatisierten Einzelentscheidung;

					f. die verfügbaren Angaben über die Herkunft der Personendaten, falls diese nicht bei der betroffenen Person erhoben werden ; g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4. [3] Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis~~, das Zustandekommen und die Auswirkungen der Entscheidung~~. [5bis] Ausnahmsweise können der betroffenen Person die mit dem Auskunftsersuchen zusammenhängenden Kosten auferlegt werden a. wenn das Ersuchen einen übermässigen Aufwand verursacht, der nicht vom Verantwortlichen zu verantwortenden ist; oder b. bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Auskunftsbegehren einer betroffenen Person. Wobei in solchen Fällen die Auskunft auch gemäss Art. 21 auch verweigert oder eingeschränkt werden kann. Der Bundesrat regelt die Einzelheiten. [5ter] Der Gesuchsteller darf die ihm vom Verantwortlichen übermittelten Daten nicht zu anderen als datenschutzrechtlichen Zwecken verwenden. Insbesondere ist jede Verwendung der Daten im Rahmen von Zivil- oder Strafprozessen oder Verwaltungsverfahren, die nicht die Durchsetzung von Datenschutzrechten des Gesuchstellers betreffen, unzulässig. [6] Niemand kann im Voraus auf das Auskunftsrecht verzichten.
UBS AG	VE-DSG	21			**Begründung** Angesichts des oben dargelegten Missbrauchs des Auskunftsrechts zur Prozessvorbereitung bzw. zur Erlangung von Beweisen während laufender Prozesse müsste ein effektiver Mechanismus gegen solchen Missbrauch vorgesehen werden. In diesem Zusammenhang wäre denkbar, eine in der Praxis bewährte Vorgehensweise aus dem Bereich der Strafverfolgung anzuwenden (vgl. Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI); SR 361): Danach könnte der Verantwortliche bei begründetem Verdacht auf Missbrauch die herauszugebenden Personendaten einem Dritten (bspw. dem EDÖB) übergeben. Dieser würde anstelle des Gesuchstellers die Einhaltung bzw. Verletzung des Datenschutzes prüfen und sein Prüfergebnis in Form einer anfechtbaren Verfügung vorlegen (vgl. eine

					analoge Regelung in Art. 8 Abs. 2 BPI). Aufgrund der obengenannten Rechtsprechung beantragen wir, den offensichtlichen Rechtsmissbrauch explizit als Rechtfertigung aufzunehmen, um ein Ersuchen abzulehnen. Der EDÖB soll in Zweifelsfällen entscheiden, ob ein Missbrauch vorliegt oder nicht, falls die betroffene Person dies wünscht. **Formulierungsvorschlag** [1] Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. [1bis] Ausserdem kann die Auskunft nach diesem Gesetze verweigert werden, wenn das Ersuchen offensichtlich nicht datenschutzrechtlichen Zwecken dient. Lehnt der Verantwortliche ein Ersuchen nach diesem Absatz ab, kann die betroffene Person verlangen, dass der Beauftragte entscheidet, ob das Ersuchen datenschutzrechtlich motiviert ist. [1ter] Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Auskunftsbegehren einer betroffenen Person kann der Verantwortliche entweder a. ein angemessenes Entgelt gemäss Art. 20 Abs. 5[bis] verlangen; oder b. sich weigern, aufgrund des Auskunftsbegehrens tätig zu werden. Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.
UBS AG	VE-DSG	23	2	d	**Begründung** Zur Begründung wird auf die Ausführungen zu Profiling unter Art. 3 lit. f VE DSG sowie unter Art. 4 Abs. 6 VE DSG verwiesen. **Formulierungsvorschlag** Abs. 2 lit. d: streichen

UBS AG	VE-DSG	24			**Begründung** In Art. 24 Abs. 2 sollte „möglicherweise“ ersatzlos gestrichen werden. Dieser Begriff ist überflüssig und schafft Rechtsunsicherheit. Art. 24 Abs. 2 lit. a müsste dahingehend angepasst werden, dass ein überwiegendes Interesse auch dann vorliegt, wenn die betroffene Person nicht Vertragspartei ist, aber der fragliche Vertrag in ihrem Interesse abgeschlossen wurde (vgl. auch Begründung zu Art. 6 Abs. 1 lit. b). Die Einschränkung gemäss Art. 24 Abs. 2 lit. c Ziff. 1 ist nicht sachgerecht und müsste gestrichen werden. Sie verkennt, dass bspw. Massnahmen der sozialen Hilfe (Art. 3 lit. c Ziff. 6) von zentraler Bedeutung für die Beurteilung der Kreditwürdigkeit sein können. Ein Verzicht darauf würde zu Fehlbewertungen führen, was nicht im Interesse der betroffenen Person sein kann. Mit Art. 24 Abs. 2 lit. g ist ein Rechtfertigungsgrund einzuführen, welcher den Einsatz neuer Technologien (insbesondere Profiling) zur Steigerung der Sicherheit bzw. der Prävention von Straftaten gegen das Vermögen der betroffenen Person ermöglichen würde. Art. 24 Abs. 2 lit. h entspricht dem Ausschlussgrund gemäss Art. 14, der für die Information nach Art. 13 und das Auskunftsrecht gemäss Art. 20 gelten soll. Konsequenterweise muss dieser Ausschlussgrund auch als legitimes Interesse des Verantwortlichen gelten, dass von den Datenschutzgrundsätzen (Art. 4 bzw. Art. 23 Abs. 2 lit. a) abweichende Bearbeitungen rechtfertigen kann. **Formulierungsvorschlag** 2 Ein überwiegendes Interesse der bearbeitenden Person ist ~~möglicherweise~~ gegeben, wenn diese insbesondere: a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner oder andere Personen in deren Interesse der Vertrag abgeschlossen wurde, bearbeitet; c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn: 1. ~~es sich dabei nicht um besonders schützenswerte Personendaten handelt,~~

					g. die Daten zur Erhöhung der Sicherheit und Vermeidung von erheblichen Nachteilen für die betroffene Person bearbeitet werden, wofür sie auch Profiling durchführen kann. Personendaten zur Feststellung, Ausübung, Durchsetzung oder Verteidigung von Rechtsansprüchen bearbeitet.
UBS AG	VE-DSG	37ff.			**Art. 37 ff. – im Allgemeinen** Das System des geltenden DSG hat sich bewährt. Sachverhaltsabklärungen, Empfehlungen des EDÖB und Klagen beim Bundesverwaltungsgericht sowie Bundesgericht stellen eine ausgewogene Mischung aus effektiven Behörden- sowie Gerichtsverfahren sowie rechtsstaatlichen „Checks and Balances“ dar. Die bisherige Erfahrung zeigt, dass für eine Abkehr von diesem System keine Notwendigkeit existiert. Sollte am vorgeschlagenen Konzept zur Organisation des EDÖB im Grundsatz festgehalten werden, schlagen wir folgende Anpassungen vor:
UBS AG	VE-DSG	41			**Begründung** Die Einschränkung des geltenden DSG, wonach der EDÖB nur dann eine Untersuchung von sich aus durchführen kann, wenn eine grössere Zahl von Personen betroffen ist, müsste in Art. 41 Abs. 1 wiederaufgenommen werden. Das Verfahren vor dem Beauftragten ist ein öffentlich-rechtliches; es ist daher auch nicht geeignet und auch nicht dazu vorgesehen, um Ansprüche aus der Persönlichkeitsverletzung geltend zu machen. Dafür muss der zivilrechtliche Weg beschritten werden. Folglich ist es auch nicht sachgerecht, dass jede Datenschutzverletzung untersucht wird. Dies würde sowohl beim EDÖB als auch beim Untersuchten unnötig wertvolle Ressourcen binden. Im Sinne der Verhältnismässigkeit sollte daher eine Untersuchung nur in schweren Fällen stattfinden. Sodann sind die Zwangsmassnahmen gemäss Art. 41 Abs. 3 nicht zu rechtfertigen. Diese führen ausserdem zu Kompetenzkonflikten, wenn gleichzeitig eine Strafuntersuchung stattfindet. Aus der Sicht der Verhältnismässigkeit, sollten daher nur derjenige über Zwangsmittel greifen, die im Strafverfahren vorgesehen sind. Im Übrigen unterscheidet sich die Untersuchung gemäss DSG genau darin von jener gemäss KG. Im Kartellrecht ist es die Verwaltungsbehörde, welche das "Strafverfahren" führt und die Sanktionen ausspricht. Im reinen Verwaltungsverfahren besteht aber für spezialgesetzliche

					Untersuchungsbefugnisse kein Raum. Es ist ferner nicht einzusehen, weshalb für das Verfahren beim EDÖB nicht einfach wie im Verwaltungsrecht üblich, das VwVG anwendbar sein soll, wie das in Art. 44 ohnehin vorgesehen ist. **Formulierungsvorschlag** [1]Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen**,** dass eine Datenbearbeitung ~~gegen die Datenschutzvorschriften verstossen~~ die Persönlichkeit einer grösseren Anzahl von Personen verletzen könnte (Systemfehler). [3] streichen
UBS AG	VE-DSG	42			**Begründung** Diese Bestimmungen sind ersatzlos zu streichen. Die geltende Regelung, wonach der EDÖB beim Bundesverwaltungsgericht eine entsprechende Massnahme beantragen musste, hat sich bewährt und sollte nicht ohne Not geändert werden. Auch hier besteht kein Erfordernis über die allgemeinen Regeln des VwVG hinauszugehen. Zudem bleibt hier auch zu erwähnen, dass die betroffenen Personen auch auf zivilprozessualem Weg die Möglichkeit haben entsprechende Massnahmen einzuleiten (Vgl Art. 28 ff. ZGB). **Formulierungsvorschlag** Streichen
UBS AG	VE-DSG	44	3		Aufgrund des in Art. 44 Abs. 3 vorgesehenen Entzugs der aufschiebenden Wirkung hat das vorgeschlagene System für das betroffene Unternehmen weitreichende Folgen; möglicherweise auch erhebliche Wettbewerbsnachteile im Verhältnis zu direkten Konkurrenten. **Formulierungsvorschlag** Streichen

UBS AG	VE-DSG	50 ff.			**<u>Begründung</u>** Rechtsnatur, Konzept und Durchsetzung des Sanktionenregimes des VE DSG geht über die ERK 108 sowie über die DSGVO hinaus. Das vorgeschlagene System ist aus verschiedener Hinsicht zu überdenken: • Grundsätzlich stellt sich die Frage, ob die mit Strafe bedrohten Sachverhalte überhaupt strafwürdig sind. Unserer Ansicht nach ist dies zu verneinen. • Dies gilt nicht nur, aber ganz besonders auch für die fahrlässige Tatvariante. Hier genügen die bestehenden Mechanismen, welche einer Persönlichkeitsverletzung entgegengehalten werden können. • Aufgrund der Masse der Daten, die schon nur aufgrund gesetzlicher Pflichten bearbeitet werden müssen, lassen sich insbesondere bei grossen Unternehmungen einzelne Pflichtverletzungen kaum verhindern. Müsste jedes Mal der Strafrichter angerufen werden, wäre dies völlig unverhältnismässig. • Offensichtlich unverhältnismässig erscheint uns die persönliche Strafbarkeit von Mitarbeitern (insbesondere bei fahrlässiger Begehung). Dies ist angesichts des massiv erweiterten Tatbestandes äusserst problematisch. • Jeglicher Umgang mit Personendaten wäre potentiell immer strafrechtlich relevant. Dies würde einen ganz erheblichen Eingriff in übliche Arbeitsprozesse im Arbeitsalltag darstellen, welche nicht mehr bewältigt werden könnten. Sämtliche an einer Datenbearbeitung beteiligten Mitarbeitenden würden potentiell pauschal kriminalisiert und dadurch in ihrer beruflichen sowie gesellschaftlichen Existenz bedroht. Dies würde gerade in Dienstleistungsbetrieben praktisch eine hohe Anzahl an Mitarbeiter betreffen. • Es ist fraglich, wie sich diese Meldepflicht mit dem *nemo tenetur* Grundsatz verträgt. Es kann nicht angehen, dass Unternehmen einer uneingeschränkten Meldepflicht gegenüber dem Beauftragten unterliegen und damit gleichzeitig dem Staatsanwalt für dessen Verfahren gegen das Unternehmen oder dessen Mitarbeiter die Fakten liefern würden. Für Informationen, die im Rahmen der Mitwirkungspflicht bei Untersuchungen des Beauftragten geliefert werden, müsste deshalb eine Verwendungsbeschränkung gelten. Sie dürften nicht in Strafverfahren gegen das Unternehmen oder deren Mitarbeiter oder in Schadenersatz- oder ähnlichen Zivilprozessen mutmasslich geschädigter

					Personen gegen das Unternehmen verwendet werden. • Überdies unterläge die Verfolgung und Beurteilung der nach Art. 50 ff. VE DSG strafbaren Handlungen den Staatsanwaltschaften der Kantone. Wie und ob sich dabei innert nützlicher Frist eine schweizweit einheitliche Praxis entwickeln kann, an denen sich die Unternehmen orientieren können, ist höchst fraglich. • Besonders stossend ist der Umstand, dass aus objektiver Sicht untergeordnete Dokumentations- sowie Meldepflichten mit beispielloser Härte geahndet würden. • Unverständlich und für die Angleichung an das EU-Recht nicht notwendig ist sodann die Verschärfung und Ausweitung des Tatbestands der Verletzung der beruflichen Schweigepflicht (Art. 52). Für den Fall, dass im Hinblick auf die Adäquanzerklärung der Datenschutzgesetzgebung durch die EU ein gewisser Sanktionsmechanismus als notwendig erachtet werden sollte, schlagen wir vor die Strafbestimmungen wie folgt zu überarbeiten: • **Reduktion des Straftatbestandes auf die heute geltende Vorschrift von Art. 34.** • Falls dennoch am Ausbau der Sanktionen festgehalten wird, sollte zumindest folgendes beachtet werden: ○ **Streichen der persönlichen Strafbarkeit von Mitarbeitern von Unternehmen und** ○ **Streichen der fahrlässigen Tatvariante und Strafbarkeit nur bei direktem Vorsatz (wider besseres Wissen)** Schliesslich stellt das Sanktionenregime des VE DSG ein gravierendes Hindernis auf dem Weg zum angestrebten Angemessenheitsentscheid der EU-Kommission dar: Damit der vorgenannte Entscheid positiv ausfällt, müssen Sanktionen wegen Verstössen gegen die DSGVO auch in der Schweiz vollstreckt werden können. Damit hierfür der ordentliche Amts- bzw. Rechtshilfeweg beschritten werden kann, muss die Voraussetzung der sog. doppelten Strafbarkeit erfüllt werden können. Wir könnten uns daher unter bestimmten Voraussetzungen auch ein verwaltungsrechtliches Sanktionensystem vorstellen, wie dies von der economiesuisse vorgeschlagen wird, allerdings nur mit einem klar begrenzten und verhältnismässigen Strafmass und ohne die Kompetenz beim EDÖB für Zwangsmassnahmen. Dies erscheint besonders wichtig, um weiterhin ein vertrauensvolles Verhältnis zwischen EDÖB und den betroffenen Unternehmen zu

					gewährleisten. Die Möglichkeit Zwangsmassnahmen anzuordnen und schliesslich solche durchzuführen würde dieses Vertrauensverhältnis und eine gute Zusammenarbeit zerstören. Ebenso könnten überbordende Sanktionskompetenzen dieses Verhältnis massiv beeinträchtigen, was kaum im Interesse der Datenschutzgesetzgebung und der betroffenen Personen sein kann.
UBS AG	DSG	59			**Begründung** Die Übergangsbestimmungen beschränken sich auf die Regelungen von Art. 16, 18 und 19. In Tat und Wahrheit lässt sich der mit zahlreichen veränderten bzw. neuen Pflichten ausgestattete VE-DSG nur im Zuge einer umfassenden IT-gestützten Umstellung der gesamten internen Datenbearbeitungsprozesse bewerkstelligen. Dies geht weit über Art. 16, 18 und 19 VE-DSG hinaus und umfasst sämtliche geänderten oder neuen Pflichten und andern zur Strukturierung der rechtskonformen Datenbearbeitung notwendigen Regeln. Mit Blick auf die Komplexität des neuen VE-DSG erachten wir eine Umsetzungsfrist von mindestens 3 Jahren als absolut zwingend. **Formulierungsvorschlag:** Die Übergangsfrist für das ~~Zwei Jahre nach~~ Inkrafttreten dieses Gesetzes beträgt 3 Jahre. ~~a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen;~~ ~~b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.~~
UBS AG	GwG	34 & 34bis (neu)			Wir unterstützen ausdrücklich die entsprechenden Vorschläge der SBVg.

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

(vorab per Email in Word- und PDF-Fassung an: jonas.amstutz@bj.admin.ch)

Wallisellen, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Frau Bundesrätin

Am 21. Dezember 2016 wurden interessierte Kreise eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. UPC Schweiz GmbH nimmt diese Gelegenheit der Meinungsäusserung gerne wahr.

Unsere Stellungnahme, für welche wir das vom EJPD zur Verfügung gestellte Formular verwendet haben, finden Sie im Anhang. Sie enthält in einem ersten Teil generelle Anregungen zum Vorentwurf und geht dann in der Folge im Detail auf die einzelnen Bestimmungen ein. Bestimmungen, zu denen wir keine Bemerkungen resp. Anträge haben, wurden bewusst weggelassen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

Nadine Zollinger
Vice President Legal & Regulatory

Liliane Ackle
Regulatory Affairs Specialist

Anhang: erwähnt

UPC Schweiz GmbH
Richtiplatz 5
8304 Wallisellen
+41 58 388 91 11
upc.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : UPC Schweiz GmbH

Abkürzung der Firma / Organisation : UPC

Adresse : Richtiplatz 5, 8304 Wallisellen

Kontaktperson : Liliane Ackle, Regulatory Affairs Specialist, Abteilung Legal & Regulatory

Telefon : 058 388 91 13

E-Mail : liliane.ackle@upc.ch

Datum : 4.4.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
UPC	**Erhöhter administrativer und finanzieller Aufwand auf Seiten der Verantwortlichen:** Generell kann festgehalten werden, dass die neuen Bestimmungen praktisch einheitlich zu einem vermehrten administrativen und somit auch finanziellen Aufwand auf Seiten des Verantwortlichen führen werden (erweiterte Informationspflicht, Datenschutz-Folgenabschätzung, Dokumentationspflicht etc.). Insbesondere hinsichtlich der erweiterten Informationspflicht plädieren wir für die Akzeptanz pragmatischer Lösungsansätze, mit welchen sich die Informationspflicht dennoch mit dem Tagesgeschäft von Unternehmen vereinbaren liessen. Hierbei denken wir in erster Linie an das Zugänglichmachen der Informationen in den Allgemeinen Geschäftsbedingungen oder via Webseiten des Datenbearbeiters, anstelle einer aktiven Kommunikation gegenüber des Datensubjekts.
UPC	**Gleichwertiges Datenschutz-Niveau in der Schweiz und der EU:** Ein erleichterter Datenverkehr zwischen Ländern, welcher insbesondere durch die Anerkennung eines gleichwertigen Datenschutzes unter den Ländern erreicht wird, ist im Interessen der Unternehmen. Da insbesondere der freie Datenverkehr mit der EU für die Schweizer Wirtschaft von zentraler Bedeutung ist, soll die Schweiz ein mit der EU vergleichbares Datenschutz-Niveau ausweisen können. Vor diesem Hintergrund ist die Entwicklung des Datenschutzes in der EU mitunter ein Grund für die Revision des DSG, dies hält übrigens auch der Erläuterungsbericht des EJPD/BJ fest: die Revision des DSG soll die Datenschutzgesetzgebung den Anforderungen der Verordnung (EU) 2016/679 annähern: Die Annäherung an die Verordnung (EU) 2016/679, zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108, würden die Voraussetzung bilden, dass die Europäische Kommission die Schweiz weiterhin als ein Land mit einem angemessenen Datenschutzniveau einstuft.[1] Wir möchten hierzu jedoch festhalten, dass zur Erreichung eines vergleichbaren Datenschutzniveaus keine buchstabengetreue Umsetzung der EU-Datenschutzgrundverordnung (Verordnung (EU) 216/679, in der Folge auch DSGVO) in Schweizerisches Recht nötig ist. Dies sollte bei der Ausgestaltung der Schweizerischen Bestimmungen beachtet werden. Bei der jetzigen Ausgestaltung des Vorentwurfs fällt auf, dass die Bestimmungen in vielen Fällen über das Schutzniveau der EU hinausgeht. Dies betrifft unter anderem die Informationsplichten gegenüber

[1] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 5.

	betroffenen Personen (vgl. Bemerkungen zu Art. 13 Abs. 3 und 4 VE-DSG), die Informationsplichten gegenüber des Datenschutzbeauftragten über Datenschutz-Folgenabschätzungen (vgl. Bemerkungen zu Art. 16 Abs. 3 VE-DSG), die Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge (vgl. Bemerkungen zu Art. 19 lit. a VE-DSG) sowie die Information betroffener Personen bei aufgrund von Datenbearbeitungen getroffener Entscheidungen (vgl. Bemerkungen zu Art. 20 Abs. 3 VE-DSG).
UPC	**Keine Doppelspurigkeiten bei der Aufsicht:** Schweizer Unternehmen, die eine Tätigkeit in der Europäischen Union ausüben, unterstehen auf der Grundlage von Art. 3 DSGVO i.V.m. Art. 55 Abs. 1 DSGVO auch der Aufsicht der nationalen Datenschutzbehörden. Diese Doppelaufsicht bringt einerseits zahlreiche Rechtsunsicherheiten mit sich und andererseits verursacht sie eine massive administrative Zusatzbelastung der Schweizer Unternehmen. Es ist mit der Europäischen Union eine Gleichbehandlung auszuhandeln, damit die Schweizer Datenschutzaufsicht gegenseitig in das Konzept des „One-Stop-Shop“ nach Art. 56 DSGVO einbezogen werden kann. Heute steht diese für Unternehmen ausserhalb der EU nicht zur Verfügung.
UPC	**Fehlende verfassungskonforme Regulierungskosten Folgeabschätzung (RFA):** Die Bundesverfassung verpflichtet in Art. 170 die Bundesversammlung, die Massnahmen des Bundes auf ihre Wirksamkeit zu prüfen („Die Bundesversammlung sorgt dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden.“). Nach Art. 141 Abs. 2 Bst. f) ParlG müssen in der Botschaft an das Parlament eine Kosten-Nutzen Abschätzung sowie nach Bst. g) die Folgen für die Wirtschaft und die Gesellschaft erläutert werden. Auf Seite 23 des Erläuterungsberichts zum VE-DSG werden die Regulierungskosten als unbedeutend eingestuft. **Diese Einschätzung ist falsch**. Alle Unternehmen bearbeiten heute in zunehmendem und komplexem Mass Personendaten bzw. Rohdaten für Persönlichkeitsprofile und sind damit von den Bestimmungen direkt betroffen. **Die Regulierungskosten sind für alle Unternehmen massiv höher als beschrieben!**
UPC	**Mängel der Regulierungsfolgenabschätzung (RFA):** Die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG wirft sowohl in Bezug auf die Quantität der Befragungen wie auch in Bezug auf die Qualität Fragen auf. Die Studienverfasser selbst äussern sich dazu wie folgt: „Die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten waren sowohl in Bezug auf Quantität als auch Qualität unzureichend; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands.“[2]

[2] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 8.

	„Die Quantität und die Qualität des Rücklaufs aus der Unternehmensbefragung ermöglichte es nicht, in repräsentativer Weise eine Hochrechnung zur Schätzung der finanziellen Auswirkungen zu erstellen." [3] Es erstaunt deshalb, dass das EJPD im Erläuterungsbericht zum Schluss kommt, die zu erwartenden Regulierungskostenfolgen seien unbedeutend. Im Bericht wird lediglich angegeben, dass die fehlenden statistischen Erhebungen durch Gespräche mit Fachpersonen ausgeglichen worden sind. Auch das ist falsch: Uns ist bekannt, dass es sich dabei um ein dreistündiges Gespräch vom 4. Mai 2016 mit neun Fachpersonen handelte, wo auch ein Vertreter von UPC anwesend war. Die anwesenden Vertreter haben bei der mündlichen Erörterung der Fragen wiederholt darauf hingewiesen, dass eine verbindliche Beurteilung der „statistischen" Ergebnisse aufgrund der unzureichenden Quantität und Qualität der Umfrageergebnisse absolut unmöglich sei. Die kritischen Aussagen der angeblich befragten Fachpersonen sind im Bericht heute mit keinem Wort erwähnt. Wir sind der Meinung, dass damit die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt wurde. Das ist für einen Vorentwurf von derartiger wirtschaftlicher Tragweite nicht akzeptabel und wir behalten uns diesbezüglich alle rechtlichen Massnahmen ausdrücklich vor, sollte dieser Umstand im Zuge der Abwicklung des weiteren Gesetzesprojekts keine Beachtung finden.
UPC	**Methodisch fehlerhafte Durchführung der Regulierungsfolgeabschätzung:** Die Einteilung der Unternehmen in drei Kategorien scheint völlig willkürlich und basiert nicht auf der tatsächlichen Betroffenheit. So werden zum Beispiel die Mehrheit der gewerblichen KMU-Betriebe (wie Metzgerei, Schreinerei, Papeterie, Spenglerei, Elektriker, lokale Transporteure, Baubetriebe, Bauernbetriebe, Velomechaniker, Coiffeur etc.) in das Segment A als Unternehmen mit geringer datenschutzrechtlicher Exponierung und keinem oder geringem Einsatz von Web-IT-Technologien eingeteilt. Dabei wird verkannt, dass heute – und vor allem in Zukunft – jedes Unternehmen moderne Informatikmittel einsetzt, eine Internetseite und Social Media-Profile betreibt und damit Personendaten bearbeitet.
UPC	**Falsche Angaben zur Regulierungsfolgenabschätzung im VE-DSG:** Die Folgekosten für die Wirtschaft werden überhaupt nicht quantifiziert. Im Erläuterungsbericht wird festgehalten, dass die Analyseergebnisse zeigen würden, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen nur geringfügig betroffen seien und die Auswirkungen der Revision auf diese Unternehmen somit verhältnismässig gering seien.[4] Wir verweisen in diesem Zusammenhang auf die Kostenschätzungen auf S. 27 ff. der RFA DSG[5], welche den Umsetzungsaufwand der im VE-DSG vorgesehenen Massnahmen aufzeigen.

[3] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.
[4] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 23.
[5] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 27 ff.

UPC	**Forderungen grundsätzlicher Natur:** - Eine klare Regelung der Einwilligung und eine gesetzliche Vermutung der Einwilligung bei definierten Vorgängen, wie zum Beispiel einem Vertragsverhältnis würden den Unternehmen wesentlich mehr Rechtssicherheit und weniger administrativen Aufwand bringen. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten. - Auf die unüberschaubare Menge von Informations- und Dokumentationspflichten der Unternehmen sowie der rein administrativen Meldungen an den Beauftragten ist grundsätzlich zu verzichten. Hingegen sollten Unternehmen vom Beauftragten innerhalb von 30 Tagen eine verbindliche Beurteilung einer Datenbearbeitung verlangen können (Negativattest, *Comfort Letter* oder dergleichen). - Auf eine Ausweitung des Strafenkatalogs ist zu verzichten. Insbesondere sind nur materielle Datenschutzverletzungen zu sanktionieren und keinesfalls Verletzungen von Dokumentations- oder Meldepflichten an den Beauftragten. Es bestehen heute genügend Möglichkeiten bei tatsächlichen Verstössen, Sanktionen gegen fehlbare Unternehmen zu verhängen. Der Verweis auf das Persönlichkeitsrecht für Ansprüche von betroffenen Personen hat sich ebenfalls bewährt und muss nicht geändert werden.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
UPC	VE-DSG	3		c	Der Begriff „besonders schützenswerte Personendaten“ wird auf „biometrische Daten“ (Ziffer 4) ausgeweitet. **Antrag zu Art. 3 lit. c Ziff. 4:** Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Der im Erläuterungsbericht enthaltene Hinweis[6], wann auch Fotos als biometrische Personendaten gelten, ist unverständlich. Es ist klarzustellen, wann Fotos als Personendaten gelten; dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biometrische Daten gelten.
UPC	VE-DSG	3		d	Die Definition des Bearbeitens wurde mit den Bezeichnungen des „Speichern“ und des „Löschen“ ergänzt. Da es sich hierbei um eine Annäherung an den Wortlaut gemäss E-SEV 108 und der Richtlinie (EU) 2016/680 handelt, ist diese Ergänzung zu begrüssen.
UPC	VE-DSG	3		f	Der Begriff „Persönlichkeitsprofil“, welcher eine Besonderheit der Schweizerischen Gesetzgebung darstellt, wird mit dem Begriff „Profiling“ ersetzt. Der Begriff des „Profiling“ ist zu unbestimmt und gefährdet damit die Rechtssicherheit mit nicht ermittelbaren Kostenfolgen für die gesamtschweizerische Wirtschaft. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem „Persönlichkeitsprofil“ des geltenden Rechts abzulehnen. Kommt hinzu, dass die nicht reflektierte Übernahme von Begriffen des ausländischen Rechts dazu führt, dass sich die Anwendung und Auslegung von Schweizer Recht zukünftig an der ausländischen

[6] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 43.

					Rechtsprechung orientieren wird. Dies ist in diesem konkreten Beispiel auch deshalb zu vermeiden, weil der Begriff des „Profiling" im Vorentwurf im Vergleich zur DSGVO sogar noch ausgeweitet wird. Die DSGVO wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE-DSG auf jede Bearbeitungsweise. **Antrag zur Art. 3 lit. f:** Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes „Daten". Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um „Personendaten". Andere Daten werden gemäss Erläuterungsbericht durch den Begriff „Personendaten" konsumiert. *„~~Profiling~~* ***Persönlichkeitsprofil****: jede Auswertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre, oder Mobilität;"*
UPC	VE-DSG	3		h/i	Art. 3 lit. h und lit. i VE-DSG führen neu die Begriffe des „Verantwortlichen" (lit. h) und des „Auftragsbearbeiters" (lit. i) ein. Beim Verantwortlichen handelt es sich gemäss Erläuterungsbricht um die private Person oder das Bundesorgan, die oder das über den Zweck, die Mittel und den Umfang der Bearbeitung der Daten entscheidet. Dabei müssen zwei Kriterien kumulativ erfüllt sein: Die private Person oder das Bundesorgan muss zum einen festlegen, zu welchen Zwecken die Daten bearbeitet werden, zum anderen muss diese resp. dieses darüber bestimmen, mit welchen Mitteln dies erfolgt.[7] Mit der Einführung und Definition dieser neuen Begriffe entfällt das Konzept des „Inhabers einer Datensammlung" (Art. 3 lit. i DSG). Der Begriff des Inhabers der Datensammlung setzte die zweite Bedingung (Bestimmung, mit welchen Mitteln die Bearbeitung erfolgt) nicht voraus. Beim Auftragsbearbeiter handelt es sich gemäss Erläuterungsbericht um die private Person oder das Bundesorgan, die oder das im Auftrag des Verantwortlichen Daten bearbeitet. Der Vertrag zwischen dem Verantwortlichen und dem Auftragsbearbeiter kann unterschiedlicher Art sein (Auftrag, Werkvertrag

[7] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 44/45.

					oder gemischter Vertrag). Ein Arbeitnehmer mit einem Arbeitsvertrag ist gegenüber seinem Arbeitgeber aber kein Auftragsbearbeiter.[8] Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsberarbeiter" ist verschwommen und führt zu einer unklaren – teilweise unsinnigen – Aufteilung der Verantwortung und zu Doppelspurigkeiten. Zudem wird übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen kann. Laut Art. 16, 18 und 19 VE-DSG wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für wen?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den Verantwortlichen?) geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den Verantwortlichen?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht. **Antrag zu Art. 3 lit. h und i:** Beibehaltung der bisherigen Terminologie („Inhaber der Datensammlung“ und „Datensammlung“), *eventualiter* zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. **Generelle Bemerkung:** Dass „Arbeitnehmer mit einem Arbeitsvertrag“ nicht unter den Begriff des "Auftragsbearbeiters" fallen, steht zwar im Erläuterungsbericht. In Anbetracht der merkwürdigen Formulierung „Arbeitnehmer mit Arbeitsvertrag“ wäre es aber dringend nötig, dies klar und deutlich im Gesetzestext zu normieren (Simpler Vorschlag: „Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter“).
UPC	VE-DSG	4	2		Art. 4 Abs. 2 VE-DSG besagt, dass die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen hat und verhältnismässig sein muss. **Antrag zu Art. 4 Abs. 2:** In Absatz 2 ist zu ergänzen, dass nicht nur die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und verhältnismässig zu sein hat, sondern auch die Ausübung anderer Rechte und Pflichten

[8] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 45.

					gemäss diesem Gesetz: *„Die Bearbeitung der Personendaten **sowie jegliche Ausübung anderer Rechte und Pflichten gemäss diesem Gesetz haben** nach Treu und Glauben zu erfolgen und müssen verhältnismässig sein.“*
UPC	VE-DSG	4	3		Art. 4 Abs. 3 VE-DSG besagt, dass Personendaten nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden dürfen. Das Wort „klar“ ist überflüssig und schafft Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Der Erläuterungsbericht argumentiert, es sei mit der redaktionellen keine materielle Änderung beabsichtigt.[9] Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann in der Praxis eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. **Antrag zu Art. 4 Abs. 3:** Streichen des Wortes „klar“: *„Personendaten dürfen nur zu einem bestimmten und für die betroffene Person ~~klar~~ erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.“*
UPC	VE-DSG	4	4		Gemäss Art. 4 Abs. 4 VE-DSG dürfen Personendaten nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person erlaubt, als dies für den Zweck ihrer Bearbeitung erforderlich ist. Die Dauer der Bearbeitung/Aufbewahrung bestimmt sich bereits aus dem Grundsatz der Verhältnismässigkeit (vgl. Art. 4 Abs. 2 VE-DSG). **Antrag zu Art. 4 Abs. 4:** Streichen.

[9] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 46.

UPC	VE-DSG	4	5		Art. 4 Abs. 5 VE-DSG regelt den Grundsatz der Richtigkeit der Daten. Gemäss Erläuterungsbericht ist keine materielle Änderung beabsichtigt.[10] Ein Vergleich mit dem derzeit geltenden Art. 5 Abs. 1 DSG jedoch ergibt, dass darin keine Nachführung vorgesehen ist. Eine solche Nachführung, wie sie nun in Art. 4 Abs. 5 VE-DSG gefordert wird, ist nicht erfüllbar. Bekanntlich fängt die "Bearbeitung" schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE-DSG). Weiter ist es auch nicht möglich, allen künftigen Veränderungen des Status einer Person nachzugehen, über die in einem bestimmten Zeitpunkt Daten bearbeitet wurden, weshalb auch das „unvollständig“ gestrichen werden sollte. **Antrag zu Art. 4 Abs. 5:** Beibehaltung des geltenden Art. 5 Abs. 1 DSG. *Eventualiter* ist Abs. 5 wie folgt zu beschränken: *„Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind ~~und wenn nötig nachgeführt wurden.~~ Unrichtige ~~oder unvollständige~~ Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert werden.*"
UPC	VE-DSG	4	6		Art. 4 Abs. 6 hält unter anderem fest, dass für die Bearbeitung von besonders schützenswerten Personendaten und das Profiling die Einwilligung der betroffenen Person ausdrücklich erfolgen muss. Wird unserem Antrag zur Beibehaltung des Begriffs „Persönlichkeitsprofil“ statt gegeben, sollte der Begriff „Profiling“ hier gestrichen werden und sich das Erfordernis der ausdrücklichen Einwilligung auf besonders schützenswerte Personendaten beschränken. **Antrag zu Art. 4 Abs. 6:** Streichen des Begriffs „Profiling“: *„Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich*

[10] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 47.

					sein.
UPC	VE-DSG	5	5		Die Bekanntgabe von Daten in Länder, welche nicht auf der Positivliste des Bundesrates stehen, ist und soll möglich sein, wenn ein geeigneter Schutz anderweitig gewährleistet ist.[11] Wird dieser Schutz aufgrund standardisierter Garantien in Verträgen (Art. 5 Abs. 3 lit. c VE-DSG) oder aufgrund verbindlicher unternehmensinterner Datenschutzvorschriften (Art. 5 Abs. 3 lit. d VE-DSG) gewährleistet, gilt jedoch eine Genehmigungspflicht durch den Beauftragten. Gemäss Art. 5 Abs. 5 VE-DSG teilt der Beauftragte dem Verantwortlichen oder dem Auftragsbearbeiter spätestens 6 Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 lit. c Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 lit. d Ziffer 1 genehmigt sind oder nicht. Die hier vorgesehene 6-monatige Frist erscheint in Anbetracht dessen, dass gerade in Unternehmen die Genehmigung für die finale Ausgestaltung und Implementierung von Projekten wegweisend ist, zu lange und sollte auf längstens 6 Wochen verkürzt werden. Weiter scheint es übertrieben, diese Pflicht dem Auftragsbearbeiter aufzuerlegen, dieser handelt schliesslich nach Weisungen des Verantwortlichen. **Antrag zu Art. 5 Abs. 5: Anpassung** *„Der Beauftragte teilt dem Verantwortlichen ~~oder dem Auftragsbearbeiter~~ spätestens ~~sechs Monate~~* ***sechs Wochen*** *nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Abs. 3 Buchstabe c Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht.“* **Generelle Bemerkung zu Art. 5 Abs. 4 bis 6:** Der Auftragsbearbeiter sollte generell aus diesen Bestimmungen gestrichen werden.

[11] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, 48-51.

UPC	VE-DSG	5	7		Gemäss Art. 5 Abs. 7 VE-DSG erstellt der Bundesrat eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleisten. Heute wird eine Liste solcher Staaten mit der Gewährleistung eines angemessenen Schutzes vom EDÖB geführt. Wenn diese Kompetenz neu dem Bundesrat zugeteilt ist, muss sichergestellt sein, dass – in Hinblick auf die operative Rolle der Bundesrates – die Liste dennoch ausreichend dynamisch ist und regelmässig nachgeführt wird. **Antrag zu Art. 5 Abs. 7:** *„Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet**. Die Liste basiert auf einem kontinuierlichen Staaten-Monitoring und wird quartalsweise aktualisiert.**“*
UPC	VE-DSG	6	2		Art. 6 Abs. 2 VE-DSG besagt, dass der Verantwortliche oder der Auftragsbearbeiter dem Beauftragten mitzuteilen haben, wenn sie Personendaten nach Absatz 1 lit. b, c und d desselbigen Artikels bekannt geben. Diese Meldepflicht scheint unverhältnismässig, insbesondere wenn neben dem Verantwortlichen auch immer noch der Auftragsbearbeiter diese Bekanntgabe melden muss. Es ist in der Doppelnennung nicht klar, wer schlussendlich für die Erfüllung der Meldepflicht verantwortlich ist, was wohl zu einer zweifachen Meldung führen wird. Die Bestimmung ist weiter auch deshalb heikel, weil solche Meldungen z.T. sensible Geschäftsinformationen betreffen (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetzen auch für Dritte einsehbar werden. **Antrag zu Art. 6 Abs. 2:** Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters.
UPC	VE-DSG	7	2		Gemäss Art. 7 Abs. 2 VE-DSG muss der Verantwortliche sich vergewissern, dass der Auftrags-bearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat erhält die Kompetenz, weitere Pflichten des Auftragsbearbeiters zu präzisieren. Die Pflichten des Auftragsbearbeiters ergeben sich aber bereits aus den Pflichten des Verantwortlichen und des zwischen diesem und dem Auftragsbearbeiter abgeschlossenen Vertrages.

					Antrag zu Art. 7 Abs. 2: Streichung der Kompetenz des Bundesrates: *„Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. ~~Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters.~~“*
UPC	VE-DSG	8			Art. 8 Abs. 1 VE-DSG besagt, dass der Beauftragte Empfehlungen der guten Praxis erarbeiten kann, welche die Datenschutzvorschriften konkretisieren. Dabei soll er interessierte Kreise beiziehen und Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen berücksichtigen. Abs. 2 sieht vor, dass der Verantwortliche sowie interessierte Kreise die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten können. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Abs. 3 schliesslich sieht vor, dass die Empfehlungen des Beauftragten resp. die von ihm genehmigten Empfehlungen veröffentlicht werden. Die Empfehlungen der guten Praxis scheinen auf den ersten Blick begrüssenswert. Es ergeben sich jedoch folgende Befürchtungen: Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der von diesem vordefinierten "interessierten Kreise" ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. Es ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen tel quel als Ermessensindikator zugrunde legen werden. Der Beauftragte wird damit im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich faktisch gemäss seinen Eindrücken Recht setzen. Dies wiegt umso schwerer, als der Beauftragte nicht einmal Jurist oder Anwalt sein oder über Erfahrungen in der Unternehmensjurisprudenz verfügen muss. **Antrag zu Art. 8:** Streichen.
UPC	VE-DSG	9			In Art. 9 Abs. 1 VE-DSG erstaunt die Aussage, dass bei Einhaltung der Empfehlungen der guten Praxis des Beauftragten der Verantwortliche davon ausgehen könne, die damit konkretisierten Bestimmungen

					des DSG befolgt zu haben. Dies scheint gewagt, finden sich doch branchen- und unternehmens-spezifische Unterschiede, welche nie alle in Empfehlungen der guten Praxis aufgenommen werden können. In Verbindung mit unserem Antrag zu Art. 8 VE-DSG scheint auch Art. 9 Abs. 2 nicht ausreichend, um verhindern zu können, dass die Empfehlungen der guten Praxis des Beauftragen nicht schleichend als Ermessensindikatoren herbeigezogen werden und somit einen praktisch zwingenden Charakter entwickeln würden. **Antrag zu Art. 9:** Streichen.
UPC	VE-DSG	12			Art. 12 VE-DSG soll die Handhabung von Daten verstorbener Personen regeln. Die Einführung dieser neuen Bestimmung ist auf diverse politische Vorstösse[12] zurückzuführen. Sie gehören unseres Erachtens nicht ins Datenschutzgesetz, sondern sollten im Erbracht geregelt sein. Die dort zu erlassenden datenschutzrechtlichen Bestimmungen sind *lex specialis* zum DSG. Generell ist zu vermerken, dass die Bestimmungen mehr offene Fragen als Klarheit hervorrufen. Gemäss Art. 12 Abs. 1 soll die Einsicht in die Daten der verstorbenen Person gewährt werden, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen. Erfahrungsgemäss fehlen dem Verantwortlichen in der Praxis die Hintergründe, um im einzelnen Fall abschätzen zu können, ob überwiegende Interessen des Ver-storbenen oder von Dritten vorliegen. Weiter ist die Verknüpfung des schutzwürdigen Interesses mit Verwandtschaftsgraden unbegründet und willkürlich. Mit der Regelung von Art. 12 VE-DSG würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwin-gen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären. **Antrag zu Art. 12:** Streichen.

[12] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 10-12.

UPC	**3. Abschnitt:** **Pflichten des Verantwortlichen und des Auftragsbearbeiters**				**Generelle Bemerkungen:** Es fehlt an Übergangsbestimmungen, welche regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE-DSG auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar und führt über Jahre hinweg zu grossen Unsicherheiten in der Praxis. Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention – und nicht die DSGVO – den Massstab für die Angemessenheit des Datenschutzes zu liefern haben.
UPC	VE-DSG	13	1-4		Neu soll der Verantwortliche die betroffene Person gemäss Art. 13 Abs. 1 VE-DSG über die Beschaffung von Personendaten informieren. Dies stellt eine Ausweitung der Informationspflicht dar, gemäss heutigem Recht (Art. 14 DSG) ist die betroffene Person lediglich bei der Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen zu informieren, dies allerdings auch dann, wenn die Daten bei Dritten beschafft werden. Da die neue Informationspflicht jegliche Datenbeschaffung umfasst, stellt dies für Datenbearbeiter eine der wichtigsten Neuerungen des revidierten DSG dar. Gemäss Art. 13 Abs. 2 VE-DSG teilt der Verantwortliche der betroffenen Person diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach dem DSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Zwar werden in lit. a bis c einige konkrete Angaben von notwendigen Informationen gemacht, dennoch bleibt offen, über was genau informiert werden muss. Weiter schreibt Art. 13 Abs. 3 VE-DSG vor, dass bei Bekanntgabe von Personendaten an Dritte, die betroffene Person über die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger informiert werden muss. Art. 13 Abs. 4 VE-DSG schliesslich verlangt, dass wenn die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen wird, der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die bearbeitet werden, mitgeteilt werden müssen. Art. 13 Abs. 1 bis 4 zusammengefasst, sind betroffene Personen in den folgenden Situationen zu

					informieren: - bei der Beschaffung jeglicher Personendaten bei Dritten; - bei der Bekanntgabe von Personendaten an Dritte und - bei der Weitergabe von Personendaten an Auftragsbearbeiter. Es ist davon auszugehen, dass die Umsetzung dieser Bestimmungen in der Praxis zu einer **kontinuierlichen Information betroffener Personen** führen wird. Das Beschaffen von Daten bei Dritten ist insbesondere im Bereich von Marketingkampagnen üblich und erfolgt häufig. Die Ausweitung der Informationspflicht auf sämtliche Personendaten hätte zur Folge, dass bei jeder dieser Datenbeschaffung die betroffene Person informiert werden müsste. Auch ist es in den meisten Unternehmen üblich, gewisse Services an externe Dienstleister auszulagern. Diese Auftragsbearbeiter können je nach Art der Geschäftstätigkeit relativ häufig wechseln. Bei Versand von personalisierten Kundenbriefen beispielsweise müsste also jedes Mal informiert werden, wenn das Informationsmaterial von einer anderen Druckerei gedruckt würde. Weiter ist festzuhalten, dass mit diesen erweiterten Informationspflichten die betroffene Person im Rahmen einer Datenerhebung **doppelt kontaktiert** werden würde: von jenem Verantwortlichen, der die Daten bei Dritten beschafft sowie in der gleichen Sache von jenem Verantwortlichen, der die Daten an den Dritten bekannt gegeben hat. Dies untermauert das Argument, dass diese erweiterten Informationspflichten zu einer Informationsflut gegenüber den betroffenen Personen führt. Schliesslich ist zu bemerken, dass im Rahmen dieser Bestimmungen sämtliche Unternehmen Aufschluss darüber geben müssten, mit welchen Dritten sie für welche Serviceleistungen zusammenarbeiten und von welchen Dritten sie Daten beziehen, was ein Einblick in die Geschäftsgeheimnisse der Unternehmen bedeutet. Die derzeit vorgesehenen Bestimmungen erachten wir aufgrund obenstehender Erläuterungen als unverhältnismässig und nicht zielführend. Eine erweiterte Informationspflicht mit dem Ziel von mehr Transparenz gegenüber der betroffenen Person ist nachvollziehbar, es ist wohl aber auch nicht im Sinne der betroffenen Person, fortlaufend mit Informationen überflutet zu werden. Vielmehr sollten die Mitteilungen nach Art. 13 Abs. 3 und Abs. 4 VE-DSG pauschaler erfolgen können.

					Antrag zu Art. 13 Abs. 3: Dahingehende Anpassung, dass betroffene Personen lediglich über die Kategorien der Empfängerinnen und Empfänger informiert werden müssen. Dies mitunter auch deshalb, weil die derzeitige Formulierung des Entwurfs es offen lässt, in welchen Fällen über die Empfänger konkret und in welchen nur über die Kategorien der Empfänger informiert werden muss: *„Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem ~~die Empfängerinnen und Empfänger oder~~ die Kategorien der Empfängerinnen und Empfänger mit."* **Antrag zu Art. 13 Abs. 4:** Dahingehende Anpassung, dass betroffene Personen nur über die Kategorien der Auftragsbearbeiter und die Kategorien der bearbeiteten Daten informiert werden müssen und nicht über Identität und Kontaktdaten des Auftragsbearbeiters. Zumal diese Bestimmung weiter geht als die EU-Regelungen: *„Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person ~~die Identität und Kontaktdaten des~~ **die Kategorien** der Auftragsbearbeiter~~s~~ sowie die ~~Daten oder~~ Kategorien von Daten, die er bearbeitet, mit."* **Generelle Bemerkung zur Informationspflicht gemäss Art. 13 VE-DSG:** In der Vergangenheit wurde von Seiten EDÖB für eine Lösung plädiert, bei der Unternehmen der in Art. 13 VE-DSG geforderten Informationspflicht nachkommen können, indem sie die entsprechenden Informationen auf ihren Webseiten oder in Allgemeinen Geschäftsbedingungen zugänglich machen. Die Bestimmungen lesen sich nun aber so, dass bei jeder Datenbeschaffung, Datenbekanntgabe und Datenweitervergabe die betroffene Person detailliert informiert werden muss, es sei denn, sie verfüge schon über die entsprechenden Informationen. Die vom EDÖB angetönte Webseiten-Lösung wäre unseres Erachtens zu begrüssen, da sie für interessierte Personen immer noch zielführend ist, jedoch verhindert, dass betroffene Personen permanent mit Informationen zugedeckt werden.
UPC	VE-DSG	13	5		Art. 13 Abs. 5 VE-DSG definiert, dass wenn Personendaten nicht bei der betroffenen Person beschafft werden, die betroffene Person spätestens bei der Speicherung der Daten informiert wird. Falls die Daten nicht gespeichert werden, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.

					Die sich daraus ergebende Informationsflut ist schlicht nicht umsetzbar und zudem unverhältnismässig. Hinzu kommt, dass die Bestimmung weitergeht als die DSGVO, die hinsichtlich des Informationszeitpunkts kulanter ist (1-monatige Frist). Die Transparenzpflicht gemäss Art. 4 VE-DSG bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird. **Antrag zu Art. 13 Abs. 5:** Streichen. *Eventualiter* ist die aktive Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten zu beschränken.
UPC	VE-DSG	14	1		Art. 14 VE-DSG regelt Ausnahmen von der Informationspflicht und Einschränkungen, ist dabei jedoch enger gefasst als die SEV 108. Absatz 1 sollte um den Fall ergänzt werden, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung), in den betroffen Kreisen als bekannt gilt oder aus den Umständen ersichtlich ist. **Antrag zu Art. 14 Abs. 1: Ergänzung** *„Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt,* ***die Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist, in den betroffenen Kreisen als bekannt gilt oder aus den Umständen ersichtlich ist.“***
UPC	VE-DSG	14	2		In Art. 14 Abs. 2 VE-DSG sollte der Ausnahmekatalog um den Fall erweitert werden, dass keine besonders schützenswerten Personendaten bearbeitet werden. Die Bestimmung des VE-DSG entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der hohen Strafen, die der VE-DSG für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden. **Antrag zu Art. 14 Abs. 2: Ergänzung** *„Werden die Personendaten nicht bei der betroffenen Person beschafft, entfällt die Informationspflicht,*

					wenn: ***a. keine besonders schützenswerten Personendaten bearbeitet werden;*** ***b ~~a.~~** *die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder* ***c. ~~b.~~** *die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist."*
UPC	VE-DSG	14	4	a	Gemäss Art. 14 Abs. 4 lit. a VE-DSG kann die Übermittlung von Informationen eingeschränkt, aufgeschoben oder darauf verzichtet werden, wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt. Hier ist das Kriterium der fehlenden Bekanntgabe an Dritte zu streichen, denn somit würde die Weitergabe von Daten innerhalb eines Konzern (der als Dritter gilt) unnötig erschwert. **Antrag zu Art. 14 Abs. 4 lit. a:** *„Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten:* *a. wenn es sich beim Verantwortlichen um eine private Person handelt~~,~~ **und** falls überwiegende Interessen des Verantwortlichen dies erfordern ~~und er die Personendaten nicht Dritten bekannt gibt~~*;"
UPC	VE-DSG	15	1		Gemäss Art. 15 Abs. 1 VE-DSG hat der Verantwortliche die betroffene Person zu informieren, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht und die Entscheidung rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat. Die Begriffe „rechtliche Wirkungen" und „erhebliche Auswirkungen" sind sehr breit und somit unklar gefasst und führen zu Rechtsunsicherheit. **Antrag zu Art. 15 Abs. 1:** Streichen, *eventualiter* ist die Bestimmung um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a DSGVO zu ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss.

					Generelle Bemerkung: Art. 15 VE-DSG erscheint insgesamt als untauglicher Versuch, Konsumenten vor jeder Art automatisiert getroffener Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche“ Auswirkung ist, dürfte letztlich von der Sensibilität des Betroffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte. Art. 22 DSGVO nimmt im Gegensatz zum VE-DSG den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor. Eine von der DSGVO abweichende Regelung wäre demnach zweifellos auch für die Schweiz zulässig. Es ist nicht nachvollziehbar, weshalb hier ein „Swiss Finish“ erfolgt. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung seit der Gründung des Bundesstaates frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Das hat nichts damit zu tun, ob die Grundlage für einen solchen Entscheid aus Papier, aus Menschen oder aus Algorithmen stammt.
UPC	VE-DSG	15	2		Art. 15 Abs. 2 VE-DSG gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern. Hier stellt sich die Frage, ob die sich daraus ergebende Informationspflicht über die für die Einzelentscheidung bearbeiteten Personendaten – wenn nicht ganz gestrichen – nicht auf Fälle beschränkt werden sollte, bei denen die betroffene Person die Angaben erfragt. Gemäss Erläuterungsbericht soll die Informations- und Anhörungspflicht sicherstellen, dass die betroffene Person nicht Entscheidungen unterworfen ist, die ohne menschliches Zutun erfolgen[13]. Weiter soll hiermit vermieden werden, dass die Entscheidung auf falschen Daten beruht und die betroffene Person deswegen einen Nachteil erleidet. Dies alles wäre auch bei Streichung von Art. 15 Abs. 2 gegeben, da betroffenen Personen ohnehin ein Auskunftsrecht bez. über sie bearbeitete Daten zusteht. Weiter sehen auch die EU-Bestimmungen ein solches Recht zur Äusserung zu bearbeiteten Daten in der Regelung zu automatisierten Einzelentscheiden nicht explizit vor.

[13] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 60.

					Antrag zu Art. 15 Abs. 2: Streichen.
UPC	VE-DSG	15	3		Art. 15 Abs. 3 VE-DSG sieht eine Ausnahme der Informations- und Anhörungspflicht vor, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht. Es ist nicht nachvollziehbar, weshalb gerade der Staat automatisierte Entscheidungen ohne Informations- und Anhörungspflicht durchführen darf. **Antrag zu Art. 15 Abs. 3:** Streichen.
UPC	VE-DSG	16			Art. 16 Abs. 1 VE-DSG sieht vor, dass bei einer Datenbearbeitung, welche zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Art. 16 Abs. 2 VE-DSG präzisiert, was diese Datenschutz-Folgenabschätzung enthalten muss: sie soll die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen umschreiben, welche vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern. Art. 16 Abs. 3 VE-DSG sieht weiter vor, dass der Verantwortliche oder der Auftragsbearbeiter den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen zu benachrichtigen hat. Ein erhöhtes Risiko für die Persönlichkeit liegt beispielsweise bereits beim Erstellen eines Profilings oder der Übermittlung von Daten in Drittstaaten ohne angemessenes Schutzniveau vor . Folglich ist die Hürde für das Erstellen einer Datenschutz-Folgenabschätzung in der Praxis schnell erreicht. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschätzungen bei jeder beliebigen Datenbearbeitung vornehmen zu müssen; abgesehen davon muss die Abschätzung ohnehin durchgeführt werden, um herauszufinden, ob die Daten-bearbeitung zu einem erhöhten Risiko für die Persönlichkeit führt. Die Kosten sind angefallen, selbst wenn man zum Schluss käme, dass gar keine Risiken bestehen. Hier wird ein bürokratisches Monstrum freigesetzt, das in der Privatwirtschaft im Ergebnis nichts ausser gigantischen Kosten bringen wird. Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier, Zeit und Geld dafür aufwenden müssen. Denn anders als der Bund, der – wie im vorliegenden Fall – meint, mit wenig Geld eine verfassungskonforme Regulierungskosten-

					folgenabschätzung machen zu können, hat der private Datenbearbeiter mit seiner Existenz gerade zu stehen, wenn er einer solchen Verpflichtung nicht im Sinne des Gesetzes nachkommen sollte. **Antrag zu Art. 16:** Streichen.
UPC	VE-DSG	16	3		Die Pflicht gemäss Art. 16 Abs. 3 VE-DSG, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht gemäss Art. 16 Abs. 4 VE-DSG sind in jedem Fall zu streichen. Die 3 Monatsfrist ist weiter viel zu lang und zeugt nicht von einem Verständnis wirtschaftlicher Prozesse. Wenn es bei solchen Folgeabschätzungen Beanstandungen gibt, dann hat der Beauftragte Einwände innert 7 Tagen zu adressieren, ansonsten Geschäftsprozesse während Monaten blockiert bleiben müssen. Wir weisen dazu auch darauf hin, dass allein die Überprüfung der zu erwartenden Schwemme solcher Meldungen, ein Herr von neuen Beamten erforderlich machen wird, die nichts anderes tun, als solche Folgeabschätzungen zu prüfen. **Antrag zu Art. 16 Abs. 3 und 4:** Streichen.
UPC	VE-DSG	17	1		Gemäss Art. 17 Abs. 1 VE-DSG hat der Verantwortliche dem Beauftragten jede unbefugte Datenbearbeitung oder den Verlust von Daten unverzüglich zu melden, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person. Eine Mitteilung hat gemäss Art. 17 Abs. 2 VE-DSG auch an die betroffene Person zu erfolgen, wenn es zu ihrem Schutz erforderlich ist oder der Beauftragte es vorsieht. Die Meldepflicht umfasst dementsprechend jede Datenbearbeitung, die gegen das DSG verstösst, beispielsweise auch eine Zweckentfremdung oder eine Datenbearbeitung, die nicht den Transparenzansprüchen entspricht. Dies würde in der Praxis zu einer Flut an Meldungen an den Verantwortlichen führen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen,

					gehört zu den zentralen Verfahrensgarantien unseres Rechtsstaates. Es ist nicht zu rechtfertigen, dass diese Garantie gerade im Datenschutzrecht nicht mehr gewährleistet werden soll; dies umso weniger, als der Beauftragte gemäss Art. 45 VE-DSG ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE-DSG Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer Flut von Selbstanzeigen zu rechnen, die erneut nur den Apparat des Beauftragten übermässig aufblähen würde. **Antrag zu Art. 17 Abs. 1 und 2:** Ersatzlos streichen
UPC	VE-DSG	17	3-4		Gemäss Art. 17 Abs. 3 VE-DSG kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten, dies aus den in Art. 14 Abs. 3 und 4 genannten Gründen. Art. 17 Abs. 4 VE-DSG betrifft die Meldung von Verletzungen des Datenschutzes durch den Auftragsbearbeiter. Er soll den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung informieren. **Bemerkung zu Art. 17 Abs. 3 und 4:** Vgl. Antrag zu Art. 14 Abs. 4 **Zusätzliche Bemerkung zu Art. 17 Abs. 4:** Hier erschliesst es sich uns nicht, weshalb sich die Meldepflicht bei Auftragsbearbeitern auf unbefugte Datenbearbeitungen beschränkt, der Verlust von Daten aber nicht erwähnt wird.
UPC	VE-DSG	18			Art. 18 Abs. 1 VE-DSG soll den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen fördern. Abs. 1 verpflichtet Verantwortliche und Auftragsbearbeiter, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. Die Einführung dieser Regelung ist auf deren Bestehen in der E-SEV 108 (Art. 8 Ziffer 3) sowie in der Richtlinie (EU) 2016/680 (Art. 20 Abs. 1) zurückzuführen. Der „Datenschutz durch die Technik“, auch bekannt als das Prinzip des „Privacy by Design“ basiert auf dem Primat, dass sich Technik und Recht

					gegenseitig ergänzen sollen, dabei soll datenschutzfreundliche Technik die Einführung von rechtlichen Regeln reduzieren.[14] Insbesondere sollen dabei die Grundsätze nach Art. 4 VE-DSG umgesetzt und eingehalten werden. Daten sollen beispielsweise in regelmässigen Abständen gelöscht oder standard-mässig anonymisiert werden. Art. 18 Abs. 2 VE-DSG verpflichtet den Verantwortlichen resp. den Auftragsbearbeiter dazu, mittels geeigneter Vorsteinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werde, die für den jeweiligen Verwendungszweck erforderlich sind. Dieser Grundsatz umschreibt den Ansatz „Privacy by Default". Bei Voreinstellungen handelt es sich gemäss Erläuterungsbericht um jene Einstellungen, die standardmässig zur Anwendung kommen, sofern der Nutzer keine abweichende Eingabe macht. Im Zusammenhang mit einer Datenbearbeitung bedeute dies, dass der Bearbeitungsvorgang standardmässig möglichst datenschutzfreundlich eingerichtet ist, ausser der Nutzer würde diese Voreinstellungen ändern[15]. Hinsichtlich dieser Ansätze des „Privacy by Design" und des „Privacy by Default" drängt sich der Hinweis auf, dass diese Regelungen im Grundsatz bereits durch Art. 11 VE-DSG gegeben sind: Der Verantwortliche und der Auftragsbearbeiter haben die Sicherheit der Personendaten zu gewährleisten. Sie schützen diese durch angemessene **technische** und **organisatorische Massnahmen** gegen unbefugtes Bearbeiten und Verlust. Art. 18 Abs. 1 VE-DSG enthält einzig noch die Präzisierung, dass die Massnahmen bereits ab dem Zeitpunkt der Planung der Datenbearbeitung zu treffen sind, was sich jedoch von selbst versteht, wenn die allgemeine Sicherheit der Personendaten von Anfang an bestehen muss. Art. 18 VE-DSG ist deshalb unseres Erachtens redundant, da die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit gemäss Art. 11 VE-DSG Datenbearbeiter bereits dazu verpflichten, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert.

[14] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 63-64.

[15] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 64-65.

					Dies gilt auch für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen. **Antrag zu Art. 18 Abs. 1 und 2:** Streichen.
UPC	VE-DSG	19			Art. 19 lit. a VE-DSG sieht vor, dass der Verantwortliche und der Auftragsbearbeiter ihre Datenbearbeitung dokumentieren müssen. Dadurch werde gemäss Erläuterungsbericht des Bundesrates die bisherige Verpflichtung ersetzt, Datensammlungen beim Beauftragten zu registrieren[16]. Während im derzeitigen Recht für Private diverse Ausnahmen von der Registrierung bestehen, gilt die neu vorgesehene Dokumentationspflicht einheitlich für alle Datenbearbeitungsvorgänge. Dies führt zu einem erweiterten administrativen Aufwand, sowohl auf Seiten der Verantwortlichen wie auch auf Seiten des Beauftragten. Die in Art. 19 lit. b VE-DSG vorgesehene Informationspflicht der Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung ist von vornherein nicht umsetzbar. Teilweise lassen sich dagegen auch absurde Beispiele vorbringen: Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine allfällige Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gemäss Art. 25 machen zu müssen. Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Auch hier gilt es, sich auch in die Situation der Informationsadressaten zu versetzen. Dass Millionen unnützer Mitteilungen versandt werden ist das eine; dass aber jeder Einzelne tausende solcher Informationen von allen Datenbearbeitern erhält, das andere. Diese Informationen sind die neuen „Spam Waves“ und werden bei den Adressaten keinerlei Wirkung erzielen, geschweige denn, diese in ihren Persönlichkeiten schützen. **Antrag zu Art. 19:**

[16] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 68.

					Ersatzlos streichen
UPC	VE-DSG	20	3		Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die Verordnung (EU) 216/679 (Art. 15 Abs. 1 lit. h) wie auch die Richtlinie (EU) 2016/680 sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell. Um die bereits bez. der Ausführungen zu Art. 13 VE-DSG angesprochene Informationsflut gegenüber der betroffenen Person einzudämmen, ist die in Art. 20 VE-DSG vorgesehenen Informationspflicht gegenüber der betroffenen Person bei jeder aufgrund einer Datenbearbeitung getroffenen Entscheidung auf automatisierte Einzelentscheidungen zu reduzieren und Art. 20 Abs. 3 VE-DSG entsprechend zu streichen oder zumindest dahingehend abzuschwächen, dass die Information nur in groben Zügen erfolgen muss und somit keine Offenbarung von Geschäftsgeheimnissen bedingt. **Antrag zur Art. 20 Abs. 3:** Streichen, *eventualiter* ist Art. 20 Abs. 3 auf die Pflicht zu beschränken, den Betroffenen in groben Zügen über den Entscheid informieren zu müssen.
UPC	VE-DSG	23	2	d	Art. 23 Abs. 2 lit. d besagt, eine Persönlichkeitsverletzung liege insbesondere dann vor, wenn ein Profiling ohne ausdrückliche Einwilligung der betroffenen Person erfolgt. **Antrag zu Art. 23 Abs. 2 lit d:** Streichen, zum Profiling vgl. Bemerkungen zu Art. 3 lit. f VE-DSG.
UPC	VE-DSG	24	2		Art. 24 VE-DSG äussert sich zu Rechtfertigungsgründen hinsichtlich Verletzungen der Persönlichkeit und es wird definiert, unter welchen Bedingungen ein überwiegendes Interesse der bearbeitenden Person geltend gemacht werden kann. Die neue Formulierung führt jedoch zu Rechtsunsicherheit. **Antrag zu Art. 24 Abs. 2, erster Satz:** Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text („möglicherweise gegeben“) schafft nur eine zusätzliche Rechtunsicherheit:

					*„Ein überwiegendes Interesse der bearbeitenden Person **wird vermutet** ~~ist möglicherweise gegeben~~, wenn dieser insbesondere:“* **Antrag zu Art. 24 Abs. 2 lit. a:** Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft Abgrenzungsfragen auf, für welche der VE-DSG keine Antworten liefert: „in ~~unmittelbarem~~ Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages Personendaten über ihren Vertragspartner bearbeitet;“
UPC	VE-DSG	28	1-2		Art. 28 VE-DSG regelt die automatisierte Datenbearbeitung im Rahmen von Pilotversuchen durch Bundesorgane. Der Bundesrat erhält die Kompetenz, vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling unter gewissen Voraussetzungen zu bewilligen. Dazu hat er vorgängig die Stellungnahme des Beauftragten einzuholen. **Antrag zu Art. 28 Abs. 1 und 2:** Die Bestimmung entweder streichen, oder die entsprechende Möglichkeiten sind auch Privaten zu eröffnen.
UPC	VE-DSG	37	1		Art. 37 VE-DSG regelt die Ernennung und die Stellung des oder der Öffentlichkeitsbeauftragten. Absatz 1 hält fest, dass der oder die Beauftragte vom Bundesrat für eine Amtsdauer von vier Jahren gewählt wird. Seine resp. ihre Wahl ist durch die Bundesversammlung zu genehmigen. Hier fordern wir, dass dem Bundesrat ein Vorschlagsrecht zukommt, die Wahl jedoch durch das Parlament erfolgt. Es ist nicht ersichtlich, was die blosse Genehmigung einer Wahl bringen soll. In Anbetracht des zukünftig angedachten Gewichts des Postens des oder der Beauftragten – er/sie soll über grosse Kompetenzen und Wirkungsgrad mit erheblichen finanziellen Auswirkungen auf die Schweizer Wirtschaft verfügen – ist eine Wahl durch das Parlament gerechtfertigt. **Antrag zu Art. 37 Abs. 1:** „Die oder der Beauftragte wird vom Bundesrat ~~für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen.~~ **zur Wahl vorgeschlagen und vom Parlament für**

					eine Amtsdauer von vier Jahren gewählt.“
UPC	VE-DSG	37	4		Art. 37 Abs. 4 VE-DSG hält fest, dass der oder die Beauftragte über ein ständiges Sekretariat und ein eigenes Budget verfügt. Sie oder er stellt sein Personal an. **Antrag zu Art. 37 Abs. 4:** Das Budget wird durch das Parlament genehmigt.
UPC	VE-DSG	38	2		Art. 38 VE-DSG regelt die Wiederwahl und Beendigung der Amtsdauer. Abs. 2 besagt, der oder die Beauftragte sei für eine neue Amtsdauer wiedergewählt, es sei denn der Bundesrat verfüge spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl. Das Verfahren über eine Verfügung kommt einem Kündigungsverfahren gleich, das in der Praxis nur aus wichtigen Gründen möglich ist. Das Wahlorgan soll in seiner Wahl aber frei sein. **Antrag zu Art. 38 Abs. 2:** Der oder die Beauftragte ist für jede Amtsperiode neu zu wählen.
UPC	VE-DSG	39	2		Art. 39 Abs. 2 VE-DSG hält fest, der Bundesrat könne dem oder der Beauftragten gestatten, eine Nebenbeschäftigung (nach Abs. 1 desselben Artikels) auszuüben. Dies, wenn dadurch die Ausübung seiner Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden. Für die Vermeidung von Interessenskonflikten ist absolute Transparenz unabdingbar, weshalb solche Bewilligungen offenzulegen sind. **Antrag zu Art. 39 Abs. 2: Ergänzung** *„Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1 auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.* ***Erteilte Bewilligungen sind offenzulegen.“***
UPC	VE-DSG	41	2		Gemäss Art. 41 VE-DSG kann der Beauftragte von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder gegen eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Gemäss Abs. 2 haben das Bundesorgan oder die private Person dem Beauftragten die verlangten Aus-

					künfte zu erteilen und die ihm für die Untersuchung notwendigen Unterlagen zur Verfügung zu stellen. **Antrag zu Art. 41 Abs. 2:** Hier ist zu ergänzen, dass bei Untersuchungen gegen Private alle Untersuchungsakten nicht dem Öffentlichkeitsgesetz unterliegen, da ansonsten über diesen Umweg Betriebsgeheimnisse an Dritte gelangen könnten. Wenn Unternehmen verpflichtet sind, dem Beauftragten alle notwendigen Unterlagen zur Verfügung zu stellen, müssen sie die Garantie haben, dass diese nicht veröffentlicht werden. Der Beauftragte veröffentlicht bei Untersuchungen gegen private Personen nur die Empfehlung. Vgl. hierzu auch Bemerkung zu Art. 44 Abs. 2.
UPC	VE-DSG	41	3		Gemäss Art. 41 Abs. 3 VE-DSG kann der Beauftragte ohne Vorankündigung Räumlichkeiten inspizieren und/oder den Zugang zu allen notwendigen Daten und Informationen verlangen, sollte das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nachkommen. **Antrag zu Art. 41 Abs. 3:** Diese Bestimmung ist nur akzeptabel, wenn das Unternehmen Rechtsmittel gegen die Auskunftsverfügung hat. Eine unbestimmte Verletzung von Mitwirkungspflichten darf nicht zu Strafsanktionen oder publizitätswirksamen Aktionen des Beauftragten gegen Unternehmen führen. Bevor solche Massnahmen ergriffen werden, muss eine Editionsverfügung des Beauftragten einer gerichtlichen Überprüfung zugänglich sein.
UPC	VE-DSG	41	4		Gemäss Art. 41 Abs. 4 VE-DSG darf der Beauftragte ausserhalb von Untersuchungsverfahren überprüfen, ob private Personen/Bundesorgane die Datenschutzvorschriften einhalten und darf sie beraten. Ein Tätigwerden des Beauftragten gegenüber Privaten ohne Anzeige einer Datenschutzverletzung ist strikt abzulehnen. Wenn Anhaltspunkte vorliegen, kann der Beauftragte nach Art. 41 Abs. 1 formell vorgehen. Es dürfen hier keine mehrgleisigen Verfahren ohne Rechtsschutz für die betroffenen Parteien eingefügt werden. Im Gegenteil, es müsste für Unternehmen möglich sein, Sachverhalte rechtsverbindlich durch den Beauftragten überprüfen und mittels Attest der Datenrechtskonformität genehmigen zu lassen. **Antrag zu Art. 41 Abs. 4: Streichen von „private Personen“** *„Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob ~~private Personen oder~~*

					Bundesorgane die Datenschutzvorschriften einhalten und sie beraten."
UPC	VE-DSG	41	5		Art. 41 Abs. 5 VE-DSG hält fest, dass bei Anzeige einer betroffenen Person der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung zu informieren hat. **Antrag zu Art. 41 Abs. 5: Ergänzung resp. Streichung** Die anzeigende Person hat keine Parteistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte Absatz 5 auch gestrichen werden.
UPC	VE-DSG	42	1		Gemäss Art. 42 Abs. 1 VE-DSG kann der Beauftragte vorsorgliche Massnahmen verfügen. **Antrag zu Art. 42 Abs. 1:** Vorsorgliche Massnahmen sind – auch im Persönlichkeitsschutz – immer Sache der Gerichte. Hier ist die bisherige Regelung mit dem Antrag beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts beizubehalten. Es sollte hier nicht von den bewährten rechtsstaatlichen Prozessen abgewichen werden. Jedenfalls gibt es dazu keine ausreichenden Rechtfertigungsgründe. Formulierungsvorschlag: „~~Der Beauftragte kann vorsorgliche Massnahmen verfügen~~ **Der Beauftragte kann beim Bundesverwaltungsgericht vorsorgliche Massnahmen beantragen**, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern."
UPC	VE-DSG	43	1		Art. 43 VE-DSG regelt Verwaltungsmassnahmen. Gemäss Art. 1 kann der Beauftragte bei Verletzung von Datenschutzvorschriften verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden. Anstelle der Empfehlung und des nachfolgenden Gerichtswegs wie im heutigen Recht wird hier auch die Klage- und Beweislast umgekehrt. Das ist abzulehnen. Der Beauftragte hat in der Verfügung die Rechtsverletzung nachzuweisen. **Antrag zu Art. 43 Abs. 1:** Eine Verfügung sollte nur nach der Durchführung einer Untersuchung zulässig sein, in welchem dem betroffenen Datenbearbeiter selbstverständlich auch das rechtliche Gehör gewährt wurde. Eine Datenvernichtung darf nicht durch den Beauftragten angeordnet werden können, da dies nicht wieder

					gutzumachende Folgen hat (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 41 reicht zum Schutz Betroffener völlig aus.
UPC	VE-DSG	44	2		Gemäss Art. 44 Abs. 2 VE-DSG sind in Verfahren lediglich das Bundesorgan oder die private Person Partei. Drittpersonen haben keine Parteistellung und kein Akteneinsichtsrecht, was zu begrüssen ist. **Antrag zu Art. 44 Abs. 2:** Es ist zu ergänzen, dass Untersuchungsunterlagen nicht dem Öffentlichkeitsgesetz unterliegen (vgl. auch Antrag zu Art. 41 Abs. 2 VE-DSG).
UPC	VE-DSG	44	3		Art. 44 Abs. 3 VE-DSG hält fest, dass Beschwerden gegen vorsorgliche Massnahmen nach Art. 42 keine aufschiebende Wirkung zukommt. **Antrag zu Art. 44 Abs. 3:** Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Vielmehr wäre vorzusehen, dass die aufschiebende Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt nicht praktikable Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann indem zulässig beurteilt wird, oder dgl.
UPC	VE-DSG	45			Art. 45 VE-DSG erteilt dem Beauftragten eine Anzeigepflicht. Erfährt er im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit. Ein Recht zur Anzeige würde hier völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE-DSG). **Antrag zu Art. 45 VE-DSG:** Streichen.
UPC	VE-DSG	46	2		Art. 46 VE-DSG regelt die Amtshilfe zwischen schweizerischen Behörden. Abs. 2 hält fest, wem der Beauftragte Informationen und Personendaten bekannt gibt (den für den Datenschutz zuständigen kantonalen Behörden, den zuständigen Strafverfolgungsbehörden, den Bundesbehörden etc.).

					Antrag zu Art. 46 Abs. 2. Hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen.
UPC	VE-DSG	47	1		Art. 47 VE-DSG regelt die Amtshilfe zwischen schweizerischen und ausländischen Behörden. **Antrag zu Art. 47 Abs. 1**. Auch hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen, insbesondere auch für Informationen, die in der Schweiz dem Berufsgeheimnis unterliegen. Die Herausgabe vertraulicher Unternehmensdaten darf nicht im Ermessen des Beauftragten liegen, sondern – wenn überhaupt – nur mit Zustimmung des betroffenen Unternehmens zulässig sein.
UPC	VE-DSG	48	2		Art. 48 VE-DSG hält fest, der Beauftragte erstatte der Bundesversammlung periodisch sowie bei Bedarf Bericht. Gemäss Abs. 2 informiert er in Fällen von allgemeinem Interesse die Öffentlichkeit über seine Feststellungen und Verfügungen. **Antrag zu Art. 48 Abs. 2:** Damit der Beauftragte die Persönlichkeitsrechte wahrt, soll er nur über die Tatsache einer Untersuchung informieren: *„In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über die ~~Feststellungen und Verfügungen~~* ***Untersuchungen****."*
UPC	VE-DSG	49		d	Art. 49 VE-DSG regelt weitere Aufgaben des Beauftragten. Gemäss lit. d erteilt er der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann. Wenn der Beauftragte eine Aufsichtsfunktion inne hat, kann er nicht gleichzeitig eine Konsumentenschutzaufsicht erfüllen. **Antrag zu Art. 49 lit. d:**

					Streichen.
UPC	**8. Abschnitt:** **Strafbestimmungen**				**Generelle Bemerkungen:** Hinsichtlich Strafbestimmungen ging man im Vorfeld der Revision von der Einführung von Verwaltungssanktionen aus. Dies auch mit Blick auf die DSGVO (Art. 83). Art. 50 ff. VE-DSG übernimmt nun aber im Wesentlichen Art. 34 DSG, wobei die maximale Busse von bisher CHF 10‘000 auf CHF 500‘000 angehoben wird und die Bestimmungen auf die neuen Pflichten des Verantwortlichen und des Auftragsbearbeiters ausgeweitet werden. Das gesamte Sanktionssystem ist zu überarbeiten. Es führt zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden und Unternehmen. Unverständlich ist zudem, dass gerade die Verwaltung von den Strafsanktionen ausgenommen werden soll. Es wird komplett vergessen und ausgeblendet, dass vor noch nicht langer Zeit, die Gefahr im Umgang mit Daten nicht von Privaten und nicht von Unternehmen, sondern vom Staat selbst ausgegangen ist (Stichwort: Fichen-Affäre). Es wäre naiv zu glauben, dass sich diese Bedrohung in den letzten 20 Jahren komplett verflüchtigt hätte. Mit einer zunehmend hohen Verwaltungsquote von gegen 40% wäre ein sehr hoher Anteil der Berufstätigen vom Sanktionssystem ausgenommen. Das ist höchst zweifelhaft und politisch nicht zu rechtfertigen. Alternative: Der Beauftragte soll als Aufsichtsbehörde untersuchen und verfügen können. Unternehmen sollen sich in diesem verwaltungsrechtlichen Verfahren wehren können. Erst wenn rechtskräftige Entscheide nicht umgesetzt worden sind, sollten Strafsanktionen greifen. Es besteht kein Rechtfertigungsgrund, von diesem in anderen Belangen des Bundesrechts verankerten Prinzip abzuweichen.
UPC	VE-DSG				Art. 50 VE-DSG regelt Bussen bei Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten. Es sind Bussen von bis zu CHF 500‘000 vorgesehen, wer fahrlässig handelt, wird mit einer Busse von bis zu CHF 250’00 betraft. **Generelle Bemerkung zu Art. 50:** Die Fahrlässigkeit (vgl. Abs. 4) ist von der strafrechtlichen Sanktionierung generell auszunehmen. Der Bussenrahmen ist auf eine maximale Höhe von CHF 5'000.- bzw. – im Wiederholungsfall – auf maximal CHF 10'000.- zu begrenzen. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen anzusetzen, sicher nicht Beträge bis CHF 500'000.-. Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit

					den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.- für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Grössenordnungen. Bussenbeträge über CHF 100'000.- sind bislang in der Schweiz nicht bekannt. Die Erhöhung des Strafrahmens auf CHF 500‘000.- ist daher völlig überrissen und nicht nachvollziehbar.
UPC	VE-DSG	50	1	b	**Antrag zu Art. 50 Abs. 1 lit. b:** Ändern, Art. 13 ist vollständig von der Sanktionierung auszunehmen.
UPC	VE-DSG	50	1	c	**Antrag zu Art. 50 Abs. 1 lit. c:** Streichen. Ist vollständig von der Sanktionierung auszunehmen.
UPC	VE-DSG	50	2	a/b	**Antrag zu Art. 50 Abs. 2, lit. a und b:** Streichen. Da die Meldepflichten sowieso massiv reduziert werden müssen, ist auch diese Bestimmung zu streichen.
UPC	VE-DSG	50	2	e	**Antrag zu Art. 50 Abs. 2, lit. e:** Ändern. Diese Bestimmung ist auf Vorfälle zu beschränken, die schwerwiegend sind und mehr als 1‘000 Personen betreffen.
UPC	VE-DSG	50	2	f	**Antrag zu Art. 50 Abs. 2, lit. f:** Streichen. Hier genügt die bestehende Strafbestimmung im StGB.
UPC	VE-DSG	50	3	a	**Antrag zu Art. 50 Abs. 3, lit. a:** Streichen. Die dem Bst. a zugrundeliegende Bestimmung gemäss Art. 19 Bst. b ist in der Praxis gar nicht umsetzbar. Daher ist auch die Strafbestimmung zu streichen.
UPC	VE-DSG	50	4		**Antrag zu Art. 50 Abs. 4:** Streichen. Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen (vgl. generelle Bemerkung zu Art. 50 VE-DSG).
UPC	VE-DSG	51	1		Art. 51 VE-DSG regelt die Verletzung der Sorgfaltspflichten. Auch hier sind Bussen von bis zu CHF 500‘000 vorgesehen, wer fahrlässig handelt, wird mit einer Busse von bis zu CHF 250’000 betraft. **Generelle Bemerkung zu Art. 51 Abs. 1:** Bei Vorsatz sind Bussen bis CHF 10‘000 angemessen.

UPC	VE-DSG	51	1	a	**Antrag zu Art. 51 Abs. 1 lit. a**: Die Meldepflicht von Art. 6 Abs. 2 ist von der Busse auszunehmen, da ansonsten tausende von KMU unwissentlich kriminalisiert werden.
UPC	VE-DSG	51	1	d	**Antrag zu Art. 51 Abs. 1 lit. d:** Streichen; erst die Folgeabschätzung kann ja zeigen, ob eine Folgeabschätzung notwendig wäre. Die Strafdrohung führt dazu, dass dieses Verfahren für jede Datenbearbeitung durchgeführt werden muss. In der Rechtsfolgeabschätzung werden Kosten von CHF 5‘000 – 30‘000.- pro Durchführung veranschlagt, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU führen würde.
UPC	VE-DSG	51	1	e	**Antrag zu Art. 51 Abs. 1 lit. e:** Streichen; Hier handelt es sich um eine unbestimmte Handlungsdefinition, die dadurch kaum eine Strafbarkeit auslösen kann.
UPC	VE-DSG	51	1	f	**Antrag zu Art. 51 Abs. 1 lit. f:** Streichen; die Strafdrohung führt dazu, dass alle Prozesse für die Datenbearbeitung vorsorglich dokumentiert werden müssen, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU, führen würde. In der RFA wurden diese Kosten nicht erhoben.
UPC	VE-DSG	51	2		**Antrag zu Art. 51 Abs. 2:** Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen.
UPC	VE-DSG	52			Art. 52 VE-DSG regelt die Verletzung der beruflichen Schweigepflicht. Dabei ist eine Ausweitung auf den Begriff „geheime Personendaten“ vorgesehen. **Antrag zu Art. 52 VE-DSG:** Streichen. Der bisherige Art. 35 DSG hat die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten geregelt. Die Ausweitung auf den unbestimmten Begriff „geheime Personendaten“ wird abgelehnt. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Damit würde jeder Bearbeiter von Personendaten einer strafbewehrten Schweigepflicht unterworfen. Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist völlig unverhältnismässig. Eventualiter wäre es sinnvoller, die Strafbarkeit in dieser Bestimmung auf Auftragsbearbeiter und Beauftragte zu beschränken
UPC	VE-DSG	53			Art. 53 VE-DSG regelt Übertretungen in Geschäftsbetrieben. Dabei soll von der Ermittlung der strafbaren Personen Umgang genommen werden, und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse CHF 100‘000 nicht überschreitet. Die

					bestehenden Regelungen im Verwaltungsstrafrecht und im Strafrecht sind ausreichend. **Antrag zu Art. 53:** Streichen.
UPC	VE-DSG	54			Art. 54 VE-DSG hält fest, dass die Verfolgung und Beurteilung den Kantonen obliegt. Die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet werden und ist somit vom Bund zu führen. **Antrag zu Art. 54:** Streichen.
UPC	VE-DSG	55			Bei Übertretungen verjährt die Strafverfolgung gemäss Art. 55 in fünf Jahren, nachdem die Tat begangen wurde. **Antrag zu Art. 55:** Die Verjährungsfrist ist bei 3 anstatt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109) und wäre ausreichend und sachgerecht.
UPC	VE-DSG	59			Zwei Jahre nach Inkrafttreten des revidierten DSG müssen die Verantwortlichen und Auftragsbearbeiter in der Lage sein, eine Datenschutzfolgenabschätzung nach Art. 16 vorzunehmen. Weiter müssen sie für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen gemäss den Artikeln 18 und 19 lit. a treffen. Dies bedeutet, dass die sogenannten Ansätze des *Privacy by Design* und *Privacy by Default* umgesetzt sein müssen. Weiter müssen die Verantwortlichen und Auftragsbearbeiter zwei Jahre nach Inkrafttreten ihrer Dokumentationspflicht nachkommen. Die Umsetzungsfrist für die weiteren Bestimmungen bleibt im jetzigen Vorentwurf undefiniert und wirft Fragen auf. **Antrag zur Art. 59 VE-DSG:** Um Rechtsunsicherheit zu vermeiden, ist eine einheitliche Umsetzungsfirst von 2 Jahren für jegliche Bestimmungen des VE-DSG vorzusehen.

Sammlung Änderungsvorschläge: Aufhebung und Änderung anderer Erlasse	
11. Zivilprozessordnung	**Antrag zu den zivilprozessualen Bestimmungen:** Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Da in Datenschutzfragen der Beauftragte eine Aufsichtsfunktion ausübt, kann er bei Verstössen aktiv werden. Es braucht hier keine weitere soziale Gerichtsbarkeit. Für zivilrechtliche Verfahren genügen die bestehenden Regeln. Das kostenlose Prozessieren könnte hier eine Flut – auch von mutwilligen – Klagen auslösen. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll – wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist – seine Kostenrisiken abwägen müssen, ehe Gerichte bemüht werden.
13. Strafgesetzbuch	**Antrag zu Art. 179novies:** Die Strafbarkeit der Beschaffung ist zu beschränken auf Daten die einem Berufsgeheimnis unterliegen sowie auf besonders schützenswerte Personendaten. Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe zu bestrafen ist unverhältnismässig. Hier reicht eine Geldstrafe.
37. Fernmeldegesetz **vom 30. April 1997**	**Bemerkung zu datenschutzrechtlichen Regulierungen im Fernmeldegesetz:** Es ist klarzustellen, dass datenschutzrechtliche Regulierungen im Fernmeldegesetz und in dessen Ausführungsbestimmungen als lex specialis den allgemeinen Datenschutzbestimmungen des DSG und dessen Ausführungsbestimmungen vorgehen.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
UPC	Keine Bemerkungen.

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
UPC	Keine Bemerkungen.

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
UPC	n/a	Keine Bemerkungen.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
UPC	n/a	Wir weisen darauf hin, dass wir Bemerkungen zum Erläuternden Bericht jeweils direkt bei der Anregung zu den jeweiligen Artikeln einfliessen liessen.

Vereinigung Schweizerischer Assetmanagement- und Vermögensverwaltungsbanken
Association de Banques Suisses de Gestion
Associazione di Banche Svizzere di Gestione Patrimoniale ed Istituzionale
Association of Swiss Asset and Wealth Management Banks

VAV
ABG

Eidgenössisches Justiz- und Polizeidepartement EJPB
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern
per E-Mail an: jonas.amstutz@bj.admin.ch

Zürich, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Besten Dank für die Möglichkeit zur Stellungnahme im Rahmen der Vernehmlassung zur Totalrevision des Bundesgesetzes über den Datenschutz (DSG), von der wir gerne Gebrauch machen.

Die VAV teilt die in den Stellungnahmen von economiesuisse und der Schweizerischen Bankiervereinigung zum Vorentwurf des Bundesgesetzes über die Totalrevision des Datenschutzgesetzes (VE-DSG) vom 16. März 2017 dargestellten Einschätzungen und Kritikpunkte. Wichtig und erhaltenswert ist aus Sicht der VAV, die Gleichwertigkeit und Angemessenheit des schweizerischen Datenschutzniveaus mit demjenigen des europäischen Rechts (z.B. EU-Datenschutz-Grundverordnung (DSGVO), Konvention 108 des Europarates) auch inskünftig zu erhalten und zu modernisieren. Insofern begrüsst die VAV den VE-DSG.

Allerdings sollte dieser nicht in unnötiger Weise und kontraproduktiv über die europäischen Vorgaben hinausgehen. Ein „Swiss Finish“, der insbesondere zu unnötigem administrativem Aufwand für die Wirtschaft führt, ist abzulehnen, zumal eine Verschärfung über den europäischen Mindeststandard einen Wettbewerbs- und Standortnachteil für international tätige Datenbearbeiter in der Schweiz mit sich bringt. Dementsprechend sind Anpassungen an der Vorlage notwendig (insbes. was die Melde-, Genehmigungs- und Informationspflichten der Schweizerischen Unternehmen angeht), damit die Unternehmen das revidierte DSG (bzw. die europäischen datenschutzrechtlichen Mindestanforderungen) in der Praxis entsprechend anwenden bzw. umsetzen können und insgesamt keine Rechtsunsicherheit entsteht. Der dringende Abstimmungsbedarf zwischen der Schweiz und der EU (vgl. auch Motion « Gegen Doppelspurigkeiten im Datenschutz - Motion Fiala, 16.3752) ist auch daher notwendig, da die DSGVO keine klaren Regeln betreffend Gültigkeit für Unternehmen ausserhalb des Territoriums der EU enthält. Hier besteht insbesondere das Risiko für Schweizer Unternehmen, sich nach der Schweizerischen Rechtsordnung strafbar zu machen (vgl. z.B. Art. 271 StGB).

Im Lichte dieser grundsätzlichen Überlegungen möchten wir einige konkrete Punkte hervorheben:

1) Der Vorentwurf sieht weite Informations- und Meldepflichten vor, die für die Unternehmen einen unverhältnismässigen administrativen Aufwand mit sich bringen, ohne den Schutz für die Kunden zu erhöhen. Dazu zählt z.B. die Anforderung, die Kunden über die Identität und Kontaktdaten sämtlicher auswärtiger Auftragsbearbeiter zu informieren. Ebenso sind damit verbundene Pflichten, die eine Offenlegung von Geschäftsgeheimnissen gegenüber dem EDÖB nach sich ziehen (wie z.B. bei der automatisierten Einzelfallentscheide, Datenschutz-Folgeabschätzung und

Mitteilung von Verstössen gegen den VE-DSG), substanziell zu reduzieren. Als zentrales Anliegen erachten wir daher eine Entschlackung der Informations- und Meldepflichten als zwingend notwendig.

2) Unverhältnismässig ist ferner die Pflicht, bei den Kunden eine ausdrückliche Einwilligung für das sogenannte Profiling – wie in Art. 4 Abs. 6 und 23 Abs. 2 Bst. b VE-DSG vorgesehen – einzuholen. Zumal der Begriff „Profiling" im VE-DSG sehr breit definiert wird und damit deutlich über die entsprechende Regelung der EU hinausgeht.

3) Aus Rechtssicherheits- und Äquivalenzgründen sollte mit der Regulierung der DSGVO die Erweiterung der Ausnahmebestimmung im Zusammenhang mit Verträgen (Art. 6 Abs. 1 lit. b VE-DSG) in Übereinstimmung gebracht werden. Die Ausnahme ist auf diejenigen Fälle auszuweiten, in denen die betroffene Person nicht Vertragspartei ist, der betroffene Vertrag aber in ihrem Interesse ist oder zu ihren Gunsten abgeschlossen wurde (z.B. bei internationalen Transaktionen des Handels und der Verwahrung von Wertschriften).

4) Die neue Regelung betreffen Daten einer verstorbenen Person (Art. 12 VE-DSG) ist im VE-DSG fehlplatziert und führt zu Rechtsunsicherheiten (Erben sind bereits durch die erbrechtliche Universalsukzession ausrechend legitimiert). Diese Bestimmung sollte daher ersatzlos gestrichen bzw. – sofern erforderlich – im Erbrecht entsprechend ergänzt werden.

5) Die im Vorentwurf vorgeschlagene Regelung betreffend Datenschutz-Folgeabschätzung, die bei vorgesehenen Datenbearbeitungen mit „voraussichtlich erhöhtem Risiko" für die Persönlichkeit der betroffenen Person durchzuführen ist, ist anzupassen, zumal der Begriff „erhöhtes Risiko" unklar und nicht EU-kompatibel ist (DSGVO spricht von einem „hohen Risiko"). Die Frage, ob ein erhöhtes Risiko vorliegt, kann allenfalls erst nach der Durchführung einer Datenschutz-Folgenabschätzung beantwortet werden, was unbefriedigend ist. Eine solche Prüfung wird aber nötig sein, da die Bestimmung strafbewehrt ist. Dies wird dazu führen, dass in der Praxis auch für Bearbeitungen, für die grundsätzlich keine formale Datenschutz-Folgeabschätzung erforderlich wäre, eine solche durchgeführt werden müsste, was nicht zielführend ist. Die damit verbundene Meldepflicht gegenüber dem EDÖB sowie dessen dreimonatige Beantwortungsfrist sind ausserdem praxisfern und werden die Datenbearbeiter stark behindern (z.B. werden dadurch wichtige Projekte ungebührlich lang verzögert).

6) Darüber hinaus braucht es eine Relativierung der neu eingeführten Anhörungspflichten und Auskunftsrechte (dies insbes. auch bei automatisierten Einzelfallentscheiden), welche an den Wortlaut der DSGVO anzupassen sind. Inwiefern eine Ausweitung des Auskunftsbegehrens auf sämtliche Datenbearbeitungen und hängigen Verfahren einen Mehrwert bringt, ist zu hinterfragen. Gerade auch die vorgesehene Kostenlosigkeit des Auskunftsrechts führt zu Fehlanreizen bzw. zu einem unverhältnismässigen Mehraufwand für die Unternehmen. Praxisorientierte bzw. optionale Massnahmen zugunsten der Unternehmen, um dem Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken Einhalt zu gebieten (die „nota bene" bereits im heutigen DSG verankert sind), fehlen an dieser Stelle jedoch komplett und sollten im Vorentwurf ergänzt werden.

7) Erstaunlich ist sodann, dass der Vorentwurf auf die im aktuellen DSG festgehaltene Funktion des „Betrieblichen Datenschutzverantwortlichen" (BDSB) verzichtet und damit auf verbundene Erleichterungen der Meldepflichten eines Unternehmens. Einerseits stellt die Bezeichnung eines BDSB in der Praxis eine unabdingbare Grundvoraussetzung für die Umsetzung des Datenschutzes dar, und anderseits besteht auf europäischer Ebene eine Pflicht zur Einsetzung eines BDSB (vgl. Art. 37 DSGVO, Randziffer 63 Schengen Richtlinie (EU) 2016/680). Zudem kann und soll die Benennung eines BDSB die Verantwortlichen und Auftragsbearbeiter von verschiedenen

Meldepflichten an den Beauftragten (EDÖB) entlasten, aber auch den Beauftragten von der Entgegennahme, Prüfung und Genehmigung dieser Informationen. Die Beibehaltung der gesetzlichen Verankerung eines (freiwilligen) BDSB würde den administrativen Aufwand auf beiden Seiten minimieren.

8) Speziell betonen möchten wir, dass das mit dem VE-DSG vorgeschlagene Sanktionssystem (Art. 50 ff. VE-DSG) weder verhältnismässig noch dienlich ist. Wir lehnen es daher klar ab: Aufgrund des persönlichen und strafrechtlichen Charakters der vorgesehenen Sanktionen geraten Mitarbeiter/innen eines Unternehmens zu stark in den Fokus der Sanktionierung. Dies wird durch die Höhe der Bussen und die vorgesehene Möglichkeit der Bestrafung für fahrlässiges Handeln zusätzlich verschärft. Stossend ist ferner, dass gemäss Art. 53 VE-DSG nur eine subsidiäre Strafbarkeit des Unternehmens bei Wiederhandlung im Geschäftsbetrieb vorgesehen ist. Der Compliance- und Verwaltungsaufwand der Unternehmen würde exponentiell steigen, da sich die Verantwortlichen und ihre Mitarbeiter/innen gegen die zusätzlichen strafrechtlichen Risiken absichern müssten. Dies hemmt das unternehmerische Handeln unnötig und belastet die Standortattraktivität der Schweiz. Insofern sollten Verwaltungsstrafen mit einer klaren institutionellen Trennung zwischen Untersuchungs- und Entscheidbehörde, und nicht strafrechtliche Sanktionen gegen Individuen im Fokus stehen. Ferner geht der Vorentwurf auch hier über die europäischen Regelungen hinaus.

Für die Kenntnisnahme und wohlwollende Prüfung unserer Ausführungen möchten wir uns im Voraus bedanken. Gerne stehen wir Ihnen für Rückfragen zur Verfügung.

Freundliche Grüsse

Dr. Pascal Gentinetta
Geschäftsführer

Simon Binder
Public Policy Manager

Amstutz Jonas BJ

Von: Steck Marcel <marcel.steck@ed-steck.ch>
Gesendet: Donnerstag, 30. März 2017 16:27
An: Amstutz Jonas BJ
Betreff: Stellungnahme des VbN zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de.doc

Sehr geehrter Herr Amstutz

Namens des VbN übermittle ich Ihnen unsere Stellungnahme
Wir danken für Ihre Kenntnisnahme

Freundliche Grüsse

M. Steck
Fürsprecher und Notar

Verband bernischer Notare
Geschäftsstelle
Marktgasse 37, Postfach, 3001 Bern
Tel. 031'320'37'32 Fax 031'320'37'30
E-Mail vbn@ed-steck.ch
Homepage www.bernernotar.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Verband bernischer Notare

Abkürzung der Firma / Organisation : VbN

Adresse : Marktgasse 37

Kontaktperson : M. Steck

Telefon : 031/320'3732

E-Mail : info@bernernotar.ch

Datum : 30.3.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	3		j	Begriffe Neue Litera j. Beauftragter: Beauftragte und Beauftragter nach Art. 37 ff Begründung der Begriff wird erstmals in Art. 2 Abs. 3 des VE erwähnt. Der Vollständigkeit halber wäre eine Ergänzung angebracht.
Fehler! Verweisquelle konnte nicht		11	1		Abs. 1 ergänzen mit … unbefugtes Bearbeiten*, unbefugten Zugriff* oder Verlust geschützt werden Begründung. Der Unbefugte Datenzugriff durch Dritte ist nicht im Begriff ‚Datenbearbeitung' enthalten. Die

gefunden werden.					Verletzung des Datenschutzes auch den unbefugten Zugriff mitumfasst, kann lediglich aus dem Erläuternden Bericht erschlossen werden; so bspw. aus Ziffer 8.1.3.5.
Fehler! Verweisquelle konnte nicht gefunden werden.		12	2		Abs. 2 ergänzen ... eine faktische Lebensgemeinschaft führten, *oder der Willensvollstrecker* Begründung: Der Erblasser setzt insbesondere wenn keine Erben der 1. Parantel oder Lebenspartner vorhanden sind, ein Willensvollstrecker zur umfassenden Abwicklung des Nachlasses ein. Der Willensvollstrecker hat die Interessen des Erblassers umfassend zu wahren. Dazu gehören auch die Daten der verstorbenen Person. Die gesetzliche Fiktion dass gewissen Personen ein schutzwürdiges Interesse zukommt ist auf den Willensvollstrecker auszudehnen.
Fehler! Verweisquelle konnte nicht gefunden werden.			3		Abs. 3 streichen Begründung. Der Absatz hebt das Berufsgeheimnis von Anwälten und Notaren integral auf. Jeder Notar, jeder Anwalt führt heute Personendaten im Sinne von Art. 3 lit. a, beispielsweise eine Adresskartei seiner Klienten. Der Notar führt zudem ein Urschriftenregister. Nach Meinung der herrschender Lehre sowie des Bundesgerichts ist das Berufsgeheimnis nach dem Tod des Mandanten vom Rechtsanwalt bzw. vom Notar grundsätzlich auch gegenüber den Erben zu beachten und das Recht zur Entbindung vom Berufsgeheimnis geht zufolge der Höchstpersönlichkeit des Verhältnisses zwischen Rechtsanwalt bzw. Notar und Mandant nicht einfach auf die Erben über (STRAZZER in successio 2014 S. 113, 119; Kommentierung zum Urteil des Zürcher Obergerichts vom 4.11.2014; BGE 135 III 597 E. 3.2. und E. 3.3.). Will der Rechtsanwalt auf eine Anfrage nach allfälligen Personendaten machen, so muss er sich über die kantonale Anwaltsaufsichtsbehörde vom Berufsgeheimnis entbinden lassen. Analoges gilt für das Notariat, wobei insbesondere im Kanton Bern keine Möglichkeit besteht sich vom Berufsgeheimnis entbinden zu lassen.
Fehler! Verweisquelle konnte nicht gefunden werden.		17	1		Abs. 1 ergänzen mit… unbefugte Datenbearbeitung, *Datenzugriff* oder den …. Begründung. Vgl. bei Art. 11 Abs. 1

Fehler! Verweisquelle konnte nicht gefunden werden.			4		Abs. 4. ergänzen: Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung, unbefugten Datenzugriff und über einen Verlust von Daten Begründung: Damit der Verantwortlich die Pflichten nach den Absätzen 1 und 2 dieses Artikels nachkommen kann, muss er entsprechend informiert werden. Diese erfordert eine analoge Pflicht des Auftragsbearbeiters.
Fehler! Verweisquelle konnte nicht gefunden werden.		50	3	b	Abs. 3 lit. b ergänzen: den Verantwortlichen über eine unbefugte Datenbearbeitung *unbefugten Zugriff oder Verlust* nach Artikel 17 Absatz 4 zu informieren Begründung vgl. bei Art. 17 Abs. 4
Fehler! Verweisquelle konnte nicht gefunden werden.		51	1	c	Abs. 1 lit. c ergänzen: es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung*, unbefugten Zugriff oder Verlust* zu schützen (Art. 11); Begründung. Vgl. bei Art. 11 Abs. 1
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler!	

Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Amstutz Jonas BJ

Von: Philipp Rüfenacht <p.ruefenacht@kellerpatent.ch>
Gesendet: Montag, 3. April 2017 07:47
An: Amstutz Jonas BJ
Betreff: Totalrevision DSG: Stellungnahme des VESPA
Anlagen: Totalrevision DSG Stellungnahme VESPA.doc

Sehr geehrter Herr Amstutz

In der Beilage lasse ich Ihnen im Rahmen der Totalrevision des Datenschutzgesetzes die Stellungnahme des Verbandes der freiberuflichen Europäischen und Schweizer Patentanwälte (VESPA) zukommen.

Besten Dank und freundliche Grüsse

Dr. Philipp Rüfenacht

Präsident VESPA

p. A. Keller & Partner Patentanwälte AG
Eigerstrasse 2
Postfach
CH-3000 Bern 14
Switzerland
Telefon +41 (0) 31 310 80 80
Telefax +41 (0) 31 310 80 70
p.ruefenacht@kellerpatent.ch
www.vespa.swiss

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Verband der freiberuflichen Europäischen und Schweizer Patentanwälte

Abkürzung der Firma / Organisation : VESPA

Adresse : c/o Keller & Partner Patentanwälte AG, Eigerstrasse 2, 3000 Bern 14

Kontaktperson : Philipp Rüfenacht

Telefon : 031 310 80 80

E-Mail : p.ruefenacht@kellerpatent.ch

Datum : 03.04.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
VESPA	Der VESPA (Verband der freiberuflichen Europäischen und Schweizer Patentanwälte) wurde im Jahre 1978 als Interessensvertretung der freiberuflich tätigen zugelassenen Vertreter beim Europäischen Patentamt ("European Patent Attorneys") mit Sitz in der Schweiz gegründet. Seit Inkrafttreten des Schweizer Patentanwaltsgesetzes im Jahre 2011 steht die Mitgliedschaft auch im Patentanwaltsregister eingetragenen Schweizer Patentanwälten offen. Damit sieht sich der VESPA heute als Berufsverband, der für die Interessen der gesamten freiberuflichen Patentanwaltschaft in der Schweiz und ihrer Klienten (zu einem grossen Teil Schweizer KMUs) einsteht. Im Rahmen der vorliegenden Stellungnahme äussert sich der VESPA ausschliesslich in Bezug auf eine Änderung, welche die Register für Immaterialgüterrechte betrifft.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
	DSG	2	2	d (alt)	Wir halten die Unterstellung der Patent-, Marken- und Designregister unter das DSG als verfehlt. Wir schliessen uns in diesem Punkt der unten reproduzierten Stellungnahme des LES-CH vom 15. März 2017 an und erlauben uns, vorab folgende zusätzliche Bemerkungen anzubringen: 1. Im erläuternden Bericht wird nicht darauf eingegangen, dass es öffentliche und nicht-öffentliche Register des Privatrechtsverkehrs gibt: Nach Art. 81 Abs. 1 ZStV kann etwa eine Person beim Zivilstandsamt des Ereignis- oder Heimatortes lediglich Auskunft über die Daten verlangen, die *über sie* geführt werden. Dagegen sind etwa das Handelsregister (Art. 930 OR) und das Patentregister (Art. 95 Abs. 1 PatV) für *jedermann* öffentlich. 2. Es gibt also nach geltendem Recht öffentliche und nicht-öffentliche Register „des Privatrechtsverkehrs“. Diese Differenzierung darf nicht übergangen werden. Die handelsbezogenen Register müssen vollständig öffentlich bleiben und sollten nicht dem Datenschutz unterstellt werden. 3. Es kann keinen Zweifel daran geben, dass auch die *internationalen Immaterialgüterregister* „Register“ im Sinne des DSG sind. Der Bund hat für die internationalen Publizitätsinstitute staatsvertraglich die Kompetenzen an die internationalen Registerbehörden EPA und der WIPO delegiert. Besonders sichtbar ist dies vor allem dort, wo die Eintragungen im internationalen Register nicht in das nationale Register überführt werden und eo ipso Schutz in der Schweiz geniessen (z. B. bei IR-Marken). Wollte man hinsichtlich der Unterstellung der Register unter den Datenschutz zwischen nationalen und internationalen Registern unterscheiden, würde dies – je nachdem wie man’s nimmt – zu einer massiven Ausländer- bzw. Inländerdiskriminierung führen: die Registerdaten würden jeweils unterschiedlich behandelt bzw. einem unterschiedlichen Regime unterstellt. Dies kann nicht sein. Es ist zudem schleierhaft, wie das DSG

					beispielsweise gegenüber WIPO als registerführender Behörde durchgesetzt werden soll. inhaltliche Stellungnahme des LES-CH: Dans le cadre de ses activités, le LES-CH a pris connaissance de l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données (ci-après "ALPD") qui prévoit dorénavant de soumettre les registres publics de propriété intellectuelle à la loi sur la protection des données. Dans le délai imparti au 4 avril 2017, l'association LES-CH conteste le bien-fondé de ce changement de paradigme visant à soumettre à l'ALPD les registres publics de propriété intellectuelle découlant notamment de la loi fédérale sur les marques et des indications de provenance géographiques, de la loi fédérale sur les brevets ("LBI") et de la loi fédérale sur les designs, tous gérés par l'Institut fédéral de la propriété intellectuelle. A ce jour, une personne (physique ou morale) peut obtenir un monopole sur une marque, un brevet ou un design. La contrepartie automatique et obligatoire de ce monopole est la publicité du registre et la consultation par tout tiers des pièces contenues dans ce même registre. Il s'agit de principes cardinaux essentiels à la viabilité du système puisqu'ils sont les seuls à même de permettre la transparence - et donc le contrôle - du système. Les seules limitations actuelles portées à ces deux principes sont (i) la garantie de pouvoir classer à part les documents qui contiennent des secrets de fabrication ou d'affaires (art. 36 al. 3 de l'Ordonnance sur la protection des marques ("OPM"), art. 65 LBI, art. 22 de l'Ordonnance sur les designs ("Odes")) et la destruction des documents suite à une radiation/révocation du droit de propriété intellectuel (art. 39 OPM, art 92 OBI, art. 24 ODes). Les utilisateurs du système sont ainsi parfaitement informés du fait que les données communiquées dans le cadre d'une procédure devant l'Institut fédéral de la propriété intellectuelle sont entièrement accessibles au public. Le LES-CH est d'avis que l'application de l'ALPD aux registres publics de propriété intellectuelle est inappropriée car elle ne permet pas de tenir compte de (i) l'intérêt public général à pouvoir accéder à toutes les données échangées en vue de l'octroi d'un monopole et (ii) des deux principes cardinaux précités. Ce constat ne signifie pas que la protection des données ne doit pas trouver du tout d'application dans le domaine de la propriété intellectuelle, mais elle doit s'effectuer par des dispositions spéciales, contenues directement dans les lois spécifiques de propriété intellectuelle. Seule une telle approche permet de tenir compte des particularités des divers droits de propriété intellectuelle et de régler, en fonction du registre

					(marque, indications géographies, brevet, design, etc.), les questions relatives à la protection des données. Au surplus, la tendance actuelle est très clairement de permettre un accès immédiat online à l'ensemble du dossier. Cette pratique est largement répandue au niveau européen et tant l'Office de l'Union européenne pour la propriété intellectuelle que l'Office Européen des Brevets offrent un accès électronique online à l'ensemble des pièces de la procédure, y compris les échanges entre les parties et entre les parties et l'office. Les utilisateurs suisses du système militent pour qu'une telle offre soit aussi disponible pour les registres publics suisses de propriété intellectuelle, ce qui permettra d'accroître encore la transparence et l'efficacité du système. Il va sans dire que l'application de l'ALPD à ces registres va entraver inutilement un tel développement. Pour les motifs précités, le LES-CH est d'avis que la suppression de l'exception prévue actuellement à l'article 2 al. 2 let. d LPD n'a aucune raison d'être et demande que cette exception perdure, à tout le moins pour les registres publics de droits de propriété intellectuelle.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.		

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

VERBAND FREIER AUTOHANDEL SCHWEIZ
ASSOCIATION INDÉPENDANTE COMMERCE AUTOMOBILE SUISSE
ASSOCIAZIONE SVIZZERA DEI COMMERCIANTI DI VEICOLI INDIPENDENTI
SWISS ASSOCIATION OF INDEPENDANT VEHICLE TRADERS

Mitglied von:
sgv usam
Schweizerischer Gewerbeverband
economiesuisse

BA Justiz
E - 5. April 2017
Act

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Eingabe von:

VFAS – Verband freier Autohandel Schweiz
Bremgartenstrasse 75
5610 Wohlen
Telefon 056 619 71 32
katrin.portmann@vfas.ch

Sehr geehrte Frau Bundesrätin

Wir freuen uns, dass Sie den relevanten Wirtschafts- und Branchenverbänden die Möglichkeit einräumen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu beziehen. Obwohl wir nicht direkt eingeladen wurden, ist es uns wichtig, die Anliegen unserer Branche einzubringen.

Kernanliegen der Schweizer Wirtschaft zum VE-DSG

Im Datenschutzgesetz ist für Unternehmen, insbesondere auch KMU, ein Maximum an Flexibilität und ein Minimum an Belastung zu wahren.

Spielräume im Verhältnis zum internationalen Recht sowie das etablierte System der Selbstregulierung sind so weit als möglich zu nutzen und beizubehalten. Einen überschiessenden „Swiss Finish" lehnen wir kategorisch ab.

Die Initiative für Empfehlungen der guten Praxis muss stets zwingend von (Branchen)Verbänden ausgehen. Die Selbstregulierung ermöglicht es mittels Bezug zur Praxis, sachgerechte Lösungen zu entwickeln.

Spezifische Forderungen des freien Autohandels (DSG; SR 235.1 sowie Art. 8)

Seit 1956 vertritt der VFAS die Interessen des unabhängigen und freien Autohandels in der Schweiz. Wir sind der einzige unabhängige Verband, der sich gegen die Marktmacht von Grosskonzernen in der Automobilbranche einsetzt. Wir wehren uns gegen sämtliche Einschränkungen und Behinderungen des freien Autohandels. Dabei setzen wir uns kompromisslos für dessen Förderung, für eine hohe Qualität im Autohandel sowie einen grösstmöglichen Kundennutzen ein.

i. Keine öffentliche Bekanntgabepflicht der Fahrzeug-Indentifizierungs-nummer (VIN)

Im Juli 2015 hat der eidgenössische Datenschutz- und Öffentlichkeitsbeauftrage (EDÖB) auf der Basis einer im Auftrag des Bundesamts für Strasse (ASTRA) erstellten Expertise entschieden (vgl. Beilage; Schreiben vom 6. Juli 2015; Bekanntgabe von Fahrgestellnummern (VIN) durch das ASTRA), dass VIN-Nummern im Sinne des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) als schützenswerte Personendaten gelten. Der Schutz der VIN-Nummern liegt insbesondere auch im Interesse von Konsumentinnen und Konsumenten.

1. Bedeutung der VIN im Direkt-/Parallelimport: Für Direkt- und Parallelimporteure stellen Fahrgestellnummern ein zentrales Element ihres Geschäftsgeheimnisses dar und sind aus diesem Grund schützenswert. Generalimporteure sind in der Lage, mittels dieser Angabe den ausländischen Verkäufer von Direkt-/Parallelimporten ausfindig zu machen und damit über die werksinternen elektronischen Systeme Informationen über folgende Elemente zu gewinnen:

- Käufer der Fahrzeuge in der Schweiz (Firmen/Privatpersonen);
- erzielte Verkaufspreise und Konditionen;
- bei Vermittlungsgeschäften über professionelle Parallelimporteure: Namen, Angaben, Adressdaten und Identitätspapiere von Endkonsumenten.

Nicht zuletzt könnte der aus Sicht der Generalimporteure unliebsame Direkt-/Parallelimport mittels Drohungen und Druck auf die nun bekannten ausländischen Lieferanten zum Erliegen gebracht werden. Dies wird schon heute praktiziert: Generalimporteure lesen vor Ort auf den Verkaufsplätzen der Direkt- und Parallelimporteuren systematisch Fahrgestellnummern ab und missbrauchen die daraus erhaltenen Erkenntnisse für Retorsionsmassnahmen gegen ausländische Lieferanten und somit zur Schädigung dieses Vertriebswegs.

2. Bedeutung von Fahrgestellnummern für Konsumenten: Auf Basis einer Fahrgestellnummer können persönliche Angaben von Fahrzeughaltern ausfindig gemacht werden, ohne dass diese von dieser Weitergabe dieser Daten Kenntnis erhalten oder sich dagegen aussprechen könnten. Dieser verdeckte Datenfluss ist im Interesse des Persönlichkeitsschutzes zu vermeiden.

3. Folgen einer Bekanntgabe: Die preisregulierende Funktion der Direkt- und Parallelimporteure wird von zahlreichen Schweizer Behörden und Institutionen (z. B. Wettbewerbskommission, Preisüberwacher, Konsumentenschützer) sowie parteiunabhängig von der Politik ausdrücklich gewünscht. Es wäre mehr als unglücklich, wenn diese wichtige Wettbewerbsfunktion aus vermeintlichen datenschutzrechtlichen Gründen entfiele. Die Vermeidung der Abschottung des Schweizer Marktes und das Verhindern einer Hochpreisinsel Schweiz ist Aufgabe aller Bundesbehörden.

ii. Keine Publikationspflicht für sensible CO2-Daten

Eine Veröffentlichung der sensiblen Daten im Rahmen der CO2-Zielerreichung liesse direkte Rückschlüsse auf den Geschäftsgang und die Strategie juristischer Personen und deren Geschäftsinhaber (natürliche Personen) zu, was der heutigen Praxis des Datenschutzes diametral widerspricht.

Ausserdem könnten auf der Basis von publizierten sensiblen Daten auch Rückschlüsse auf die finanziellen Verhältnisse der entsprechenden Firmen und natürlichen Personen gezogen werden, was das DSG per se nicht zulassen möchte.

Der VFAS fordert im Namen seiner Mitglieder und der Schweizer Konsumentinnen und Konsumenten, dass

i. der Schutz der VIN-Nummer im Rahmen der VE-DSG auf der Basis des Entscheids des EDÖB vom 6. Juli 2015 erhalten bleiben muss und VIN-Nummern weiterhin als schützenwerte Personendaten im Sinne des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) gelten und als solche in der Gesetzesvorlage Eingang finden;

ii. der Schutz von sensiblen Daten im Rahmen der CO2-Zielerreichung ebenfalls in die überarbeitete Gesetzgebung Eingang findet. Als Sekundärforderung wäre die Empfehlung der guten Praxis konsequent anzuwenden.

Des Weiteren stützen wir unsere Stellungnahme auf die übergeordnete, gesamtwirtschaftliche Stellungnahme von economiesuisse:

1. Einleitende Bemerkungen

Ein angemessenes und wirksames Datenschutzgesetz ist für die Wirtschaft von grosser Bedeutung. Dieses muss Raum für die wirtschaftliche Entwicklung lassen sowie der Rechts- und Investitionssicherheit dienen. Darüber hinaus sind Akzeptanz und Vertrauen der Nutzer in den Datenschutz eine zentrale Voraussetzung für die Fortentwicklung der immer wichtiger werdenden digitalen Wirtschaft und der Nutzung des damit verbundenen wirtschaftlichen Potentials.

Überschiessende und im Geschäftsalltag nicht praktikable Regulierungen wirken sich demgegenüber innovationshemmend aus. Sie können der Wettbewerbsfähigkeit von Unternehmen auf nationaler Stufe, vor allem aber auch im internationalen Umfeld schaden. Zu weitgehende Bestimmungen, welche den Individuen ihre Handlungsfähigkeit absprechen, führen zudem zu einer Bevormundung der Bürger.

Angesichts der dynamischen technologischen aber auch der internationalen Entwicklungen im Bereich Datenschutz ist für die Schweiz von Bedeutung, dass sie mit modernen Regelungen den Zugang insbesondere zum EU-Raum nicht unnötig einschränkt. Damit die Schweizer Regulierung aus Sicht der EU als äquivalent angesehen werden kann, reicht es jedoch, wenn sie die grundlegenden Garantien einhält (vgl. Erw. 104 DSGVO / US-EU Privacy Shields). Daneben hat sich das Schweizer Datenschutzrecht auch an der Konvention 108 des Europarates zu orientieren, welche für die Schweiz verbindlich gilt, dies unter Berücksichtigung auch der Richtlinie (EU) 2016/680.

Hierbei ist innerhalb der internationalen Vorgaben ein Maximum an Flexibilität für den Schweizer Standort zu erhalten; die Wirtschaft soll nicht durch übertriebene Bestimmungen («Swiss Finish») mit unnötigem administrativen Aufwand belastet werden. Dieser wäre überdies auch aus einer gesamtheitlichen Sicht kontraproduktiv, weil solche Schweizer Besonderheiten einen einheitlichen internationalen Datenraum verhindern würden und damit auch zulasten der Schweizer Unternehmen wettbewerbsverzerrend wirken würden.

Auf Basis des Vorentwurfes hat economiesuisse auf Grund der Rückmeldungen der Mitglieder in seiner Arbeitsgruppe Datenschutz sowie in der Rechtkommission den Anpassungsbedarf erarbeitet. Der notwendige Handlungsbedarf wurde von der Wirtschaft erarbeitet. Im Folgenden wird aufgezeigt, wie die Regelungen bzw. deren Reichweite beschränkt werden können und wo weitere grundsätzlichere Anpassungen vorzunehmen sind.

2. Zweck

Die Zweckbestimmung ist anzupassen. Gerade auch unter Berücksichtigung der Strategie des Bundesrates für eine «digitale Schweiz» ist der Zweck um «die Förderung des freien Verkehrs der Personendaten» zu ergänzen. Dies entspricht auch der Zielsetzung der europäischen Verordnung.

3. Geltungsbereich

Kein Schutz für juristische Personen
Die Abschaffung des Datenschutzes für Unternehmen analog der DSGVO und E-SEV 108 wird begrüsst. Dieser hat in der Praxis kaum eine Rolle gespielt.

Neues Missbrauchspotential beim Auskunftsrecht
Der VE-DSG sieht neu vor, dass das Datenschutzgesetz auch auf bereits rechtshängige Zivilprozesse und laufende Strafverfahren zur Anwendung gelangen soll. Dieser erweiterte Geltungsbereich birgt erhebliches Missbrauchspotential beim Auskunftsrecht (Beweisbeschaffung über die zivilprozessualen Editionsrechte hinaus). Es braucht griffige Mechanismen, welche dem Rechtsmissbrauch oder der nicht vorgesehenen Anwendung dieser Bestimmung im Zivilprozess oder im Strafverfahren entgegenstehen (vgl. nachfolgend Ziff. 11).

Regelung des räumlichen Anwendungsbereichs / IPR
Im VE-DSG fehlt eine Regelung zum räumlichen Anwendungsbereich des Gesetzes. Es ist damit nicht klar, wer nach schweizerischem Datenschutzrecht Rechtsschutz verlangen kann und welche Durchsetzungsmöglichkeiten in der Schweiz für Verletzungen, welche nach ausländischem Recht beurteilt werden, bestehen (vgl. Art. 130/139 IPRG). Die Anwendbarkeit des Datenschutzgesetzes in internationalen Verhältnissen sollte präzise geregelt werden. Hierbei wäre ein weiter Anwendungsbereich des Schweizer Datenschutzrechts in Einklang mit den internationalen Bestimmungen wünschenswert.

Art. 139 Abs. 1 IPRG sieht ein weitgehendes Recht eines Geschädigten vor, das anwendbare Recht zu wählen. Dadurch werden Verantwortliche in der Schweiz potentiell der Datenschutz-Grundverordnung der EU (oder einem anderen ausländischen Datenschutzgesetz) unterworfen. Dies führt zu einer weitergehenden extra-territorialen Anwendbarkeit, als dies gemäss den betreffenden Bestimmungen der DSGVO der Fall ist. Art. 139 Abs. 3 IPRG sollte dahingehend eingeschränkt werden, dass ein ausländischer Erfolgsort im Sinne von Absatz 1 Buchstabe c nicht allein damit begründet werden kann, dass die Daten im betreffenden Land gespeichert sind. Andernfalls würden die Verantwortlichen in der Schweiz leichthin in Gerichtsverfahren im Ausland gezwungen.

4. Begriffe

Definition der Bestimmbarkeit bei Personendaten
Art. 3 lit. a VE-DSG sieht keine Definition der Bestimmbarkeit vor. Es ist zu konkretisieren was unter «bestimmbaren Personendaten» zu verstehen ist.

Einschränkung der Definition der besonders schützenswerten Personendaten
Die Ausweitung des Begriffs der «besonders schützenswerten Personendaten» auf genetische und biometrische Daten geht zu weit. Der Wortlaut widerspricht den Erläuterungen im Bericht: Angedacht war die Erfassung von Daten, welche zum Zweck bearbeitet werden, eine natürliche Person eindeutig zu identifizieren. Dies entspricht auch der Stossrichtung der Konvention 108. Nach der im VE-DSG vorgeschlagenen Definition wäre beispielsweise künftig jedes Gesichtsfoto als biometrisches Datum erfasst. Die Definition ist entsprechend einzuschränken.

Einschränkung der Definition des Profiling
Die Definition des Begriffs «Profiling» ist im VE-DSG sehr breit gefasst und geht deutlich über die entsprechende Regelung der EU hinaus. In der DSGVO hängt die Zulässigkeit des Profiling von der Wahrnehmung der betroffenen Interessen ab. Nur in Fällen, in denen das Profiling Teil einer *automatischen Entscheidung* wird und rechtliche Wirkung erzeugt, gelten andere Vorschriften. Der VE-DSG vermischt die beiden Institute: Erfasst ist auch das «menschliche», d.h. manuelle Profiling (z.B. eine schriftliche Mitarbeiterbeurteilung oder die Alterskapitalberechnung einer Versicherung) sowie nicht-personenbezogene Daten. Dies stellt eine unzulässige Ausweitung des Geltungsbereiches dar und steht im Widerspruch zu Art. 2 Abs. 1 VE-DSG.

Die Definition des Begriffes ist analog der DSGVO auf die *automatisierte* Auswertung von *Personen*daten zu begrenzen. Zudem ist die Auswertung, bzw. Analyse keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte auswirkt. Die Bestimmung sollte daher anstatt «Auswertung» analog der DSGVO den Begriff «Bewertung» verwenden.

Einführung des betrieblichen Datenschutzbeauftragten
Es besteht klar der Wunsch, eine Regelung zur Bezeichnung eines betrieblichen Datenschutzbeauftragten auf freiwilliger Basis vorzusehen. Dies kann mit einer entsprechenden Erleichterung bei den Pflichten unter dem DSG verknüpft werden (vgl. nachfolgend, Ziff. 8.2). In diesem Sinne ist auch eine Definition des betrieblichen Datenschutzbeauftragten erforderlich.

5. Grundsätze

Klare Terminologien
Der VE-DSG verschärft den Grundsatz der Erkennbarkeit des Zweckes unnötigerweise mit dem Zusatz der «klaren» Erkennbarkeit. Diese Anpassung an die Terminologie des DSGVO ist in diesem Falle verfehlt, da die Schweizer Regelung einem unterschiedlichen Grundkonzept folgt (Erkennbarkeit im Rahmen einer klaren Zweckbindung). Die Verschärfung ist auslegungsbedürftig und produziert damit auch Rechtsunsicherheit. Der Zusatz ist nicht erforderlich und zu streichen.

Dies gilt auch für den Begriff der «eindeutigen» Einwilligung von Art. 4 Abs. 6 VE-DSG: Damit wird lediglich wiederholt, was bereits heute unter dem risikobasierten Ansatz gilt. Der Zusatz ist ebenfalls wegzulassen. Auch wann eine Einwilligung «ausdrücklich» sein soll, ist nicht klar. Jedenfalls muss auch passives Verhalten als gültige Einwilligung gelten, damit weiterhin die im Massengeschäft unumgänglichen Allgemeinen Geschäftsbedingungen (AGB) verwendet werden können. Das Erfordernis der Ausdrücklichkeit für das Profiling muss gestrichen werden (vgl. Ziff. 4).

Keine Nachführungspflicht
Auch die permanente Nachführungspflicht geht zu weit und ist nicht praktikabel. Der 1. Satz von Art. 4 Abs. 5 VE-DSG ist entsprechend ersatzlos zu streichen.

6. Auslandtransfer

Unnötige Wiederholung von Grundsätzen
Art. 5 Abs. 1 VE-DSG wiederholt bereits statuierte Grundsätze und ist im Kontext von Art. 5 verwirrend und überflüssig. Der Absatz ist deshalb zu streichen.

Keine Feststellung durch den Bundesrat
Die neu vorgesehene Feststellung durch den Bundesrat, ob Daten im Ausland genügend geschützt sind, bedeutet eine unsachliche und unnötige Einschränkung. Diese Feststellung würde besser durch den Verantwortlichen, gestützt auf eigene Abklärungen und Kenntnisse, erfolgen. Die Bestimmung ist im Sinne einer geringeren Einschränkung anzupassen.

Unklare und widersprüchliche Kategorisierung der Garantien
Die Unterscheidung in Art. 5 Abs. 3 VE-DSG zwischen «spezifischen» und «standardisierten» Garantien ist unklar und macht aus Sicht der Praxis keinen Sinn. Erschwerend kommt hinzu, dass die standardisierten Garantien einer Genehmigung durch den EDÖB bedürfen.

Auch Binding Corporate Rules (BCR) unterliegen der Genehmigungspflicht, diese stellen aber eine Untergruppe der spezifischen Garantien dar. Für diese wiederum ist jedoch nur eine Informationspflicht vorgeschrieben. Dies ist widersprüchlich.

6.1 Genehmigungspflicht

Berücksichtigung von Geheimhaltungsinteressen / Kürzung der Genehmigungsfrist
Es sollte lediglich zwischen Standardverträgen und anderen Verträgen/Garantien unterschieden werden. Spezifische Garantien sind in der Regel in Verträgen enthalten. Es ist praxisfern und insbesondere im Zusammenhang mit dem BGÖ problematisch, wenn diese dem EDÖB vorgelegt werden müssen.
Schliesslich ist die für eine Genehmigung vorgesehene Frist des EDÖB von 6 Monaten nicht praktikabel. Im Tagesgeschäft sind entsprechende Bewilligungen kurzfristig erforderlich. Mit derart ausgedehnten Fristen ist eine Verwendung solcher Garantien/BCR kaum noch möglich, da ein Unternehmen nach Vertragsabschluss nicht derart lange warten kann. Die Frist ist auf das heutige Mass von 30 Tagen zu kürzen. Auch ist von einer unbeschränkt möglichen Verlängerung abzusehen.

Keine Genehmigung durch den Beauftragten
Einzelne Mitglieder wünschen, dass die Genehmigung von standardisierten Garantien oder verbindlichen unternehmensinternen Datenschutzvorschriften (BCR) durch den Beauftragten sogar ganz wegzulassen ist, da diese zu einem erheblichen Mehraufwand für die Unternehmen und gegebenenfalls zu Projektverzögerungen führe. Gleichzeitig trage diese kaum etwas zum besseren Datenschutz bei, da das Unternehmen weiterhin selber in der Verantwortung stehe. Ein grenzüberschreitender Datenfluss würde durch diese Regelung erheblich erschwert. Lediglich die DSGVO (nicht die Konvention 108) sieht eine entsprechende Vorgabe vor. Es wird hier klar Raum für einen sich im Verhältnis zur DSGVO differenzierenden Regelungsansatz gesehen.

Keine Informationspflicht bei Vorliegen standardisierter Garantien
Auch die pauschale Informationspflicht von Art. 5 Abs. 6 VE-DSG im Zusammenhang mit standardisierten Garantien bringt keinen Mehrwert. Es geht hier um bereits genehmigte oder anerkannte Garantien. Dies ist nicht einmal in der DSGVO vorgesehen.[1] Die Bestimmung ist entsprechend zu streichen.

6.2 Ausnahmen

Keine Einwilligung «im Einzelfall»
Die in Art. 6 Abs. 1 lit. a VE-DSG vorgesehene Ausnahme der «Einwilligung im Einzelfall» ist weder sinnvoll noch notwendig. Nach den allgemeinen Grundregeln reicht für wiederkehrende Sachverhalte bei gleichbleibender Erkennbarkeit und Erwartung eine einmalige Einwilligung. Der Zusatz «im Einzelfall» ist zu streichen. Dies gilt auch für die Bekanntgabe «im Einzelfall» (Art. 6 Abs. 1 lit. d VE-DSG).

Erweiterung der Ausnahme i. Zh. mit Verträgen
Die Ausnahmebestimmung von Art. 6 Abs. 1 lit. b VE-DSG ist mit der DSGVO abzustimmen. Die Ausnahme ist auf diejenigen Fälle auszuweiten, in denen die betroffene Person nicht Vertragspartei ist, der betroffene Vertrag aber in ihrem Interesse ist oder zu ihren Gunsten abgeschlossen wurde.

Streichung Begriffe «Gericht» und «Verwaltungsbehörde»
Die Begriffe «Gericht» und «Verwaltungsbehörde» bei Art. 6 Abs. 1 lit. c VE-DSG sind zu streichen. Die Unterscheidung ist nicht erforderlich und es stellen sich schwierige Abgrenzungsfragen.

[1] Vgl. dazu EuGH-Entscheid Schrems und Entscheid der EU-Kommission vom 16.12.2016 (keine erneute Einwilligung im Einzelfall).

Massgebend ist, dass die Datenbearbeitung zur «Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen» erfolgt.

Keine Informationspflicht bei Vorliegen eines Ausnahmetatbestandes
Die in Art. 6 Abs. 2 vorgesehene Informationspflicht, dies trotz Vorliegen eines Ausnahmetatbestandes, ist unverhältnismässig und zu streichen. Eine entsprechende Bestimmung ist weder im EU-Recht noch in der Konvention vorgesehen. Nebst zu erwartender hoher Anzahl an Meldungen wäre auch die Information des EDÖB über heikle Verfahren und (Geschäfts-)geheimnisse problematisch (BGÖ).

7. Auftragsdatenbearbeitung

Keine Vergewisserungspflicht
Die in Art. 7 neu vorgesehene Vergewisserungspflicht führt zu massivem Mehraufwand beim Outsourcing der Datenbearbeitung. Es ist unklar, welche Pflichten dem Auftragsdatenbearbeiter überbunden werden sollen. Die Vergewisserungspflicht widerspricht dem prinzipienbasierten Ansatz des VE-DSG und die Präzisierung ist gerade in Bezug auf projektspezifische Herausforderungen kontraproduktiv. Die Bestimmung ist zu streichen.

Reduzierte Anforderungen an die Einwilligung
Die Anforderung einer «schriftlichen» Zustimmung ist vor dem Hintergrund der heutigen Geschäftsprozesse, dies insbesondere auch auf Grund der komplexen Dienstleistungsverhältnisse nicht praxistauglich. Eine dokumentierte Zustimmung reicht aus; Schriftlichkeit i.S.v. Art. 13 OR ist nicht erforderlich. Es ist eine Präzisierung vorzunehmen, dass, dies auch im Einklang mit der Bestimmung in der EU, eine generelle Einwilligung für den Beizug von Sub-Auftragsdatenbearbeitenden und eine Information im konkreten Fall ausreicht.

8. Selbstregulierung

8.1 Empfehlungen der guten Praxis

Begrüssenswerte Selbstregulierung aber keine Empfehlungen des Beauftragten
Grundsätzlich sind Empfehlungen der guten Praxis in Anlehnung an das bestehende und bewährte Konzept der Selbstregulierung der Branchen zu begrüssen. Der wesentliche Vorteil liegt darin, dass so sehr knappe oder aber sehr komplexe gesetzliche Regelungen praxisnah und operativ umsetzbar präsentiert werden können. Dazu müssen themenspezifische Wünsche der Branche tatsächlich in die Regelung einfliessen. Die im VE-DSG vorgesehene Kompetenz des EDÖB, Empfehlungen der guten Praxis auf eigene Faust auszuarbeiten, widerspricht aber dem Zweck des Instituts. Es fehlen Kontrollen und Rechtsschutzmechanismen. Entsprechend besteht die Gefahr, dass der EDÖB «falsche» oder unverhältnismässige Empfehlungen im Alleingang, ohne institutionelle Kontrolle, verabschiedet. Aufgrund der Fiktion der Rechtmässigkeit von Art. 9 Abs. 1 VE-DSG würde er damit faktisch zum Gesetzgeber.

Dem stünde noch verschärfend entgegen, dass eigene Empfehlungen der interessierten Kreise nur mittels Genehmigung durch den EDÖB festgelegt werden könnten. Unter der DSGVO ist die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen.

Daraus ergibt sich, dass die Bestimmung der VE-DSG dahingehend anzupassen ist, dass die Initiative für Empfehlungen der guten Praxis stets zwingend von (Branchen)Verbänden ausgehen muss. Dies

würde der Tradition der Selbstregulierung entsprechen und brächte den Vorteil mit sich, dass solche Richtlinien von Experten mit starkem Bezug zur Praxis verfasst werden. Dies würde es ermöglichen, sachgerechte Lösungen zu entwickeln, bei denen der Beauftragte durch die Genehmigung immer noch das letzte Wort hat. Die genehmigten Empfehlungen der guten Praxis sind vom EDÖB zu publizieren.

Vermutung der Richtigkeit statt Fiktion, auch für Auftragsdatenbearbeiter
Die Fiktion, welche von der Einhaltung der Empfehlungen auf die Einhaltung Datenschutzvorschriften schliesst, ist ausserdem nicht zielführend. Es sind Konstellationen denkbar, die von den Empfehlungen nur unvollständig/unzureichend geregelt sind. Die Fiktion ist auf eine Vermutung der Richtigkeit zu reduzieren. Diese muss ebenfalls für den Auftragsdatenbearbeiter gelten.

8.2 Betrieblicher Datenschutzbeauftragter

Einführung auf freiwilliger Basis gekoppelt mit Freistellung von Meldepflichten
Der VE-DSG verlangt richtigerweise nicht die breite Einführung eines betrieblichen Datenschutzbeauftragten. Das Institut eines betrieblichen Datenschutzbeauftragten sollte weiter vorgesehen werden. Dies als Option für die Unternehmen, die sich für dieses Modell entscheiden und kombiniert mit der Freistellung von Meldepflichten gegenüber dem EDÖB. Ein betrieblicher Datenschutzbeauftragter könnte als zentrale Stelle die Pflichten für die Unternehmen oder ganze Unternehmensgruppen wahrnehmen. Damit liessen sich Doppelspurigkeiten vermeiden. Auch würde dadurch eine Anlaufstelle für Auskunftsbegehren geschaffen. Dies würde eine Flexibilisierung und gerade für grössere Unternehmen Erleichterungen mit sich bringen, ohne dass KMU belastet würden. Die betrieblichen Datenschutzbeauftragen sind auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen (z.B. bei Art. 16 Abs. 1-3 VE-DSG). (als Fazit-Forderung dann hervorzuheben)

9. Daten einer verstorbenen Person

Keine Regelung im DSG
Art. 12 VE-DSG erscheint im VE-DSG als Fremdkörper. Die Regelung könnte zu Rechtsunsicherheiten führen. Der Nachweis der persönlichen Beziehungen im Zusammenhang mit dem schutzwürdigen Interesse ist in der Praxis kaum zu erbringen. Für Geschäftsdaten bestehen gemäss spezialgesetzlichen Regelungen weitreichende legitime Dokumentations- und Archivierungspflichten, weshalb die pauschale Formulierung des Löschungsrechts nicht zielführend ist. Erben sind bereits durch die erbrechtliche Universalsukzession ausreichend legitimiert, geeignete, interessenwahrende Massnahmen vorzukehren. Die Bestimmung ist deshalb im VE-DSG zu streichen. Eine Regelung wäre an geeigneter Stelle (z.B. im ZGB) vorzusehen, dies aber zu einem späteren Zeitpunkt im Rahmen einer umfassenden Regelung in Bezug auf die Verfügung über Daten und nicht ausschliesslich aus einer datenschutzrechtlichen Sicht.

10. Pflichten

Keine pauschale Anwendung
Die pauschale Anwendung der vorgesehenen Pflichten auf alle Geschäftsmodelle und Branchen ist nicht sachgerecht und wäre mit enormem Aufwand verbunden. Es gilt, ein gestuftes Modell vorzusehen: Strengere Bestimmungen wären dabei für Geschäftsmodelle vorzusehen, welche besonders sensible Datenbearbeitungen umfassen, wie dies typischerweise bei spezifischen Marketing-Dienstleistern und Data-Minern der Fall ist. Auch bei den Pflichten ist ein risikobasierter

Ansatz vorzukehren. Zudem können branchenspezifische Regelungen weitergehende Pflichten vorsehen.

10.1 Informationspflichten

Risikobasierte Transparenzpflicht als Leitlinie
Die erweiterten Informationspflichten auf alle Personendaten bringen Mehraufwand und führen auf Grund des öffentlich-rechtlichen Charakters der Bestimmungen und den daraus fliessenden Sanktionsfolgen zu Problemen in der Praxis. Die vorgesehene massive Ausdehnung der Informationsmenge führt zu einer Überinformation der betroffenen Personen und würde sich damit kontraproduktiv auf die Transparenz auswirken. Die Regel muss grundsätzlich im Sinne einer risikobasierten Transparenzpflicht überarbeitet werden.

Konkret ist die Informationspflicht auf besonders schützenswerte Daten und überdies auf Datenbearbeitungen ausserhalb des (objektiven) Erkennbarkeitshorizonts i.S.v. Art. 4 DSG der betroffenen Person zu beschränken. Ausserdem ist klarzustellen, dass sich die Information (und damit auch die Richtigkeit und Vollständigkeit der Daten) auf den Zeitpunkt der Datenbeschaffung bezieht und nicht auf nachträgliche Änderungen. Die schliesst auch eine Pflicht zur Nachinformation klar aus. Als Kontaktdaten des Verantwortlichen muss eine klare und definierte Funktionsbeschreibung ausreichen, da die natürliche Person innerhalb einer Funktion wechseln kann.

Präzise und einheitliche Terminologien
Unklar ist auch die Differenzierung zwischen «Beschaffung» und «Bearbeitung» und die in Abs. 3 verwendeten Begriffe «Dritte» sowie «Empfängerinnen und Empfänger». Es sollten präzisere und einheitliche Terminologien verwendet werden. Es ist auch fraglich, warum der Vorentwurf den Begriff «Beschaffung» statt wie in der DSGVO vorgesehen «Erhebung» verwendet. Dadurch können sich (nachteilige) Abweichungen im Informationszeitpunkt ergeben.

Keine Mitteilung von Identität und Kontaktdaten der Auftragsdatenbearbeiter
Die Pflicht zur Mitteilung der Identität und der Kontaktdaten sämtlicher Auftragsbearbeiter ist gegenüber dem EU-Recht klar überschiessend. Sie ist weder sinnvoll noch erforderlich. Die Offenlegung der oft für untergeordnete Tätigkeiten mandatierten Auftragsdatenbearbeiter ist nur mit unverhältnismässigem Aufwand zu bewerkstelligen und greift zudem in berechtigte eigene Datenschutzinteressen sowie Geschäftsgeheimnisse der Unternehmen ein. Schliesslich ist unklar, wann genau über was informiert werden muss. Die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben ist bereits Gegenstand von Art. 7 VE-DSG. Diese Zusatzanforderung ist zu streichen.

Keine Mitteilung bei indirekter Datenbeschaffung
Die vorgesehene Informationspflicht bei der indirekten Datenbeschaffung geht zu weit und verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Dem Verantwortlichen werden die relevanten Eckwerte, insbesondere die erstmalige Speicherung, oftmals gar nicht bekannt sein. Das Aufwand-Ertragsverhältnis ist damit unverhältnismässig. Darüber hinaus sind solche direkten Informationspflichten nicht erforderlich, eine allgemeine vorgängige Information des Kunden reicht aus. Die Bestimmung ist zu streichen.

Erweiterung und Präzisierung der Ausnahmen
Die Ausnahmebestimmung von Art. 14 Abs. 3 lit. a VE-DSG ist zu eng gefasst. Direkte Einschränkungen ergeben sich nur selten aus einem Gesetz. Häufiger sieht ein Gesetz zwingende Abklärungspflichten vor, welche mit Geheimhaltungspflichten verbunden sind und welche damit mit einer Einschränkung der Informationspflicht einhergehen. Die Bestimmung ist zu präzisieren und mit

typischen Beispielen zu ergänzen (z.B. Abklärungen im Zusammenhang mit Geldwäscherei, Terrorismusbekämpfung und Korruption). Ausserdem können sich Verpflichtungen auch aus einem Vertrag ergeben. Auch dies ist zu ergänzen.

Für die Einschränkung der Berufung auf überwiegende private Interessen, d.h. auf Fälle, in denen die Personendaten nicht Dritten bekannt gegeben werden, gibt es keine sachlichen Gründe. Besonders bei Konzernverhältnissen würde daraus ein enormer administrativer Mehraufwand resultieren. Sollte die betroffene Person durch die Bekanntgabe beeinträchtigt sein, so wäre dies im Rahmen der allgemeinen Interessensabwägung von Art. 24 VE-DSG zu berücksichtigen. Die Einschränkung ist damit zu streichen.
Die Bestimmung von Art. 14 Abs. 5 VE-DSG ist nicht praktikabel und zu streichen; diese würden dazu führen, dass ständig einzelne Interessensabwägungen überprüft werden müssten. In grossen, komplexen Organisationen ist dies nicht zu bewerkstelligen.

10.2 Automatisierte Einzelfallentscheide

Begrenzung des Anwendungsbereichs und der Pflichten; insb. kein Äusserungsrecht
Die Reichweite der neu eingeführten Informations- und Anhörungspflicht sowie Auskunftsrechte bei automatisierten Einzelfallentscheiden ist zu weitgehend. Zwar kennen die Konvention 108 und die EU eine entsprechende Regelung. Der Anwendungsbereich von Art. 15 VE-DSG ist jedoch viel breiter: Der VE-DSG unterscheidet stärker zwischen Profiling und automatisieren Einfallentscheiden und sieht auch keine Ausnahmen vor. Dies hat Folgen, welche so wohl nicht beabsichtigt waren: So wären beispielsweise Spam- und Virenscanner, Zugangskontrollen via Badge und sehr viele andere Routineentscheide erfasst, die aus Gründen der Effizienz dem Computer übertragen werden. Die Automatisierung ist ein zentraler Punkt der Digitalisierung und im heutigen wirtschaftlichen Umfeld von grundsätzlicher Bedeutung. Davon profitieren auch die Kunden, z.B. durch Objektivität der Entscheidung, schnellere Prozesse und damit besserer Nutzererfahrung sowie einer attraktiven Preisgestaltung.

Insbesondere das vorgesehene Äusserungsrecht bringt keinen Mehrwert; es ist angesichts der neu vorgesehen Informationspflicht auch schlicht unnötig und für die Unternehmen wettbewerbs- und innovationsbehindernd. In der Praxis würde es wohl regelmässig zu einer Begründungspflicht führen und damit die Vertragsfreiheit der Unternehmen über Gebühr einschränken. Die Offenlegung, wie bestimmte Entscheide zustande gekommen sind, betrifft zudem oft auch Geschäftsgeheimnisse.

Die Bestimmung ist entsprechend auf schwere Fälle, bzw. solche, die erhebliche Auswirkungen auf die betroffene Person haben, zu begrenzen. Der Wortlaut ist an die entsprechende Bestimmung in der DSGVO anzupassen (insbesondere «Beeinträchtigung» statt «Wirkung» und «erhebliche» in Bezug auf beide Alternativen). Auch dann sind sinnvolle Ausnahmen notwendig, welche zumindest auf dem Verordnungsweg vorzusehen sind. Eine einmalige angemessene Information ohne ausdrückliche Einwilligung i.S.d. Gesetzessystematik ist ausreichend. Das Äusserungsrecht und der damit zusammenhängende Art. 20 Abs. 3 (Auskunftsrecht) sind zu streichen. Dies ist aufgrund des Derogationsrechts der Mitgliedstaaten der EU für die Äquivalenz nicht abträglich (vgl. Art. 22 Abs. 2 lit. c DSGVO).

10.3 Datenschutz-Folgenabschätzung

Beschränkung und Präzisierung / keine Pflicht des Auftragsdatenbearbeiters
Das in Art. 16 neu eingeführte Instrument der Datenschutz-Folgenabschätzung (Privacy Impact Assessment) ist zu weit gefasst. Die offene und dadurch unklare Formulierung führt dazu, dass für praktisch alle Datenbearbeitungen vorgängig aufwändige Abklärungen durchgeführt werden

müssten. Besonders problematisch ist die vorgesehene Sanktionierung bei Verstoss. Analog DSGVO ist eine Konkretisierung sowie eine Beschränkung auf Fälle vorzunehmen, bei denen ein *«hohes Risiko»* besteht. Darüber hinaus ist zu präzisieren, dass ein Risiko für eine Persönlichkeitsverletzung bestehen muss. Der Begriff «oder die Grundrechte» ist sodann zu streichen: Das Schweizer Recht kennt, anders als das europäische Recht, keine direkte Drittwirkung der Grundrechte. Schliesslich ist der Auftragsdatenbearbeiter von der Pflicht auszunehmen. Dieser verfügt regelmässig nicht über die notwendigen Angaben, sondern unterliegt den Entscheidungen des Verantwortlichen.

Keine Meldung oder nur bei Restrisiko und Verkürzung der Frist
Die anschliessenden umfangreichen Meldepflichten sind ein klares «Swiss Finish»; sie sind unverhältnismässig und greifen in die Geheimsphäre der Unternehmen ein. Die zu erwartende «Meldeflut» ist für eine angemessene Reaktion des EDÖB kontraproduktiv. Problematisch ist auch die lange Frist, innert welcher der EDÖB Einwände mitteilen oder später eine Untersuchung einleiten kann. Damit werden falsche Anreize gesetzt. In der Gesamtheit bringt die Bestimmung keinen Mehrwert, führt jedoch zu erheblichen Rechtsunsicherheiten und innovationshemmenden Verzögerungen. Die Forderung der Konvention 108, bei geplanten Datenbearbeitungen Risiken einzuschätzen, wurde bereits durch Art. 11 VE-DSG (Datensicherheit) erfüllt. Schliesslich bestehen weitere Spezialregeln, welche bestimmte Datenflüsse bereits einer anderweitigen Überwachung unterstellen (z.B. im Bankengesetz). Doppelte Überwachungen sind aus Effizienzgründen zu vermeiden.

Eine Meldung an den EDÖB sollte nur dann erfolgen müssen, wenn *nach* ergriffenen Schutzmassnahmen ein grosses Restrisiko verbleibt. Es ist klar zu regeln, welche Informationen weitergeleitet werden müssen und wie damit bei Informationszugangsgesuchen nach dem Öffentlichkeitsgesetz umgegangen wird. Weiter ist die vorgesehene Reaktionszeit des EDÖB von drei Monaten, welche zudem laufend verlängert werden kann, auf einen Monat zu reduzieren.

Einige Mitglieder sprechen sich für die gänzliche Streichung der Meldepflicht und folglich auch von Art. 16. Abs. 4 VE-DESG aus. Auch die E-SEV 108 verlange nicht, die Behörden von der Datenschutz-Folgenabschätzung zu informieren. Eine Ausnahme der Meldepflicht sollte zumindest für Unternehmen mit einem betrieblichen Datenschutzbeauftragten vorgesehen werden.

10.4 Meldepflichten

Beschränkung auf Verstösse mit gravierenden Folgen / Begrenzung der Weitermeldung
Die vorgesehene unverzügliche Meldepflicht im Falle sämtlicher Datenschutzverstösse (inkl. Datenverluste) an den EDÖB (Data Breach Notification) ist stark einzuschränken. Sie erfasst weit mehr Fälle als die DSGVO, welche diese Pflicht nur für Verletzungen von Sicherheitsmassnahmen vorsieht, die zusätzlich zu einem Bruch oder Verlust des Gewahrsams an den Daten führen. Ausserdem kann die vorgesehene Ausnahme sachlogisch nie angerufen werden, da eine «falsche» Datenbearbeitung per Definition immer eine Verletzung von Persönlichkeitsrechten ist. Eine Pflicht ohne Eingrenzung in qualitativer und quantitativer Weise würde uferlos; jeder noch so geringe Verstoss müsste gemeldet werden, um den Sanktionsfolgen zu entgehen. Der Beauftragte sähe sich mit einer weiteren Meldungsflut konfrontiert und wäre ausser Stande, allfällig wichtige Meldungen zeitgerecht zu erkennen und geeignete Massnahmen einzuleiten. Die Meldepflicht führt auch zu einem Konflikt mit dem strafrechtlichen Grundprinzip von «nemo tenetur»[2]. Schliesslich wäre eine «unverzügliche» Meldung auch in zeitlicher Hinsicht nicht umsetzbar, da zuerst

[2] Vgl. mehr dazu unter „Aufsicht und Sanktionen".

hinreichende Informationen gesammelt werden müssen. So sieht die DSGVO eine Frist von bis zu 72 Stunden vor.

Der Begriff des «Data Breach» sollte analog E-SEV und DSGVO formuliert werden. Die Pflicht wäre damit auf Verstösse mit gravierenden Folgen zu beschränken. Als weiteres qualitatives Kriterium müsste die Tatsache ergänzt werden, dass durch die Meldung an den Beauftragten ein Mehrwert geschaffen werden kann. Dies z.B. mittels Unterstützung in Fällen, welche von den Verantwortlichen nicht mehr aus eigener Kraft bereinigt werden können. Weiter ist die Bestimmung durch ein quantitatives Element zu konkretisieren, z.B. auf Fälle, in welchen Daten von mindestens 100'000 Personen betroffen sind. Eine Meldung beim EDÖB muss den Schutz vor Sanktionen zur Folge haben (vgl. nachfolgend Ziff. 14.3). Die Weitermeldungspflicht an Dritte ist auf diejenigen Fälle zu begrenzen, bei denen die betroffene Person ein schützenswertes Interesse hat oder das Vorgehen auf Vorstoss der betroffenen Person zurückzuführen ist.

10.5 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Anpassung der Reichweite und Überführung zu den Sicherheitsbestimmungen
Die Formulierung von Art. 18 VE-DSG geht ebenfalls über jene der DSGVO hinaus. Zudem gehört diese systematisch zu Art. 11 VE-DSG (Sicherheit von Personendaten). Diese Bestimmung deckt die Anforderungen von «privacy by design» bereits. Art. 18 VE-DSG ist zu streichen, resp. in Art. 11 zu integrieren. Die Reichweite ist an das EU-Recht anzupassen.

10.6 Weitere Pflichten

Verzeichnis statt allgemeine Dokumentationspflicht / Ausnahme bis 250 Mitarbeitende
Die allgemeine Dokumentationspflicht von Art. 19 lit. a VE-DSG ist bezüglich Inhalt und Umfang unklar und geht über die vergleichbare Bestimmung der EU hinaus. Die Pflicht ist analog der DSGVO auf die Pflicht zur Erstellung «eines Verzeichnisses für regelmässige Datenbearbeitungen» einzuschränken. Die Pflicht, Datenschutzverstösse zu dokumentieren, ist zu weitgehend. Darüber hinaus ist auch eine Ausnahme der Pflicht für Unternehmen mit weniger als 250 Mitarbeitenden vorzusehen. Aus systematischen Gründen sollte auch diese Bestimmung in Art. 11 VE-DSG integriert werden.

Beschränkung der Informationspflicht an Dritte
Die Reichweite der neu vorgesehenen Pflicht, Dritten die Berichtigung, Löschung oder Vernichtung von Daten zu melden, geht sehr weit und ist in der Praxis nicht umsetzbar. Eine solche Meldepflicht ist von E-SEV 108 nicht und von der DSGVO nicht in dieser Form vorgesehen. Die DSGVO kennt eine entsprechende Meldepflicht nur unter gewissen Voraussetzungen im Zusammenhang mit dem «Recht auf Vergessen». Der VE-DSG erfasst demgegenüber auch unbedeutende Vorgänge; im täglichen Arbeitsprozess werden ständig Daten berichtigt, gelöscht oder vernichtet (z.B., weil ein Kunde bezahlt hat oder die Daten schlicht keine Relevanz mehr haben). Die Auswirkungen dieser Meldepflicht wurden offenbar überschätzt. Zu deren Bewältigung müsste eine neue Infrastruktur aufgebaut werden, welche sämtliche Empfänger über Jahrzehnte hinweg verwaltet. Eine betroffene Person ist besser in der Lage zu beurteilen, welche Daten für welche Empfänger (noch) von Interesse sind. Gerade solche Informationsansprüche der betroffenen Person sind aber bereits unter Art. 25 VE-DSG vorgesehen. Die Informationspflicht an Dritte ist analog der DSGVO auf Fälle zu beschränken, in welchen die betroffene Person die Nachinformation aus berechtigten Gründen verlangt hat.

11. Auskunftsrecht

Massnahmen gegen missbräuchliche Auskunftsbegehren
Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen und hängige Verfahren bringt grosse Aufwendungen mit sich. Umso mehr, weil ein Auskunftsbegehren im Datenschutzsystem der Schweiz nie unverhältnismässig sein kann, da auch untergeordnete Datenschutzinteressen für einen Anspruch ausreichen. Gerade auch die vorgesehene umfassende Kostenlosigkeit des Auskunftsrechts führt zu Fehlanreizen: Es sind keine Massnahmen vorgesehen, welche es den Unternehmen erlauben würden, dem Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken Einhalt zu gebieten (vgl. Ziff. 3).

Es sind griffige Massnahmen gegen den Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken vorzusehen: Die Kostenlosigkeit ist zu relativieren, so z.B. bei unverhältnismässigem Aufwand und bei Ersuchen zu nicht ausschliesslich datenschutzrechtlichen Zwecken. Zudem sind weitere Mechanismen zur Verhinderung des Auskunftsrechts bei offensichtlich nicht datenschutzrechtlichen Zwecken vorzusehen (z.B. bei Art. 21 VE-DSG).

Deutliche Einschränkung der Informationspflicht bei automatisierten Einzelfallentscheiden
Eine «Rechenschaftspflicht» in Bezug auf automatisierte Entscheide in der vorgesehenen detaillierten Form ist unverhältnismässig: Informationen darüber, wie bestimmte Entscheide zustande kommen, gehören zum Geschäftsgeheimnis. Durch die gewählte Formulierung wäre jedes Ergebnis, d.h. jeder Entscheid erfasst. Dies würde zu einem zusätzlichen Administrativaufwand führen, ohne dass damit mehr Transparenz geschaffen würde. Im Gegenteil: Kunden würden Informationen erhalten, mit denen sie gar nichts anzufangen wissen (z.B. warum sie eine Werbeanzeige nicht erhalten haben).

Die geforderte Information über Vorliegen einer automatisierten Einzelfallentscheidung (Art. 20 Abs. 2 lit. e VE-DSG) sollte in allgemeiner Weise erfolgen. Die Bestimmung von Art. 20 Abs. 3 VE-DSG sollte in Art. 15 VE-DSG integriert werden. Dessen Grundsätze («erhebliche Auswirkung») wären dabei einzuhalten. Es muss klargestellt werden, dass das Auskunftsrecht nur von der jeweils tatsächlich betroffenen Person ausgeübt werden kann. Zudem ist ein Verweis auf die Einschränkungen des Auskunftsrechts bzw. der Informationspflichten (Art. 21 i.V.m. 14 VE-DSG) anzubringen.

12. Ausnahmetatbestände

Die vorgesehenen Ausnahmetatbestände gemäss Art. 14 VE-DSG sind zu eng formuliert und nicht konsistent. Die Informationspflicht sollte immer entfallen, wenn die Information nicht möglich oder unzumutbar ist. Eine Beschränkung auf Fälle der indirekten Beschaffung oder in denen keine Weitergabe an Dritte erfolgte ist nicht nachvollziehbar. Die Bestimmung ist entsprechend anzupassen.

Weitere Ausnahmen, auch in Hinblick auf die rechtsmissbräuchliche Geltendmachung des Auskunftsrechts, sind für folgende bearbeiteten Daten vorzusehen:

— Daten, welche die betroffene Person bereits erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen;

— Aufgrund einer gesetzlichen Pflicht bearbeitete Daten, z.B. zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption;

— Daten, welche vom Auskunftspflichtigen als Geschäftsgeheimnisse qualifiziert werden;

— Rein intern bearbeitete Daten;

— Daten über Drittpersonen;

— Unter rechtsmissbräuchlichen Umständen herausverlangte Daten, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder mit häufiger, sachlich nicht nachvollziehbarer Wiederholung.

Übergabe der Informationen an Dritte bei Missbrauchsverdacht
Um Missbräuche zu verhindern, ist zudem vorzusehen, dass bei begründetem Verdacht auf Missbrauch die herauszugebenden Personendaten einem Dritten (bspw. dem EDÖB) übergeben werden können. Dieser würde anstelle des Gesuchstellers die Einhaltung bzw. Verletzung des Datenschutzes prüfen. Eine Möglichkeit bestünde darin, dass der EDÖB den Entscheid über Herausgabe in Form einer anfechtbaren Verfügung vorlegt (vgl. analoge Regelung in Art. 8 Abs. 2 BPI).

13. Besondere Bestimmungen für die Datenbearbeitung durch private Personen

Keine ausdrückliche Einwilligung beim Profiling
Gemäss Art. 23 Abs. 2 lit. d VE-DSG gälte Profiling automatisch als Persönlichkeitsverletzung, wenn nicht vorgängig eine ausdrückliche Einwilligung eingeholt wird. Diese gesetzliche Vermutung stellt einen unbegründeten partiellen Paradigmenwechsel im Schweizer Datenschutzrecht dar (von grundsätzlicher Erlaubnis der Datenbearbeitung unter Einhaltung bestimmter Voraussetzungen zum Verbot mit Erlaubnisvorbehalt). Das Erfordernis der ausdrücklichen Einwilligung beim Profiling ist entsprechend zu streichen. Durch eine entsprechende Information kann genug Transparenz geschaffen werden. Eine Regelung hat unter Art. 15 VE-DSG zu erfolgen.

Klare und erweiterte Rechtfertigungsgründe
Der Ausdruck «möglicherweise» in Art. 24 Abs. 2 VE-DSG schafft Rechtsunsicherheit. Die aktuelle Bestimmung (Art. 13 Abs. 2 DSG) wurde unnötigerweise geändert und sollte beibehalten werden.

Art. 24 Abs. 2 lit. a VE-DSG sollte analog Art. 6 Abs. 1 lit. b VE-DSG Verträge berücksichtigen, die zu Gunsten oder im Interesse der betroffenen Person geschlossen werden.

14. Aufsicht und Sanktionen

Das vorgeschlagene Sanktionsmodell wurde in unserer internen Vernehmlassung breit kritisiert. Angesichts dieser Kritik und der Bedeutung der Thematik wird zum Thema Aufsicht und Sanktionen in detaillierterer Form Stellung genommen. Zudem präsentiert die Wirtschaft im Folgenden eine Grobskizze für einen eigenen Vorschlag eines Sanktionsmodelles im Datenschutzgesetz.

14.1 Ausgangslage

Anders als die Schweiz setzen die Konvention 108 und EU-Verordnung in erster Linie auf Verwaltungssanktionen gegen Unternehmen. Bei der Regelung der Sanktionierung von Datenschutzverletzungen besteht aber ein erheblicher Spielraum: Die Konvention verlangt im Wesentlichen *geeignete gerichtliche und nicht-gerichtliche Sanktionen* (Art. 10 E-SEV 108). Die DSGVO (und auch die Richtlinie) sprechen von *wirksamen, verhältnismässigen und abschreckenden Sanktionen* und sehen explizit die Möglichkeit von strafrechtlichen Sanktionen vor (vgl. Erw. 149).

14.2 Kritik am Vorentwurf und weitere Überlegungen

Die Wirtschaft ist bei der Abwägung verschiedener Sanktionsmodelle zum Schluss gekommen, dass die im VE-DSG vorgesehenen Sanktionen und insbesondere der Weg über das Strafrecht nicht zielführend sind:

Persönliche Strafbarkeit der Mitarbeitenden
Die Mitarbeitenden eines Unternehmens geraten durch die persönliche Strafbarkeit zu stark in den Fokus der Sanktionen. Verschärft wird dies durch die Höhe der Bussen und die vorgesehene Möglichkeit der Bestrafung sogar des fahrlässigen Handelns. Damit wird der risikobasierte Ansatz, der mit der Revision verfolgt wird, untergraben.

Der strafrechtliche Charakter der Sanktionen führt dazu, dass Mitarbeitende selbständig jeden (möglichen) Verstoss bei den Behörden melden. Es bestünde sogar das Risiko, dass sie sich gegenseitig verzeigen, um nicht selber ins Visier der Strafbehörde zu geraten. Dies widerspricht der Idee einer guten Datenschutz-Governance. Der VE-DSG bietet Dritten viele Anknüpfungspunkte (sobald eine Datenerhebung stattgefunden hat), um Anzeige zu erstatten. Dies kann zu Unruhen innerhalb der Unternehmen mit entsprechenden Reputationsschäden führen.

Verurteilte Mitarbeitende wären stark exponiert. Es dürfte daher mittelfristig schwierig werden, qualifiziertes Personal zu finden, das bereit ist, die entsprechende Verantwortung zu tragen. Die Folge wäre eine sukzessive Senkung der Qualität.

Die persönliche Strafbarkeit der Mitarbeitenden entspricht auch nicht der von anderen Gesetzen vorgesehen Linie (vgl. KG, UWG, FMG, BEHG), bei welchen der Fokus klar auf der Sanktionierung der Unternehmen liegt.
Die strafrechtliche Sanktionierung würde schliesslich auch KMU stark belasten. Bei übersichtlichen Verhältnissen wäre die Identifikation fehlbarer Mitarbeitenden weit einfacher; entsprechend bestünde ein Anreiz für die Strafverfolgungsbehörden, gerade bei solchen Unternehmen unverhältnismässig streng vorzugehen.

Verstoss gegen strafrechtliche Grundprinzipien
Problematisch sind die im VE-DSG vorgesehenen Mitwirkungspflichten, dies angesichts des im Strafrecht vorherrschenden Grundsatzes des «nemo tenetur» bzw. des Selbstbelastungsverbotes. Gerade die Pflicht, Datenschutzverstösse zu melden, käme faktisch einer Pflicht zur Selbstanzeige gleich. Der Vorentwurf geht von einer verschuldensunabhängigen Sanktionierung aus und steht damit im Widerspruch zum Verschuldensprinzip: bei Erfüllung des objektiven Tatbestandes wird direkt auf die Erfüllung des subjektiven Tatbestandes geschlossen. Viele der Pflichten des VE-DSG und damit auch die daraus abgeleiteten Straftatbestände sind offen formuliert (vgl. Art. 16 Abs. 1 VE-DSG: *"...vorgesehene Datenbearbeitung [führt] voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person"*). Dies ist in Hinblick auf das

strafrechtliche Bestimmtheitsgebot bzw. eine hinreichende Voraussehbarkeit einer Norm klar abzulehnen.

Umfang von Verstössen und Meldungen
Datenbearbeitungen stellen eine alltägliche Aktivität der Unternehmen dar. Unternehmen können im Zeitalter der Digitalisierung nicht wählen, eine entsprechende Handlung vorzunehmen oder nicht. Damit unterscheidet sich das Datenschutzrecht beispielsweise vom Kartellrecht. Im VE-DSG sind kaum Erheblichkeitsschwellen vorgesehen. Folglich würden regelmässig alltägliche Vorgänge erfasst und es würden bereits auf Grund geringfügiger Vorfälle «data breaches» vorliegen. Zusammen mit den drastischen Sanktionsfolgen wäre dies auch aufgrund der daraus resultierenden Mitteilungsmenge an den EDÖB problematisch.

Strafkatalog
Im Kern entspricht der Strafkatalog grundsätzlich den europäischen Bestimmungen. Hingegen werden die Berufspflichten stark ausgebaut und es wird sogar eine Freiheitsstrafe als Sanktion vorgesehen. Diese Ausweitung der Berufspflichten ist als überschiessende Bestimmung klar abzulehnen.

Fazit
Der persönliche und strafrechtliche Charakter der Sanktionen des VE-DSG ist nicht zielführend. Er steht im Widerspruch zu gleich mehreren strafprozessualen Prinzipen. Die auf Risikoausgleich ausgerichteten Möglichkeiten des VE-DSG werden damit ausgehöhlt und der Interessensausgleich wird unnötig eingeschränkt. Gesamthaft geht das vorgeschlagene strafrechtliche Sanktionsmodell damit deutlich über die im europäischen Raum vorgesehenen Sanktionen hinaus.

14.3 Vorschlag der Wirtschaft für ein Sanktionsmodell im DSG

Aufgrund der vorangehenden Überlegungen sprechen wir uns für ein alternatives Sanktionsmodell aus. Nicht strafrechtliche Sanktionen gegen Individuen, sondern Verwaltungsstrafen gegen Unternehmen sollen dabei im Vordergrund stehen.

Auch bei Verwaltungsstrafen ergeben sich verschiedene Problemfelder, gerade auch aus rechtsstaatlicher Sicht. Das nachfolgend skizzierte Modell berücksichtigt diese und schlägt ein auf die spezielle Konstellation des Datenschutzes angepasstes, verwaltungsrechtliches Sanktionsmodell vor. Dieses soll effizient ausgestaltet sein, die richtigen Anreize setzen und den Anforderungen an ein faires Verfahren entsprechen.

Grundsatz: verwaltungsrechtliche Sanktionen für Unternehmen
Das DSG soll bei Verstössen gegen die Datenschutzbestimmungen eine Sanktionierung der Unternehmen vorsehen. Anknüpfungspunkt sind dabei Organisationsmängel des Unternehmens. Normalerweise sollte lediglich subsidiär eine strafrechtliche Verfolgung von Mitarbeitenden möglich sein. Dies verbunden mit der Einschränkung, dass in der Regel die Unternehmen selbst Anzeige erstatten. Dies würden sie in der Praxis tun, wenn sie ihre aktive Mitwirkung darlegen und aufzeigen könnten, dass eine Verletzung nicht auf einen Organisationsmangel zurückzuführen ist. Im Ergebnis würde eine Anpassung des Sanktionsziels die Situation für die Datenbearbeitenden im Sinne einer Verbesserung des Datenschutzes im Unternehmen massgeblich entschärfen.

Weiter soll eine Sanktionierung der natürlichen Personen nur bei direkt vorsätzlichem Handeln gegen die Interessen der Unternehmen in Frage kommen. Eine Abstimmung mit den bereits im BT StGB vorgesehenen Strafbestimmungen im Zusammenhang ist hierbei erforderlich. Die bereits vorhandenen strafrechtlichen Tatbestände (z.B. Verletzung des Geschäftsgeheimnisses und unbefugte Datenbeschaffung) dürften grösstenteils schon ausreichen.

Schliesslich ist der Kreis der potentiell strafrechtlich verantwortlichen Mitarbeitenden zum Vornherein einzuschränken. Es kommen i.S.v. Art. 29 StGB primär die folgenden Mitarbeiterkreise in Frage:

— VR- und GL-Mitglieder der Gesellschaft;

— VR- und GL-Mitglieder der Muttergesellschaft, falls sie bei der Tochter faktische Entscheidungskompetenzen in Anspruch nehmen;

— Mitglieder einer Kollektivgesellschaft;

— ggf. die für den Datenschutz eigenverantwortlichen Mitarbeitenden im Rechtsdienst;

— ggf. ein Compliance-Officer;

— ggf. interne und externe Datenschutzbeauftragte.

Angepasste Rolle des EDÖB und verbesserte Gewaltentrennung über eine neue Spruchbehörde
Eine Behörde, die gleichzeitig über Untersuchungs- und Spruchkompetenzen verfügt, hat die Tendenz, eine mit dem Prinzip der Gewaltenteilung nur schwer vereinbare Machtfülle zu erlangen. Die Verwaltungssanktionen sollten daher nicht von der Untersuchungsbehörde verhängt werden.

Die Ausstattung des EDÖB mit Spruchkompetenzen, sogar die im VE-DSG bereits vorgesehene Ausstattung mit Verfügungskompetenzen, kann dazu führen, dass der EDÖB zu mächtig wird und dass damit auch die Zusammenarbeit mit den Unternehmen beeinträchtigt wird. Ein auf Vertrauen basierender Austausch mit den Unternehmen ist für die Tätigkeit des EDÖB von grundsätzlicher Bedeutung; umso mehr, als ihm nach VE die Aufgabe zukommt, Empfehlungen der guten Praxis zu erlassen.

Die Verfügungskompetenzen sowie die Sanktionskompetenz könnten entsprechend in einer neuen «Datenschutz-Kommission» gebündelt werden. Diese könnte beispielsweise dem EDI oder EJPD angehängt sein. Ausschliesslich dieser käme nebst der Sanktionskompetenz auch die Verfügungskompetenzen zu, dies gerade auch im Bereich vorsorglicher Massnahmen.

Das Verhältnis zwischen «Datenschutz-Kommission» und EDÖB müsste präzisiert werden, dies insbesondere in Bezug auf die Überwachungs- und Untersuchungskompetenzen des Beauftragten i.S.v. Art. 40 f. VE-DSG.

In dieser Struktur würde der EDÖB seine bisherigen Aufgaben wahrnehmen und eine Vorselektion der ihm zugetragenen Fälle machen. Sollte sich in einem Fall eine mögliche Strafbarkeit abzeichnen, würde er die Angelegenheit der Datenschutz-Kommission weiterleiten. Bei Verfahren auf dieser zweiten Stufe würde die verwaltungsrechtliche Mitwirkungspflicht wegfallen. Gegen Entscheide dieser Spruchbehörde stünde den Betroffenen der Weg zum Bundesverwaltungsgericht als Rechtsmittelinstanz offen.

Strafkatalog
Der Strafkatalog ist mit jenem der DSGVO abzugleichen, soll jedoch nicht darüber hinausgehen. Folgende Anpassungen sind erforderlich:

— Streichung der Strafandrohung bei verweigerter Mitwirkung / Kooperation ab 2. Stufe des Verfahrens (siehe unten);

— Konkretisierung / Streichung der zu offen formulierten Tatbestände;

— Beschränkungen und Anpassungen bei den Pflichten sind beim Strafkatalog zu berücksichtigen;

— Fokus auf wesentliche Bedrohung für die Privatsphäre;

— Einführung einer Erheblichkeitsschwelle, welche sich z.B. an der Schwere der Persönlichkeitsverletzung (in quantitativer oder qualitativer Hinsicht) oder an der Höhe des entstandenen Schadens orientiert. Zu einem schweren Verstoss gegen das Datenschutzgesetz gehört auch, dass die unbefugte Datenbearbeitung vorsätzlich vorgenommen wurde;

— Verzicht auf die Pönalisierung von reinen Fahrlässigkeitsdelikten;

— Beschränkung des allgemeinen Berufsgeheimnisses auf Fälle, in denen der Geheimnisherr eine berechtigte Erwartung der Geheimhaltung hat (z.B. aufgrund eines Vertrages). Angeregt wurde auch, den heutigen Art. 35 DSG beizubehalten sowie die Bestimmung ins StGB zu übertragen.

Offen ist die Frage, ob aus Gründen der Äquivalenz bei Verstössen gegen Bearbeitungsgrundsätze eine Sanktionierung erforderlich ist.

Mitwirkungspflichten und Rechtfertigungsgründe

Neben der im Vorentwurf vorgesehenen Pflicht, Datenschutzverstösse bei den Behörden zu melden, besteht für die Unternehmen im verwaltungsrechtlichen Verfahren generell eine Mitwirkungspflicht. Wie oben kritisiert, ist eine anschliessende Bestrafung im Rahmen eines Strafverfahrens widersprüchlich und verstösst gegen das Selbstbelastungsverbot. Ein kooperatives Verhalten im Sinne einer Schadensminderung soll gefördert werden. Unternehmen, die den EDÖB informieren, mit den Behörden kooperieren und Fehler aktiv korrigieren sowie grössere Risiken zu verhindern suchen, sollen mit einer Reduktion der Sanktion oder gar einem Ausschluss der Sanktion belohnt werden (vgl. auch Art. 49a Abs. 2 KG). Dieser auf Schadensminderung ausgerichtete Ansatz entspricht den modernen Grundsätzen der Corporate Governance und fördert gleichzeitig das Ziel eines hohen Datenschutzniveaus. Gründe, die als eine Art Rechtfertigung beigezogen werden können, sind:

— Compliance-Defense: Implementierung eines tauglichen Compliance-Programmes;

— Einhaltung der Corporate Governance: Einhalten sämtlicher unternehmensinternen Regulative, Ausschöpfen der betriebsinternen Eskalationsleiter und Interventionsmöglichkeiten, Meldung eines möglichen Verstosses sowie kooperatives Verhalten gegenüber den Behörden;

— Handeln nach Treu & Glauben durch vernünftigen Umgang mit komplexen Regeln: Angemessene Umsetzung komplexer Verhältnisse (u.a. viele Beteiligte und grenzüberschreitende Verhältnisse) unter Berücksichtigung des «state of the art» und bei bestehender Rechtsunsicherheit;

— Wahrung berechtigter Interessen: Rechtfertigende Pflichtenkollision mit anderen zwingenden Rechtsregeln, welche in einer Güterabwägung im konkreten Fall überwogen haben.

Beispielsweise unter Zeitdruck angewendete etablierte Notfallszenarien (BCM) im öffentlichen Interesse zur Abwendung eines Unternehmenskonkurses (vgl. Notstand, Art. 17 StGB);

— Rechts- und Sachverhaltsirrtum (vgl. Art. 13 und 21 StGB);

— Strafrechtliche Verfolgung eines Mitarbeitenden. Eine Anzeige gegen einen direktvorsätzlich handelnden Mitarbeitenden durch das Unternehmen muss im Rahmen der Bestrafung des Unternehmens, insbesondere im Hinblick auf das Schuldprinzip, berücksichtigt werden;

— Aktive Schadensverminderung und damit die aktive Zusammenarbeit mit den Behörden im Falle einer Verletzung.

Sanktionen
Der Vorentwurf sieht eine maximale Busse von CHF 500'000 vor. Im Lichte der internationalen Vorgaben wird dies offenbar als ausreichend angesehen. Bei Verwaltungssanktionen sind in der Regel höhere Bussen, bei Unternehmen oft umsatzbezogen, vorgesehen. Datenbearbeitungen gehören jedoch zur täglichen Arbeit der Unternehmen; Verletzungen können entsprechend im Rahmen des Tagesgeschäftes geschehen. Dies muss einen Einfluss auf die Festlegung der Sanktionshöhe haben. Hierbei sind die gesamten Umstände zu berücksichtigen, darunter die Schwere und die Auswirkungen des Verstosses sowie die genannten Rechtfertigungsgründe. Als absolute Grenze ist eine maximale Busse von CHF 1 Mio. vorzusehen, welche aber regelmässig durch die genannten Kriterien relativiert werden muss. Zudem müssen auch andere Sanktionsformen wie administrative Rechtsnachteile in Betracht gezogen werden.

15. Übergangsfristen

Im VE-DSG fehlt eine umfassende Übergangsregelung. Die neuen und revidierten Bestimmungen werden die Prozesse der Unternehmen bedeutend beeinflussen. Es ist deshalb eine allgemeingültige Übergangsbestimmung von 2 Jahren aufzunehmen. Von einer Rückwirkung ist abzusehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

Katrin Portmann
Geschäftsleiterin

Joel Thiébaud
Generalsekretär

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Der stellvertretende Beauftragte

CH-3003 Bern, EDÖB, GL

VFAS
Verband freier Autohandel Schweiz
Herr Roger Kunz, Präsident
Herr Joel Thiébaud, Generalsekretär
Bremgartenstrasse 75
5610 Wohlen

Ihr Zeichen:
Unser Zeichen: A2015.06.30-0017 / GL
Sachbearbeiter/in: Caroline Gloor Scheidegger
Bern, 06.07.2015

Bekanntgabe von Fahrgestellnummern (VIN) durch das ASTRA

Sehr geehrter Herr Kunz
Sehr geehrter Herr Thiébaud

Wir beziehen uns auf Ihre Schreiben vom 2., 12. und 30. Juni 2015 sowie unsere Empfangsbestätigung vom 8. Juni 2015 und nehmen wie folgt Stellung:

Wie wir Ihnen in unserer Empfangsbestätigung vom 08.06.15 bereits mitgeteilt haben, hat uns das ASTRA zur Frage der Bekanntgabe der VIN-Nummer kontaktiert. Bei der Prüfung der Frage haben wir uns auf die rein datenschutzrechtlich relevanten Punkte beschränkt und sind, zusammengefasst, zu folgendem Schluss gekommen:

Zuerst haben wir geprüft, ob die VIN-Nummern als Personendaten im Sinne des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) gelten, da das DSG nur anwendbar ist, wenn Personendaten bearbeitet werden. Als Personendaten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Zudem fallen in der Schweiz unter dem Begriff Personendaten natürliche und juristische Personen (vgl. zum Ganzen Art. 2 Abs. 1 und Art. 3 Bst. a DSG). Wir kamen zum Schluss, dass die VIN-Nummern als Personendaten im Sinne des DSG zu betrachten sind. Denn einerseits ist davon auszugehen, dass die Datenbezüger aus dem Autogewerbe mit Hilfe der ihnen zur Verfügung stehenden technischen Mittel in der Lage wären, den Halter oder den Käufer aufgrund der vorhandenen Angaben zu identifizieren. Andererseits kann mit der VIN-Nummer resp. dem darin enthaltenen WMI-Code, und einer Internetsuche der Hersteller bestimmt werden.

Da die VIN-Nummern als Personendaten gelten, muss das ASTRA bei der Bekanntgabe dieser Daten das DSG einhalten. Als Bundesorgan darf das ASTRA die VIN-Nummer nur bekannt geben, wenn dafür eine gesetzliche Grundlage besteht. Wie uns das ASTRA erklärte, gibt es zurzeit keine entsprechende gesetzliche Grundlage. Wir haben das ASTRA darauf hingewiesen, dass eine gesetzliche

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Grundlage nur geschaffen werden könne, wenn die Bekanntgabe der VIN-Daten auch die allgemeinen Datenschutzgrundsätze (wie Verhältnismässigkeit, Zweckbindung, usw.; vgl. Art. 4 ff. DSG) einhalten würde. Dies müsste sorgfältig geprüft werden.

Aufgrund unserer Analyse gehen wir davon aus, dass sich nun die Frage des persönlichen Gesprächs erübrigt hat. Gerne stehen wir Ihnen für allfällige Fragen weiterhin zur Verfügung.

Mit freundlichen Grüssen

Jean-Philippe Walter

CC: Bundesamt für Strassen ASTRA, Herr Benno Nager, 3003 Bern

VEREINIGUNG PHARMAFIRMEN
IN DER SCHWEIZ

ASSOCIATION DES ENTREPRISES
PHARMACEUTIQUES EN SUISSE

BAARERSTRASSE 2
POSTFACH 4856
CH-6304 ZUG
TELEFON 041 727 67 80
TELEFAX 041 727 67 90
E-MAIL info@vips.ch
www.vips.ch

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

3. April 2017

Vorentwurf zum Bundesgesetz über den Datenschutz
Stellungnahme der vips Vereinigung Pharmafirmen in der Schweiz

Sehr geehrte Damen und Herren

Die vips Vereinigung Pharmafirmen in der Schweiz vertritt die Interessen von über 60 in der Schweiz tätigen Pharmaunternehmen. Im Rahmen der Vernehmlassung zum oben erwähnten Thema erlauben wir uns, Ihnen in der Anlage unsere Standpunkte zu senden. Diese entsprechen denjenigen, der scienceindustries. Deshalb legen wir unserem Schreiben der Einfachheit halber die Stellungnahme der scienceindustries vom 30. März 2017 bei und danken Ihnen für die Berücksichtigung der darin erwähnten Punkte.

Mit freundlichen Grüssen

vips Vereinigung Pharmafirmen
in der Schweiz

Walter P. Hölzle
Präsident

Thomas Binder
Geschäftsführer

- Briefkopie Stellungnahme scienceindustries vom 30.03.17

scienceINDUSTRIES
SWITZERLAND

Eidgenössiches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

scienceindustries
Wirtschaftsverband Chemie Pharma Biotech

Nordstrasse 15 · Postfach · 8021 Zürich
info@scienceindustries.ch
T +41 44 368 17 11
F +41 44 368 17 70

Zürich, 30. März 2017

Vorentwurf zum Bundesgesetz über den Datenschutz

Stellungnahme von scienceindustries

Sehr geehrte Damen und Herren

Wir beziehen uns auf den erläuternden Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG) sowie die Änderungen weiterer Erlasse zum Datenschutz und danken Ihnen für die Gelegenheit, dazu Stellung nehmen zu können.

scienceindustries ist der Schweizer Wirtschaftsverband Chemie Pharma Biotech. Sie vertritt die wirtschaftspolitischen Interessen von mehr als 250 in der Schweiz tätigen in- und ausländischen Unternehmen aus genannten und verwandten Branchen. Unsere Mitgliedunternehmen, darunter nicht weniger als sechs SMI- und zahlreiche andere kotierte Firmen, beschäftigen in der Schweiz rund 70'000 Mitarbeitende und leisten einen sehr wesentlichen Beitrag zum Wohlstand unseres Landes: rund 45% aller Schweizer Exporte stammen von ihnen und 40% der gesamten privatwirtschaftlichen Investitionen in Forschung und Entwicklung in der Schweiz werden von unseren Mitgliedfirmen getätigt. Die überwiegende Mehrheit unserer Mitgliedunternehmen sind global tätig, erzielen dabei im Schnitt rund 98% ihrer Umsätze im Ausland und beschäftigen dort zusätzlich über 320'000 Mitarbeitende. Die vielfältigen Aktivitäten unserer Industrie führen zwangsläufig zu mannigfachen Datenbearbeitungen sowie zu einem regen Datenaustausch im In- wie Ausland resp. auch grenzüberschreitend. Die Thematik ist entsprechend von eminenter Bedeutung für alle unsere Mitgliedfirmen: eine pragmatische Regelung ist dabei genauso anzustreben, wie auch gleichzeitig eine international kompatible Lösung, die einen reibungslosen Datenaustausch in andere Länder garantiert.

Klärend sei an dieser Stelle festgehalten, dass die vorliegende Stellungnahme aus Rücksicht auf die unmittelbare Betroffenheit der Unternehmen sowie die vorhandene Expertise nur auf den Vorentwurf zum Bundesgesetz über den Datenschutz (das DSG) und hierbei ausschliesslich auf jene Regelungen eingeht, welche die Privatwirtschaft direkt betreffen. Zu den übrigen sich in Revision befindlichen Rechtserlassen resp. Bestimmungen werden wir uns nicht äussern.

Äquivalenz als Massstab

Die Mitgliedfirmen von scienceindustries betreiben ein internationales Geschäft und finden sich dabei in einem sehr kompetitiven Umfeld wieder. Entsprechend wichtig ist es, dass die Rahmenbedingungen am Standort, wo die Firmen einen wesentlichen Teil ihrer Wertschöpfung erzielen, ein erfolgreiches Wirtschaften ermöglichen. Das Datenschutzrecht beschlägt zahlreiche Aktivitäten der Firmen und entfaltet somit direkte Auswirkungen auf die Rahmenbedingungen des Wirtschaftsstandortes, wobei das Schweizer Datenschutzkonzept sich bislang über weite Strecken bewährt hat. Im Bewusstsein um die Wichtigkeit des Themas sprechen sich unsere Mitgliedfirmen für einen angemessenen Datenschutz aus und setzen die entsprechenden Vorgaben in ihren Unternehmen um, was bereits heute einen beachtlichen Aufwand verursacht. Entsprechend gilt es Augenmass zu halten und inskünftig keine Regelungen einzuführen, die bei den Firmen zu weiteren grossen Aufwendungen führen, ohne dass gleichzeitig ein berechtigter Nutzen für die schutzbezogenen Personen resultiert. Auch bietet die Totalrevision die Gelegenheit, gewisse Regelungen im bestehenden Datenschutzgesetz, die sich nicht bewährt haben, zu überdenken und anzupassen.

Nach Ansicht von scienceindustries hat sich die Revision des DSG weitgehend auf das Notwendige zu beschränken und sich dabei an der Kompatibilität mit grundlegenden internationalen Vorgaben (insbes. das Übereinkommen SEV 108 sowie die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten) zu orientieren. Die grundsätzliche Äquivalenz des Schweizer Datenschutzniveaus mit diesen Vorgaben ist vor allem mit Blick auf die Fortführung des heute schon bestehenden Angemessenheitsbeschlusses durch die Kommission der Europäischen Union (EU) gerade für den grenzüberschreitenden Datenaustausch von zentraler Bedeutung. Ein revidiertes DSG muss diesen Anforderungen genügen, soll indes aus unserer Sicht nicht darüber hinausgehen und gleichzeitig bestehende Freiräume ausschöpfen.

Zentrale Anliegen der Lifescience-Industrie

- **Der Grundsatz der lex specialis ist umfassend zu verstehen: bereichsspezifische Datenschutzbestimmungen auf Gesetzes- sowie auf Verordnungsstufe müssen auch inskünftig dem DSG stets vorgehen, was insbes. für die Humanforschung von Bedeutung ist.**
- **Die Begriffe genetische wie biometrische Daten sind zu präzisieren sowie der gewählte Ansatz zum Profiling zu überarbeiten.**
- **Die Informations- und Auskunftspflichten müssen überarbeitet werden.**
- **Das Konzept des unabhängigen internen Datenschutzbeauftragten ist beizubehalten und damit verbunden sind Erleichterungen für die Verantwortlichen vorzusehen.**
- **Es sind Verwaltungssanktionen mit unmittelbarer Haftung der fehlbaren Unternehmen vorzusehen.**
- **Das Sanktionssystem ist in wesentlichen Teilen zu verbessern: insbes. ist auf Freiheitsstrafen zu verzichten und die fahrlässige Begehung straffrei zu halten.**

Grundsatz der lex specialis

Dem erläuternden Bericht zur DSG-Revision ist auf Seite 39 zu entnehmen, dass die lex specialis Regel uneingeschränkte Geltung haben soll und damit bereichsspezifische Datenschutznormen dem DSG auch weiterhin vorgehen sollen. Die uneingeschränkte Geltung dieses Grundsatzes ist angesichts der zahlreichen bereichsspezifischen Regelungen im Datenschutz von besonders grosser Bedeutung, weshalb scienceindustries die **ausnahmslose Geltung des Grundsatzes der lex specialis ausdrücklich begrüsst**. Gerade für die Lifescience-Industrie und hier im besonderen Ausmass für jene Unternehmen, die im Bereich der Humanforschung tätig sind, ist es von höchster Bedeutung, dass die bestehenden, spezifischen Datenschutzbestimmungen des Humanforschungsrechts sowie weiterer, unsere Industrie betreffende Rechtsbereiche uneingeschränkte Geltung behalten und ausnahmslos dem DSG vorgehen. Dabei ist zu beachten, dass eine Vielzahl entsprechender Regelungen nicht auf Gesetzesstufe, sondern in Verordnungen geregelt ist. Der **Grundsatz der lex specialis muss also umfassend verstanden** sein und sich nicht nur auf bereichsspezifische Bestimmungen **in anderen Gesetzen als dem DSG beziehen, sondern auch für entsprechendes Verordnungsrecht gelten.**

In diesem Zusammenhang führen die Erläuterungen unter Seite 70 des erläuternden Berichts doch zu einiger Verunsicherung, wenn die Bestimmung von Art. 24 Abs. 2 lit. e Ziff. 1 VE DSG (Rechtfertigungsgrund der Forschung, Planung und Statistik) inskünftig verschärft ausgelegt und deshalb nur noch erschwert angerufen werden kann, dies insbes. auch im Kontext der Datenaufbewahrung (Art. 4 Abs. 4 VE DSG). Diese Aussage gilt es vor dem Hintergrund der lex specialis Regel klar zu relativieren und festzuhalten, dass von dieser einschränkenden Auffassung abweichende, bereichsspezifische Datenschutzbestimmungen auf Gesetzes- wie Verordnungsstufe auch inskünftig dem DSG klar vorgehen werden. Für den Bereich der Humanforschung bedeutet dies konkret, dass auch weiterhin nicht nur die spezifischen Datenschutzbestimmungen des Humanforschungsgesetzes (HFG) sondern auch all dessen Verordnungen (wie z.B. die Humanforschungsverordnung [HVF] und die Verordnung über klinische Versuche [KlinV]) weiterhin uneingeschränkte Gültigkeit haben und auch gegenüber dem revidierten DSG stets vorgehen müssen. Eine entsprechende **explizite Klarstellung muss u.E. mindestens Eingang in die Botschaft an das Parlament** finden, ansonsten in dieser eminent wichtigen Frage eine zu grosse Rechtsunsicherheit geschaffen wird. Wird dieser Weg aus staatsrechtlichen Überlegungen als ungenügend erachtet, so muss eine Lösung gefunden werden, der den umfassenden Vorrang bereichsspezifischer Datenschutzbestimmungen ausnahmslos sicherstellt.

Werden also Daten in Übereinstimmung mit den gesamten spezifischen Vorgaben bearbeitet, so können keine Datenschutzverletzungen resultieren. Gerade am Beispiel des Humanforschungsrechts zeigt sich die sachliche Rechtfertigung zu einem solchen Ansatz, wurden dessen datenschutzspezifischen Bestimmungen insgesamt nach internationalen Grundsätzen ausgestaltet und dabei auf die berechtigten Interessen sowie das Schutzbedürfnis der Patienten gebührend Rücksicht genommen. Der Humanforschungsplatz Schweiz ist darauf angewiesen, dass diese Bestimmungen, die durchaus von gewissen Vorgaben des DSG abweichen, weiterhin uneingeschränkte Geltung haben, ansonsten die Schweiz Gefahr läuft, inskünftig noch weniger Humanforschung betreiben zu können, als sie dies heute aufgrund der administrativen Hürden und der vergleichsweise hohen Kosten schon tut. Selbstverständlich **gelten diese Ausführungen stellvertretend auch für alle anderen bereichsspezifischen Datenschutzbestimmungen**, die in anderen Gesetzen und den dazugehörigen Verordnungen geregelt sind.

Geltungsbereich und Begrifflichkeiten

Während scienceindustries die Streichung des Schutzes **juristischer Personen** begrüsst, so ortet sie einigen Anpassungsbedarf beim Geltungsbereich und den Begrifflichkeiten. Es fällt auf, dass einige Formulierungen im VE DSG nicht konsequent verwendet werden, was es mit Blick auf eine konsistente Rechtsanwendung zu verbessern gilt. Sodann soll nach unserem Verständnis des VE DSG das Datenschutzgesetz inskünftig auch im Rahmen **bereits hängiger Zivilprozesse und laufender Strafverfahren** uneingeschränkt zur Anwendung kommen, was faktisch zu einer Ausweitung des Auskunftsrechts führt. Davon ist abzusehen, denn eine solche Ausweitung des Geltungsbereichs des DSG birgt ein grosses Missbrauchspotential, weil sich damit die zivilprozessualen Editionsregeln umgehen liessen. Auch möchten wir zu einer konsequenteren Verwendung des Begriffes „**Personendaten**" anstelle des Miteinbezugs des Ausdrucks „Daten" anregen, da dies u.E. die Definitionen einzelner Konzepte unnötig ausweitet. Ebenso sind die Pflichten zwischen dem Verantwortlichen und dem Auftragsdatenbearbeiter unklar verteilt resp. ist nicht ersichtlich, nach welcher Logik diese vergeben wurden, was es auch zu verbessern gilt. Desweitern ist für uns nicht nachvollziehbar, warum inskünftig auf die Definition des Begriffs des „**Gesetzes im formellen Sinn**" verzichtet werden soll, wenn dieser im Gesetz weiterhin Verwendung findet; u.E. sollte an der bisherigen Definition festgehalten werden.

Anzupassen sind sodann Art. 3 lit. c Ziff. 3 und 4 VE DSG, welche die **genetischen** sowie die **biometrischen Daten** als besonders schützenswerte Daten festschreiben. Beide Definitionen sind zu präzisieren, indem es heissen muss: *genetische resp. biometrische Daten, die den Zweck haben, eine natürliche Person eindeutig zu identifizieren*. Die im Vorentwurf verwendete Begrifflichkeit ist zu weit gefasst und bedarf zwingend der Präzisierung, ansonsten jegliche genetischen und biometrischen Daten als besonders schützenswert gelten, dies verbunden mit den entsprechenden Erschwernissen im Umgang mit diesen Daten. Sowohl bei genetischen wie auch den biometrischen Daten muss berücksichtigt werden, dass etliche Personendaten nicht mit der Absicht zur eindeutigen Identifikation einer Person erhoben werden und dann in Ermangelung des Bearbeitungszwecks nicht unter den Anwendungsbereich des DSG fallen sollen. Zudem ist zu beachten, dass es keine allgemein zugänglichen Datenbanken über Geninformationen gibt, mittels welcher Personen allein aufgrund einer DNA-Sequenz identifiziert werden könnten. Vielmehr sind solche Datenbanken besonders geschützt, wobei für jene mit Klartext-Identifikationselementen sehr grosse Sicherheitsmassstäbe gelten, was gut und richtig ist. Umgekehrt bedeutet dies aber auch, dass in der Realität im Regelfall eine Person nicht alleine durch eine DNA-Sequenz identifiziert ist.

Ebenso ist der Begriff oder anders ausgedrückt das Konzept des **Profilings**, wie er/es in Art. 3 lit. f VE DSG vorgeschlagen wird, zu verwerfen, da auch diese Definition viel zu weit gefasst ist und im Unterschied zur Datenschutzgrundverordnung der EU (DSGVO) auch manuelle Auswertungen miterfasst sind, wie bspw. eine Mitarbeiterbewertung. Bereits der Begriff des Persönlichkeitsprofils, wie er im aktuell gültigen DSG definiert ist, hat sich in der Praxis nicht bewährt und die Gelegenheit der Totalrevision sollte dahingehend genutzt werden, Abstand von diesem Konzept zu nehmen. Der Datenschutz bezieht sich auf Daten resp. alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Damit ist das Schutzobjekt des DSG umfassend bestimmt und zudem wird präzisiert, welche dieser Angaben als besonders schützenswert gelten. Es macht deshalb keinen Sinn, eine zusätzliche Schutzkategorie hinzuzufügen, die letztlich auf einen Arbeitsprozess - die Auswertung von Daten - abzielt. Denn sollten so gewonnene Arbeitsergebnisse für sich genommen den Begriff der Personendaten wieder erfüllen, so fallen sie ohnehin unter den Anwendungsbereich des DSG. Die Auswertung als Vorgang kann indes u.E. per se materiell den Datenbegriff gar nicht erfüllen. Auch ist der im VE DSG gewählte Ansatz aus Sicht des Schutzgedankens

nicht angezeigt, denn das Profiling wird für das Datensubjekt erst dann relevant, wenn ein Profil verwendet wird und nicht bereits mit dessen Erstellung. Dies gilt es unbedingt im Auge zu behalten.

Insofern würde scienceindustries es begrüssen, wenn sich das DSG in dieser Hinsicht stärker am Ansatz der DSGVO orientiert. In Anlehnung an diese sollte das Profiling nicht mehr als eine zusätzliche Schutzkategorie umschrieben werden. Vielmehr sollte sich dessen Begriffsumschreibung darin erschöpfen, dass unter diesem ein **Verarbeitungsvorgang**, bei welchem es **mittels technischer Hilfsmittel** zu einer **automatisierten, systematischen Verarbeitung von Personendaten** kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen hervorzusagen. Gleichzeitig wäre dann im Gesetz festzuschreiben, welches die spezifischen Pflichten der Verantwortlichen im Zusammenhang mit dem so definierten Profiling sind, wobei keinesfalls über das Schutzniveau der DSGVO hinausgegangen werden darf. Zu denken wäre an wenige Informations- und Auskunftspflichten sowie allenfalls ein Widerspruchsrecht beim Profiling zu Zwecken der Direktwerbung. Klar **Abstand zu nehmen** ist indes vom Konzept, dass **Profiling per se bereits als Persönlichkeitsverletzung** gilt und damit im Ergebnis für jedes Profiling eine ausdrückliche Einwilligung der betroffenen Person vorliegen muss (Art. 23 Abs. 2 lit. d VE DSG). Wenn ein Profiling erfolgt und im Ergebnis Personendaten daraus resultieren, dann stehen diese wiederum unter dem Schutz des DSG, weshalb sich eine zusätzliche Erwähnung des Profilings ohne ausdrückliche Einwilligung als Persönlichkeitsverletzung u.E. als unnötig erweist. Angesichts des damit verbundenen erheblichen Aufwands und der entstehenden Rechtsunsicherheiten auf Seiten der Unternehmen ist dieser Vorschlag abzulehnen.

Wollte man nicht Abstand vom vorgeschlagenen Konzept nehmen, dann wäre immerhin die Definition des Profilings auf mittels technischer Hilfsmittel automatisierte, systematische Entscheidungen zur Analyse und Bewertung von auf eine bestimmte Person bezogene persönliche Merkmale zu reduzieren und zur Verneinung einer Persönlichkeitsverletzung müsste die konkludente Einwilligung genügen.

Grundsätze

Der VE-DSG verschärft den Grundsatz der Erkennbarkeit des Zwecks unnötigerweise mit dem Zusatz der **«klaren» Erkennbarkeit**. Diese Anpassung an die Terminologie des DSGVO ist verfehlt, da die Schweizer Regelung einem unterschiedlichen Grundkonzept folgt (Erkennbarkeit im Rahmen einer klaren Zweckbindung). Die Verschärfung ist auslegungsbedürftig und produziert unnötige Rechtsunsicherheit, weshalb der Zusatz zu streichen ist.

Bezugnehmend auf Art. 4 Abs. 6 VE DSG, wonach eine gültige **Einwilligung eindeutig** zu erfolgen hat, nehmen wir zur Kenntnis, dass mit der Neuformulierung wohl eine terminologische Annäherung an das Übereinkommen SEV 108 und die DSGVO beabsichtigt wurde. Unserer Ansicht nach ist jedoch die Abgrenzung zur im zweiten Satz erwähnten ausdrücklichen Einwilligung im Rahmen des Profilings nicht ersichtlich und wirft lediglich Fragen der Unterscheidung dieser beiden Begriffe auf. Der Zusatz „eindeutig" sollte daher ersatzlos gestrichen werden.

Auch wenn die **Nachführungspflicht** bereits heute im DSG vorgesehen ist, so ist dennoch festzuhalten, dass diese weit geht und bei den Firmen zu hohen Aufwendungen führt. Es wird zu beachten sein, hier auf Verordnungsstufe die Vorgaben minimal zu halten.

Datentransfer ins Ausland

scienceindustries begrüsst grundsätzlich die gegenüber dem aktuellen Gesetz beibehaltene Regelung zur Datenübertragung ins Ausland, **kritisiert indes die erweiterten Notifikations- und Genehmigungspflichten.** Zustimmend zur Kenntnis nehmen wir die vorgesehene Regelung, Daten ohne Vorliegen eines Angemessenheitsbeschlusses auf Basis von Standardklauseln exportieren zu können, stellen hierzu jedoch die Informationspflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragen (EDÖB) aufgrund des aus unserer Sicht ungünstigen Verhältnisses von Aufwand und Nutzen in Frage. Vielmehr regen wir eine Abkehr im Sinne eines weitgehenden Verzichts auf diese Pflicht – ganz im Sinne der DSGVO (Art. 46) – an.

Der Vorentwurf sieht zudem vor, dass „**verbindliche unternehmensinterne Datenschutzvorschriften**" (sog. Binding Corporate Rules - BCR) neu einer Genehmigung durch den EDÖB unterstellt sind, was uns inkonsequent erscheint, da BCRs in der Regel dann zum Tragen kommen, wenn nicht mit Standardklauseln operiert werden soll und daher als Subgruppe von spezifischen Garantien nach Art. 5 Abs. 3 lit. b VE DSG aufgefasst werden können, diese jedoch lediglich einer Informationspflicht gegenüber dem EDÖB unterstehen. Desweitern stufen wir die genannte Frist zur Genehmigung von BCRs als nicht praktikabel ein, indem aufgrund der möglichen mehrmonatigen Unklarheit die Unternehmen in ihrer Entscheidungsfreiheit, nichtstandardisierte Datenexportverträge einzugehen, eingeschränkt wären. Die Frist ist deshalb auf das heutige Mass von maximal 30 Tagen zu kürzen und von einer unbeschränkt möglichen Verlängerung abzusehen. Wünschenswert wäre aus Sicht der Rechtssicherheit zudem, dass einmal bewilligte Garantien oder BCRs bis auf weiteres Gültigkeitsstaus erhalten und nicht ohne triftige Gründe widerrufen werden können sowie eine **Beibehaltung des heutigen Art. 6 Abs. 2 lit. g DSG** (Bekanntgabe von Personendaten innerhalb derselben Unternehmung), da diese Regelung zu einer erheblichen Erleichterung des Datenaustauschs innerhalb eines Unternehmens führt.

Hervorheben und kritisch würdigen möchten wir die neue Bestimmung in Art. 6 Abs. 2 VE DSG, wonach **Datenexporte auch in jenen Fällen dem EDÖB gemeldet** werden müssen, die durch Vertragsabschluss, Vertragserfüllung oder ein ausländisches Rechtsverfahren statthaft sind. Eine solche erweiterte Notifikationspflicht würde einerseits zu einer Überflutung an Meldungen an den EDÖB führen, welche dieser kaum innerhalb nützlicher Frist bearbeiten könnte. Andererseits gilt es den damit unerwünscht herbeigeführten Effekt zu beachten, dass Unternehmen gezwungenermassen gegenüber dem EDÖB Geschäftsgeheimnisse offenzulegen hätten, was unserer Ansicht nach zu weit geht. Dies hätte zur Konsequenz, dass etwa Unterlagen aus ausländischen Gerichtsverfahren oder Untersuchungen über das Öffentlichkeitsgesetz publik gemacht werden müssten, was jedoch vielmehr der Unternehmenstätigkeit schaden als den Datenschutz verstärken würde. Aus diesen Überlegungen sprechen wir uns für eine ersatzlose Streichung der genannten Bestimmung aus.

Informations-, Auskunfts- und weitere Pflichten

Informationspflicht

Auch wenn die Informations- und Auskunftspflichten zum Kern des VE DSG gehören und aus Sicht des Datensubjekts von grosser Wichtigkeit sind, so führen sie in der nun vorgeschlagenen Form zu einer verwirrenden Überinformation der betroffenen Personen, die der gewünschten Transparenz letztlich gar zuwiderläuft. Die erweiterten Informationspflichten auf alle Personendaten bringen Mehraufwand und führen auf Grund des öffentlich-rechtlichen Charakters der Bestimmungen sowie den daraus fliessenden Sanktionsfolgen zu Problemen in der Praxis. Entsprechend muss die Regel grundsätzlich im Sinne einer **risikobasierten Transparenzpflicht** überarbeitet werden. In grundsätzlicher Hinsicht wäre u.E. eine einfache, transparente Information der betroffenen Personen allenfalls mit einer freiwillig vorzusehenden Kontaktmöglichkeit zur Ausübung ihrer Rechte nicht nur für die Unternehmen einfacher zu handhaben, sondern auch für die betroffenen Personen transparenter und würde zu deren besseren Schutz führen.

Dem VE DSG ist zum einen nicht zu entnehmen, wie die betroffene Person zu informieren sein wird. Individualisierte Informationspflichten würden mit beachtlichen Mehraufwänden einhergehen und stellten für die Unternehmen einen wesentlichen kostentreibenden Faktor dar. Daher regen wir die Einführung von **„standardisierten" Informationspflichten** an. Dies könnte beispielsweise durch einmalige datenschutzrechtliche Erläuterungen in den Allgemeinen Geschäftsbedingungen (AGB), einer Erklärung auf der Webseite („Privacy Note") oder auch durch das Anbringen von Piktogrammen, die etwa auf eine bestimmte datenschutzrelevante Verarbeitung von Daten hinweisen, erfolgen. Solche standardisierten Informationspflichten sollten durch die Verantwortlichen autonom oder allenfalls im Rahmen der guten Praxis entwickelt werden können.

Zum andern ist für uns nicht ersichtlich, über welche Einzelheiten dann im Detail informiert werden soll. Obwohl in Art. 13 Abs. 2-4 VE DSG einige konkrete Angaben enthalten sind, muss die Information letztlich dennoch alle Aspekte umfassen, die für eine betroffene Person notwendig sind, um ihre Rechte nach DSG geltend zu machen. Der erläuternde Bericht hält auf Seite 57 diesbezüglich fest, dass durch die Beschränkung auf Mindestangaben eine flexible Handhabung der Informationspflicht ermöglicht werden soll, um dadurch ein Übermass an Informationen zu verhindern. Wenngleich sich dies vernünftig liest, so führt u.E. jedoch die strafrechtliche Sanktionierung der Informationspflicht vielmehr dazu, dass Verantwortliche und Auftragsbearbeiter infolge einer Risikominimierung und der Absicherung ihrer eigenen Beurteilung sich gezwungen sehen, deutlich mehr Informationen zu liefern, als an sich gesetzlich vorgesehen wäre. Will man den durchaus begrüssenswerten flexiblen Ansatz beibehalten, so wäre die **Sanktionierung dieser Pflicht zu überdenken und nötigenfalls nur geringfügig auszugestalten**.

Hinsichtlich der Begrifflichkeiten in Art. 13 Abs. 3 VE DSG fällt sodann auf, dass die Ausdrücke **„Dritter"** und **„Empfängerinnen** und **Empfänger"** nicht definiert werden sowie keine Klarheit zur **Abgrenzung der Pflichten** des Verantwortlichen und des Auftragsdatenbearbeiters besteht. U.E. sollte dieser lediglich für Verwirrung stiftende Absatz ersatzlos gestrichen werden. Überdies geht die vorgesehene **Informationspflicht bei der indirekten Datenbeschaffung** zu weit und verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Dem Verantwortlichen werden die relevanten Eckwerte, insbesondere die erstmalige Speicherung, oftmals gar nicht bekannt sein; das Aufwand-Ertragsverhältnis ist damit unverhältnismässig. Darüber hinaus

sind solche direkten Informationspflichten nicht erforderlich: eine allgemeine vorgängige Information des Kunden reicht aus. Die Bestimmung ist deshalb ebenso zu streichen.

Mit Blick auf die entsprechenden Regelungen der EU stellen wir weiter fest, dass insbesondere Art. 13 Abs. 4 VE DSG, wonach der Verantwortliche die **Identität sowie Kontaktdaten der Auftragsbearbeiter und darüber hinaus „die Daten oder Kategorien von Daten"** mitzuteilen hat, weiter als die entsprechenden Bestimmungen in Art. 13 und 14 DSGVO geht. Wir können aus dieser Bestimmung keinen Mehrwert für die betroffenen Personen erkennen, zumal mit diesen zusätzlichen Informationen nicht der Transparenz gedient wird, sondern vielmehr eine dieser zuwider laufende Informationsüberflutung auslösen würde. scienceindustries spricht sich deshalb für eine Streichung von Art. 13 Abs. 4 VE DSG aus.

Die in Art. 14 VE DSG vorgesehenen Ausnahmeregelungen entsprechen weitgehend jenen des heutigen Gesetzestextes, wirken sich u.E. im Ergebnis jedoch enger aus, als dies mit der revidierten Konvention 108 beabsichtigt wurde. Kritisch stehen wir insbesondere Art. 14 Abs. 4 lit. a VE DSG gegenüber, wonach die Berufung auf ein **überwiegendes privates Interesse** nur dann möglich ist, wenn Personendaten nicht an Dritte weitergegeben werden. Unserer Ansicht nach wäre hierbei lediglich zu prüfen, ob das Interesse des Datenbearbeiters dem Interesse an der Information der betroffenen Person vorgeht. Ansonsten führte dies zu einer Ungleichbehandlung von Konzerngesellschaften im Vergleich zu einzelnen, unabhängigen Unternehmen, da sich erstere bei konzerninterner Weitergabe von Daten zum Zweck der Auftragsbearbeitung nicht auf diese Bestimmung berufen könnten. Aus diesem Grund regen wir an, den Zusatz *„...und er die Personendaten Dritten nicht bekannt gibt."* ersatzlos zu streichen.

Die Reichweite der neu eingeführten Informations- und Anhörungspflicht bei **automatisierten Einzelfallentscheiden** ist ebenso zu weitgehend und so nicht akzeptabel. Zwar kennen sowohl die Konvention 108 als auch die DSGVO eine entsprechende Regelung. Der Anwendungsbereich von Art. 15 VE DSG ist jedoch viel breiter: der Entwurf unterscheidet stärker zwischen Profiling sowie automatisieren Einfallentscheiden und sieht auch keine Ausnahmen vor. Dies hat Folgen, welche so wohl nicht beabsichtigt waren: So wären beispielsweise Spam- und Virenscanner, Zugangskontrollen via Badge und sehr viele andere Routineentscheide erfasst, die aus Gründen der Effizienz dem Computer übertragen werden.

So bringt v.a. das vorgesehene **Äusserungsrecht** keinen Mehrwert. Es ist angesichts der neu vorgesehen Informationspflicht auch schlicht unnötig und für die Unternehmen wettbewerbs- und innovationsbehindernd. In der Praxis würde es wohl regelmässig zu einer Begründungspflicht führen und damit die Vertragsfreiheit der Unternehmen über Gebühr einschränken. Eine solche Regelung wäre entsprechend auf schwere Fälle - also solche, die erhebliche Auswirkungen auf die betroffene Person haben - zu begrenzen und der Wortlaut an die entsprechende Bestimmung in der DSGVO anzupassen. Auch dann wären sinnvolle Ausnahmen notwendig, welche zumindest auf dem Verordnungsweg vorzusehen wären. Eine einmalige angemessene Information ohne ausdrückliche Einwilligung erschiene uns dabei als ausreichend.

Im Kontext der Informationspflicht spricht sich scienceindustries zudem für eine Prüfung des Konzepts des **„unabhängigen betriebsinternen Datenschutzbeauftragten"** (Data Protection Officer - DPO) aus, da die Ernennung eines mit umfassenden Kompetenzen und Verantwortungen ausgestatteten DPOs hierbei zu einer begrüssenswerten Entlastung des EDÖB wie auch der Unternehmen führen dürfte (vgl. dazu Ausführungen unter dem entsprechenden Absatz auf Seite 12).

Auskunftsrecht

scienceindustries nimmt die vorgesehene Ausweitung des Auskunftsrechts gemäss Art. 20 VE DSG zur Kenntnis, erachtet jedoch den in Abs. 2 eingefügten Zusatz, wonach eine **transparente Datenbearbeitung gewährleistet** sein soll, als unzweckmässig und in einem gewissen Sinne verfänglich. In extensiver Auslegung kann dieser Zusatz dahingehend verstanden werden, dass sich das Auskunftsrecht nicht auf die Daten an sich zu beschränken hat, sondern damit zusätzlich auch die Datenbearbeitungsprozesse impliziert werden. Dies könnte zur Folge haben, dass der Verantwortliche diese auch offenlegen muss, was jedoch nicht den Absichten der Auskunftspflicht entsprechen würde und darüber hinaus möglicherweise bereits an der technischen Umsetzung scheitern könnte. Aus diesen Gründen regen wir an, auf diesen Zusatz zu verzichten.

Desweitern geht der Vorentwurf auch hier hinsichtlich der **automatisierten Einzelentscheide** einiges weiter als die DSGVO, indem in Abs. 3 ein Verantwortlicher verpflichtet wird, bei jedem Entscheid, den er trifft und welchem die Bearbeitung von Personendaten zugrunde liegt, einer betroffenen Person Rechenschaft darüber abzulegen, wie und warum er zu seinem Entscheid gelangt ist und welche Konsequenzen dies für die betroffene Person zusätzlich zu den Daten hat, die hierzu verwendet wurden. Eine derart umfassend verstandene Auskunftspflicht greift in erheblichem Ausmass in die Freiheiten der Unternehmen ein und führt bei diesen zu einem unverhältnismässigen Aufwand, ohne dass daraus ein erkennbarer Nutzen für die betroffenen Personen ersichtlich ist. Die Auskunftspflicht wäre vielmehr auf das Vorliegen einer (automatisierten) Entscheidung zu beschränken, gleichzeitig kann allenfalls noch über deren Ergebnis informiert werden, **indes nicht über deren Wirkungen**, da diese gar nicht immer erkenn- oder gar abschätzbar sind. So sind übrigens vermehrt auch (automatisierte) Einzelentscheidungen denkbar, die gar nicht primär auf eine besondere (Rechts-)Wirkung ausgerichtet sind, sondern der Untersuchung von allgemeinen Verhaltensweisen dienen, womit verbunden kein Schutzbedürfnis erkennbar ist und damit auch keine Auskunftspflichten angezeigt sind. In diesem Kontext sei angefügt, dass uns Art. 20 Abs. 2 lit. e VE DSG nur dann akzeptabel erscheint, wenn ausschliesslich **Auskunft über das blosse Vorliegen einer automatisierten Einzelentscheidung** erteilt werden muss. Wird jedoch beabsichtigt, zusätzlich die Logik der automatischen Verarbeitung miteinzubeziehen, hätte dies die Offenlegung und Umschreibung einer umfassenden Anzahl an hinterlegten Algorithmen in allgemeinverständliche Erklärungen zur Folge, was bei den Unternehmen ebenso einen unverhältnismässigen Aufwand verursachen würde und daher abzulehnen ist.

Schliesslich nehmen wir zustimmend zur Kenntnis, dass die bisherige Regelung, wonach die Auskunft in Form eines Ausdrucks oder einer Fotokopie zu erteilen ist, gestrichen wurde, indes aber kostenlos sein muss. Hierzu regen wir an, spätestens auf dem Verordnungsweg **Ausnahmen von der Kostenlosigkeit** vorzusehen, wie dies in Art. 12 Abs. 5 lit. a DSGVO vorgesehen ist. Ansonsten würde das Prinzip der Kostenlosigkeit dazu führen, dass die Auskunft selbst bei wiederholten, ungerechtfertigten und extrem aufwändigen Anfragen gratis sein muss, was uns nicht hinnehmbar erscheint.

Meldung von Datenschutzverstössen

Mit Art. 17 Abs. 1 VE DSG ist neu vorgesehen, dass jeder Datenschutzverstoss dem EDÖB „unverzüglich" gemeldet werden muss, es sei denn, dieser führe „voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person". scienceindustries stellt sich auf den Standpunkt, dass keine plausiblen Gründe ersichtlich sind, weshalb die Schweizer Regelung über den entsprechenden Art. 33

DSGVO hinausgehen soll. Die DSGVO sieht eine Meldung für den Fall vor, wenn im Rahmen einer Datenbearbeitung festgestellt wird, dass eine **getroffene Sicherheitsmassnahme verletzt** wurde und diese **Verletzung zu einem Verlust der Kontrolle an den Daten** führt (vgl. Art. 33 DSGVO i.V.m. Ziff. 87 und 88 der Präambel). In der Schweiz soll die Meldepflicht hingegen jede Datenbearbeitung erfassen, die gegen das DSG verstösst: bspw. eine zweckentfremdete oder unverhältnismässige Nutzung von Daten oder eine Datenbeschaffung, die in nicht transparenter Weise erfolgt. Die Ausnahme, wann keine Meldung zu erfolgen hat, ist dabei wiederum derart formuliert, dass sie im Falle einer Datenschutzverletzung nicht gegeben sein kann, da gemäss Gesetzestext eine unbefugte Datenbearbeitung stets eine Persönlichkeitsverletzung darstellt. Aufgrund des Dargelegten und den Ausführungen zur Inkonsistenz der Bestimmung mit dem restlichen VE DSG ist dieser Artikel u.E. auf das umschriebene Niveau der DSGVO zu reduzieren. Wir regen auch in diesem Kontext an, das Konzept des unabhängigen betrieblichen Datenschutzbeauftragten zu prüfen. Soweit ein solcher in einem Unternehmen eingesetzt ist und in dieser Funktion festgestellte Datenschutzverstösse dokumentiert, könnten u.E. die Auswirkungen von Art. 17 VE DSG gemildert und damit auch die Belastung des EDÖB reduziert werden.

Weitere Pflichten

scienceindustries erachtet die in Art. 19 lit. a VE DSG erwähnte Dokumentationspflicht als umfassend und zeigt sich besorgt über die Ausführungen auf Seite 65 im erläuternden Bericht, wonach die Datenbearbeiter verpflichtet sind, ebenfalls **Datenschutzverstösse** im Sinne von Art. 17 VE DSG zu dokumentieren. Angesichts des breiten Begriffsverständnisses von Art. 17 VE DSG erscheint uns diese Dokumentation unermesslich und ohne sichtbaren Mehrwert für den Datenschutz. Wir regen deshalb an, die **Dokumentationspflicht im Grundsatz auf das Führen eines Verzeichnisses aller Datenbearbeitungen zu beschränken**, für die der Verantwortliche zuständig ist. Selbstverständlich können Unternehmen freiwillig weiter gehen. Ebenso ist die Einführung einer Ausnahme für Kleinstunternehmen sowie der kleinen und mittleren Unternehmen im Sinne einer Entlastung zu prüfen. Die DSGVO sieht hierzu beispielsweise abweichende Regelungen vor für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen.

Weitaus kritischer beurteilt scienceindustries Art. 19 lit. b VE DSG, wonach im Falle einer Berichtigung, Löschung oder Vernichtung von Daten sowie bei Verletzungen des Datenschutzes der Verantwortliche und Auftragsbearbeiter Dritten, denen sie zuvor die betroffenen Daten zugänglich gemacht haben, diese Berichtigungen etc. mitteilen müssen, soweit dies nicht oder nur mit „unverhältnismässigem" Aufwand möglich ist. Wiederum ist für uns der Mehrwert dieser Ausweitung des entsprechenden Art. 19 DSGVO nicht ersichtlich. Notwendig wäre unserer Ansicht nach die Einführung einer **Begrenzung auf jene Fälle, in denen die betroffene Person ein schützenswertes Interesse** hat, zumal die vorgesehene Bestimmung nicht vorsieht, dass die Berichtigung, Löschung oder Vernichtung auf einen Vorstoss der betroffenen Person zurückzuführen ist. Aufgrund der mannigfaltigen Gründe einer Berichtigung, Löschung oder Vernichtung von Daten, ohne dass sich dabei eine Nachinformation bisheriger Empfänger der Daten aufdrängt, kann dies zu bizarren Situationen führen. Es ist durchaus denkbar, dass eine Löschung erfolgt, weil der Inhaber die Daten nicht mehr braucht, nicht aber, weil die Daten datenschutzwidrig bearbeitet wurden oder die betroffene Person dies verlangt hat. In solchen Fällen sollte keine Pflicht nach Art. 19 lit. b VE DSG ausgelöst werden, müsste doch sonst jedes Unternehmen, das seine Archive und dergleichen bereinigt, laufend prüfen, wem es die Daten schon einmal mitgeteilt hat und diese Empfänger darüber informieren. Es erscheint uns daher nicht opportun, dass die Nachinformation lediglich wegen dem damit allenfalls verbundenen unverhältnismässigen Aufwand wegfällt. Art. 19 lit. b VE DSG ist dahingehend weiter einzuschränken, indem die Be-

stimmung nur zum Tragen kommt, wenn eine Person die **Nachinformation gestützt auf ein überwiegendes privates Interesse ausdrücklich verlangt**.

Sodann erschliesst sich uns auch in diesem Kontext der **Begriff der „Empfängerinnen und Empfänger"** nicht. Hier ist eine klärende Umschreibung zu fordern, wobei wir den Begriff so verstehen, dass der Auftragsbearbeiter nicht tangiert wird.

Datenschutz-Folgenabschätzung

scienceindustries stuft das im Vorentwurf vorgeschlagene Konzept der Datenschutz-Folgenabschätzung in verschiedener Hinsicht als problematisch ein. So erscheinen uns die Voraussetzungen für die Durchführung einer Abklärung gemäss Art. 16 Abs. 1 VE DSG äusserst tief. Ein „erhöhtes" Risiko dürfte sich in der Praxis rasch abzeichnen, wodurch für beinahe alle Datenbearbeitungen vorab entsprechende Abklärungen durchgeführt werden müssen. Seite 61 des erläuternden Berichts entnehmen wir zudem, dass die Bearbeitung von besonders schützenswerten Personendaten oder ein Profiling bereits ein Indiz für ein erhöhtes Risiko darstellen sollen, wie auch die Übermittlung in Drittstaaten ohne angemessenen Datenschutz. Es ist davon auszugehen, dass aufgrund der Strafandrohungen selbst in Fällen, in denen grundsätzlich kein erhöhtes Risiko besteht, ein entsprechendes Verfahren durchgeführt und eine Meldung an den EDÖB erfolgen wird. Der absehbare Aufwand – sei es für die Unternehmen oder den EDÖB – fiele enorm aus, ohne dass der Datenschutz dadurch gestärkt würde. Deshalb befürworten wir den Ansatz, dass die gesetzliche Pflicht zur Erstellung einer formalen, dokumentierten Abklärung auf das beschränkt wird, was die Interessenswahrung der schutzbezogenen Personen als wirklich nötig erkennen lässt. Daher schlagen wir vor, diesbezüglich an Art. 36 DSGVO anzulehnen, der **entsprechende Abklärungen erst bei Vorliegen eines „hohen" Risikos für eine Persönlichkeitsverletzung vorsieht**.

Sodann ist der Begriff der „Voraussehbarkeit" u.E. in der Schweizer Rechtspraxis nicht etabliert. Es bietet sich vielmehr an, den **Begriff der „überwiegenden Wahrscheinlichkeit"** zu verwenden, welcher im Sozialversicherungsrecht gebräuchlich ist und dort eine langjährige Konkretisierung erfahren hat. Gemäss diesem Beweisgrad genügt bundesgerichtlicher Rechtsprechung nach die blosse Möglichkeit eines bestimmten Sachverhaltes nicht; vielmehr ist im konkreten Fall jener Sachverhaltsdarstellung zu folgen, die von allen möglichen Geschehensabläufen als die wahrscheinlichste zu würdigen ist (vgl. BGE 126 V 360). Mit Blick auf die mit einer Datenschutz-Folgenabschätzung zu erwartenden erheblichen Aufwände besteht ein Interesse an einer rechtssicheren Formulierung, die möglichst Klarheit schafft ohne den Schutzgedanken zu unterwandern. Was hierbei für das Sozialversicherungsrecht genügt, darf auch für den Datenschutz als angemessen erachtet werden.

Desweitern bewerten wir die **Meldepflicht gegenüber dem EDÖB und die ihm eingeräumte Frist zur Bearbeitung praxisfern** und sind der Meinung, dass die Datenbearbeiter dadurch in ihrer Arbeit massiv behindert würden. Einige der Unternehmen aus unserer Industrie führen jährlich weit über hundert Datenschutz-Folgenabschätzungen durch, wobei eine konsequente Prüfung durch den EDÖB wohl zur Folge haben würde, dass für jedes dieser Unternehmen nur für diese Prüfungen eine eigene Person abgestellt werden müsste, was weder sinnvoll erscheint, noch möglich ist. Auch die DSGVO geht in Art. 35 weniger weit: sie verlangt eine Konsultation der Aufsichtsbehörde nur dann, wenn der Verantwortliche zum Schluss kommt, dass trotz der von ihm **ergriffenen Schutzmassnahmen ein hohes Risiko der Verletzung der Persönlichkeit**

der betroffenen Personen verbleibt. Zudem erscheint uns die dem EDÖB gewährte Frist zur Beurteilung viel zu lange: in der EU (Art. 36 Abs. 2 DSGVO) muss eine Behörde innert acht Wochen handeln, falls sie sich gegen eine Bearbeitung ausspricht; die Frist kann überdies nur in komplexen Fällen um sechs Wochen verlängert werden. In der Schweiz soll der EDÖB standardmässig drei Monate Zeit haben, mit der Möglichkeit, durch das Einfordern weiterer Information die Frist jedes Mal von neuem beginnen zu lassen. Zudem sollte klar geregelt werden, welche Informationen dem EDÖB weitergeleitet werden müssen und wie diese insbesondere bei Informationszugangsgesuchen nach dem Öffentlichkeitsgesetz (BGÖ) geschützt werden können. Datenschutz-Folgenabschätzungen von Unternehmen werden aber oftmals Geschäftsgeheimnisse enthalten, weshalb eine Einsichtnahme durch Mitbewerber vermieden werden muss.

Zusammenfassend regt scienceindustries aufgrund obiger Ausführungen an, einerseits die Begriffe des erhöhten Risikos sowie der Voraussehbarkeit im vorgeschlagenen Sinn anzupassen und den zeitlichen Rahmen zur Beurteilung der Massnahmen enger zu setzen. Desweitern soll auch die Datenschutz-Folgenabschätzung mit dem Konzept des „unabhängigen internen Datenschutzbeauftragten" verknüpft werden (vgl. dazu Ausführungen unter dem nachfolgenden Absatz).

Konzept des unabhängigen internen Datenschutzbeauftragten

scienceindustries bedauert es, dass im VE DSG das Konzept des unabhängigen internen Datenschutzbeauftragten (Data Protection Officer - DPO) keinerlei Niederschlag gefunden hat. Wir erkennen darin nicht zuletzt im Vergleich mit der DSGVO einen Mangel, den es zu beheben gilt. Denn das Konzept des DPO scheint den Bedürfnissen der Wirtschaft zu entsprechen, wie ein Blick in die entsprechende Liste des EDÖB deutlich aufzeigt. So ist im revidierten Gesetz in Analogie zur bisherigen Regelung von Art. 11a DSG am **„Institut" des DPO festzuhalten**, wobei die Unternehmen auch weiterhin **frei in der Entscheidung sein** sollen, einen solchen einzusetzen oder nicht. Die Voraussetzungen an die Stellung sowie die Aufgaben des DPO können in Anlehnung an die heute dazu bestehende Praxis zu den Art. 11a Abs. 5 lit. e DSG sowie Art. 12a und Art. 12b DSG weiterhin auf Verordnungsebene geregelt werden, wobei gleichzeitig die Äquivalenz mit den Art. 37 ff. DSGVO im Auge zu behalten wäre. Angesichts der Tatsache, dass der DPO im VE DSG gar nicht mehr vorgesehen ist, geht man seitens des Bundes offenbar von erheblichem Handlungsspielraum aus, was wir zwar ebenso einschätzen, indes vor dem Hintergrund der Äquivalenz mit den europäischen Vorgaben nicht gar soweit gehen würden, dieses Konzept überhaupt nicht mehr vorzusehen. Entscheidet sich ein Unternehmen, einen DPO einzusetzen, wäre sodann eine damit verbundene **Meldepflicht an den EDÖB** vorzusehen, der analog zur heutigen Regelung ein öffentlich einsehbares Register dieser Firmen führt. Damit ist transparent, welche Firmen von diesem Konzept Gebrauch machen, was mit Blick auf die nachfolgenden Ausführungen von Bedeutung ist.

Neben der Möglichkeit zur freiwilligen Bezeichnung eines DPO sind alsdann die im Zusammenhang mit dieser Bezeichnung verbundenen Rechtswirkungen im DSG aufzuführen. So sollten insbes. diverse **Informations- und Meldepflichten wegfallen** oder aber **mindestens gelockert** werden – soweit sie überhaupt beibehalten werden. Kommt ein DPO beispielsweise im Rahmen einer betriebsinternen Datenschutz-Folgenabschätzung zum Schluss, dass keine wesentlichen Risiken mit Blick auf den Datenschutz gegeben und entsprechend keine nennenswerten Massnahmen angezeigt sind, so können sämtliche damit zusammenhängende Meldungen an den EDÖB unterbleiben. Eine solche wäre nur dann angezeigt, wenn der DPO einerseits hohe Risiken für den Datenschutz der betroffenen Personen erkennt und anderseits deshalb

Massnahmen zur Eindämmung resp. Behebung der erkannten Risiken vorschlägt. Mit dieser Lösung wäre eine breite Abdeckung von Datenschutz-Folgenabschätzungen in den Unternehmen zu erreichen und gleichzeitig würde der EDÖB nur dann in den Prozess involviert, wenn eine Risikosituation sich manifestiert. Dies erscheint uns ein sachgerechter Ansatz, der einen effizienten Umgang mit den knappen Ressourcen auf beiden Seiten sicherstellt und gleichzeitig das Schutzniveau hoch hält. Ebenso wäre in diesem Zusammenhang eine Reduktion allfälliger Meldepflichten im Zusammenhang mit dem Datentransfer ins Ausland vorzusehen.

In diesem Kontext sei angefügt, dass scienceindustries den **Verzicht auf die Anmeldung von Datensammlungen durch private Personen begrüsst**. Ein DPO könnte auch hierbei eine wesentliche Aufgabe erfüllen, indem diese Person gestützt auf ihr Fachwissen, die Kenntnisse über das Unternehmen und seine Geschäftstätigkeiten sowie deren unabhängige Stellung am besten geeignet ist, betriebsinterne Standards für die Etablierung der notwendigen Prozesse auszuarbeiten und dabei den Datenschutz betriebsintern auf hohem Schutzniveau durchzusetzen. Verbunden mit der unsererseits geforderten Lockerung hinsichtlich der Melde- und Informationspflichten sowie ggf. weiterer Pflichten, wäre damit ein erheblicher Anreiz zur Schaffung einer solchen Stelle gegeben, was zum einen wiederum den betriebsinternen Massnahmen zur Sicherstellung des Datenschutzes und zum andern einer Entlastung des EDÖB dienen würde. Entscheidet sich hingegen ein Unternehmen, keinen DPO einzusetzen, so könnte es im Gegenzug von den damit zusammenhängenden Rechtswirkungen nicht profitieren und sähe sich schneller mit Melde- und Informationspflichten konfrontiert. Aus diesem Grund sind wir der Ansicht, dass die mit der Bezeichnung und Bekanntgabe eines DPO verbundenen Rechtswirkungen bis zu einem gewissen Grad positivrechtlich im DSG vorzusehen sind, um diesbezügliche Klarheit und im Ergebnis Rechtssicherheit zu schaffen.

An dieser Stelle wollen wir gleichzeitig festgehalten wissen, dass das unsererseits geforderte Konzept des unabhängigen internen Datenschutzbeauftragten **nicht** dazu führen soll, dass diese **Personen eine erhöhte strafrechtliche Verantwortung** trifft. Vielmehr schlagen wir dazu einen anderen Ansatz als der im Entwurf gewählte vor und verweisen aber hier auf die nachfolgenden Ausführungen zum Sanktionssystem.

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

scienceindustries spricht sich im Grundsatz positiv zum Konzept des Datenschutzes durch Technik und datenschutzfreundlichen Voreinstellungen (Art. 18 VE DSG) aus, auch wenn wir der Ansicht sind, dass sich die Bestimmungen bereits aus einer korrekten Anwendung des Bearbeitungsgrundsatzes gemäss Art. 11 VE DSG ergeben, wonach im Rahmen einer Datenbearbeitung jeweils angemessene technische und organisatorische Massnahmen zu treffen sind, um eine unbefugte Datenbearbeitung zu verhindern. Unter Berücksichtigung der entsprechenden DSGVO-Vorgaben stellen wir jedoch fest, dass die vorgeschlagene Formulierung gemäss VE DSG im Vergleich zu Art. 32 DSGVO deutlich zu restriktiv ausfällt. Insbesondere sollte berücksichtigt werden, dass die in Art. 18 Abs. 1 und 2 VE DSG vorgesehene Verpflichtung einen einklagbaren Anspruch einzelner Personen auf die Einführung solcher Massnahmen nach sich ziehen kann, was u.E. nicht die Absicht der europäischen Regelwerke war und eindeutig zu weit geht. Vielmehr sollte sich das **Schweizer Datenschutzgesetz an der entsprechenden DSGVO-Formulierung ausrichten**, in dem Sinne, dass *„Der Verantwortliche und der Auftragsbearbeiter geeignete (oder angemessene) technische und organisatorischen Massnahmen trifft/treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen".*

Dabei handelt es sich zwar um im Gesetz festgelegte Ziele, die es anzustreben gilt, indes können diese **nicht zu einklagbaren Ansprüchen einzelner Personen** führen. Diese Differenzierung ist wesentlich, um einer möglichen diesbezüglichen Klageflut entgegen zu wirken. Denn es ist zu vermeiden, dass in gewissen Kontexten realisierbare Standards auf dem Klageweg auf Branchen übertragen werden, in welchen diese keinen Sinn machen oder aus technischen Gründen noch nicht im gleichen Ausmass etabliert sind. U.E. würde sich auch eine entsprechende **Klärung in der Botschaft an das Parlament** aufdrängen.

Keine spezifischen Regelungen für verstorbene Personen

scienceindustries spricht sich aus mehreren Gründen **gegen die Einführung von spezifischen Regelungen für verstorbene Personen** aus. Vorweg möchten wir auf den in Art. 31 Abs. 1 ZGB verankerten Grundsatz hinweisen, wonach die Persönlichkeit mit dem Tod endet und eine verstorbene Person folglich auch keinen Datenschutz erlangen kann. Allenfalls kommt dieser für Personen im Umfeld der verstorbenen Person, die durch die Bearbeitung derer Daten ebenfalls betroffen sind, zum Tragen. Aus Sicht der Unternehmen sind die vorgesehenen Regelungen insofern problematisch, als sie aufgrund ihrer generell abstrakten Natur unzählige weitere, grundsätzlich mit der Bestimmung nicht beabsichtigte Anwendungsfälle miteinbeziehen und daher unvorhergesehene Nebenwirkungen entfalten können. In diesem Zusammenhang gilt es auch die Übertragung von Persönlichkeitsrechten auf Dritte zu berücksichtigen. Würde beispielsweise ein einzelner Erbe die Löschung von Daten beantragen, könnte sich das betroffene Unternehmen lediglich auf überwiegende Interessen von Dritten oder der verstorbenen Person selbst berufen, jedoch nicht auf eigene überwiegende Interessen oder gesetzliche Pflichten, wie z.B. die Aufbewahrungspflicht gemäss Art. 12 Abs. 4 VE DSG. Daraus lässt sich schlussfolgern, dass der Erbe wesentlich mehr Rechte gegenüber einem Datenbearbeiter hat als der Erblasser zu Lebzeiten, was kaum die Absicht hinter Art. 12 VE DSG sein dürfte. Die Tatsache, dass weder in der Konvention 108 noch in der DSGVO spezifische Regelungen für verstorbene Personen aufgenommen wurden, lässt uns auch an der Relevanz einer spezifischen Regelung hinsichtlich der Fortführung der Angemessenheitserklärung durch die EU zweifeln. Angesichts des oben ausgeführten fehlenden datenschutzrechtlichen Nutzens und verbunden mit den einhergehenden Rechtsunsicherheiten muss **Art. 12 VE DSG u.E. unbedingt ersatzlos gestrichen werden**. Solche Sachverhalte sollen hinreichend im Zivilrecht geklärt werden und allfällige Lücken wären entweder über dieses oder durch vertragliche Lösungen zu schliessen.

Verwaltungssanktionen mit unmittelbarer Haftung der fehlbaren Unternehmen

scienceindustries lehnt den Vorschlag des VE DSG, das Sanktionssystem über das ordentliche Strafrecht auszugestalten, entschieden ab, denn dies führte im Ergebnis zu einer Vielzahl unerwünschter Folgen. So zeitigte ein solches Konzept die primäre strafrechtliche Verantwortlichkeit der natürlichen Personen für die Verletzung sanktionierter Tatbestände und nur subsidiär könnte auf die Unternehmen durchgegriffen werden, wobei uns gerade in dieser Hinsicht Art. 53 VE DSG als untauglich erscheint. Angesichts der vorgesehenen, beachtlichen Strafdrohungen ist eine primäre strafrechtliche Verantwortung der natürlichen Personen – sprich der Mitarbeiter von Unternehmungen – nicht nur unverhältnismässig, sondern birgt auch die Gefahr, dass es unternehmensintern zu einer erhöhten gegenseitigen Anzeigeaktivität durch Mitarbeitende kommt. Dies dürfte auch kaum mehr durch interne Vorgaben des Unternehmens in Bahnen gelenkt werden können, weil jeweils ein persönliches Schicksal einer Person mit diesen Fragestellungen verbunden ist, was bekanntlich – und bis zu einem gewissen Grade auch nachvollziehbar – unberechenbare Kräfte auslöst. Mit Blick auf die vielfältigen Aktivitäten, die angesichts der verschärften Datenschutzanforderungen im Tagesgeschäft von Unternehmen zu ungewollten Datenschutzverletzungen führen können, bestünde eine eminente Gefahr, dass ein sehr weiter Kreis von Mitarbeitern laufend zur strafrechtlichen Verantwortung gezogen würde. Entsprechend sähen sich die Unternehmen im Falle von Verurteilungen der betroffenen Personen nur schon aus Gründen ihrer eigenen Compliance gezwungen, das Arbeitsverhältnis mit solchen Mitarbeitern aufzulösen, währenddem diese auf dem Arbeitsmarkt aufgrund möglicher Strafregistereinträge eine deutlich reduzierte Wiedereinstellungschance zu gewärtigen hätten. So dürfte es sich dann auch alsbald als äusserst schwierig erweisen, überhaupt noch Mitarbeiter für solche Positionen rekrutieren zu können, mit dem Ergebnis, dass das unsererseits geforderte **Konzept des unabhängigen internen Datenschutzbeauftragen faktisch nicht mehr greifen würde.** In der Konsequenz wäre gerade der Durchsetzung des Datenschutzes damit nicht gedient, währendem dieser eine zusehends lähmende Wirkung auf das Geschäftsleben entfaltet und zu einem vergifteten Betriebsklima führt. Überdies müssten sich 26 kantonale Strafuntersuchungsbehörden und Jurisdiktionen mit dem strafrechtlichen Vollzug der Datenschutzbestimmungen befassen, was angesichts der oft schwierig lokalisierbaren Datenschutzverletzungen nicht nur zu stetigen Zuständigkeitsfragen, sondern auch zu unterschiedlichen Rechtsauslegungen und entsprechender inkonsistenter Rechtsanwendung führen dürfte.

Aufgrund dieser Analyse **spricht** sich **scienceindustries** für ein System mittels **Verwaltungssanktionen verbunden mit einer primären Verantwortlichkeit** der gegebenenfalls **fehlbaren Unternehmen aus.** Denn die Datenbearbeitung findet in aller Regel in Verrichtung geschäftlicher Aktivitäten statt und generiert letztlich in diesem Kontext einen Vorteil für das Unternehmen, weshalb dieses auch in der Verantwortung stehen soll. Verwaltungssanktionssysteme existieren in der Schweiz bereits heute und man kann auf den gemachten Erfahrungen aufbauen, wobei zu beachten wäre, dass der Bereich des Datenschutzes nicht unbesehen vergleichbar mit anderen Rechtsgebieten ist, in welchen dieser Ansatz bereits gilt (insbes. Kartellrecht) und entsprechend differenzierte Vorgaben und Regelungen angezeigt wären. Wie bereits erwähnt, besteht bei den vielfältigen Aktivitäten von Unternehmungen ein erhöhtes Risiko, ungewollt gegen die verschärften Datenschutzanforderungen zu verstossen, wobei festzustellen ist, dass solche Verstösse in aller Regel nicht zu nennenswerten finanziellen Vorteilen der Unternehmen führen. Im Bereich des Datenschutzes hätte sich das Verwaltungssanktionssystem deshalb nicht an der Massgabe der Abschöpfung von unrechtmässig erworbenen Gewinnen zu orientieren, sondern an jener der Durchsetzung einer effizienten Umsetzung der datenschutzrechtlichen Vorgaben. Deshalb sind wir der Ansicht, dass der Strafrahmen auch bei der Einführung von Verwaltungssanktionen bei der vorgeschlagenen **Höchstbussengrenze von einer halben Million**

CHF begrenzt bleiben muss und dieser nicht nach oben geöffnet werden soll. Vielmehr soll der Sanktionsrahmen nach dem Grundsatz des **Auswirkungsprinzips** ausgestaltet sein, wobei je nach Schwere der vorsätzlich begangenen Datenschutzverletzung in örtlicher wie sachlicher Hinsicht die Strafe höher oder tiefer festzusetzen wäre, begrenzt eben bei der Höchststrafe von CHF 500'000.-. Eine entsprechende Differenzierung erscheint uns sachgerecht, fällt denn ein Sachverhalt mit lokaler oder regionaler Auswirkung weniger ins Gewicht, als einer mit internationaler Betroffenheit. Dasselbe gilt u.E. wenn beispielsweise eine einfache Informationspflichtverletzung gegenüber einer Einzelperson ins Verhältnis gesetzt wird mit mehrfacher Widerhandlungen gegen das DSG, welche eine Vielzahl von Personen betreffen würde.

Ebenso wäre die Gelegenheit zu nutzen, die seit Jahren im Raum stehende Kritik des ungenügenden Rechtsschutzes der Parteien im Rahmen des verwaltungsstrafrechtlichen Untersuchungsverfahrens zu beherzen und sich stärker an den Grundsätzen der Europäischen Menschenrechtskonvention (EMRK) zu orientieren. Es sollte neu vorgesehen werden, im **gesamten Verwaltungsstrafverfahren dem Grundsatz des „nemo tenetur" ungeschmälerte Geltung durch gesetzgeberische Auflagen** zu verschaffen, so dass die Parteien sich nach Eröffnung des Verfahrens nicht mehr selber belasten müssen. Möglicherweise könnte Art. 113 der eidgenössischen Strafprozessordnung (StPO) für dieses Untersuchungsverfahren für anwendbar erklärt oder eine analoge Bestimmung im entsprechenden Gesetz vorgesehen werden. Schliesslich wäre ein **System von Rechtfertigungsgründen** oder aber **mindestens Strafmilderungs- resp. Strafminderungsgründen** vorzusehen, welche die Unternehmungen im Verwaltungsstrafverfahren vorbringen können. Zu denken wäre insbes. an vorsätzlich begangene Datenschutzverletzungen durch Mitarbeitende, wie z.B. Datendiebstahl. In diesen Ausnahmefällen könnte scienceindustries auch eine zusätzliche, unmittelbare strafrechtliche Verantwortlichkeit der fehlbaren natürlichen Personen akzeptieren, falls dies dann eben zu einer Reduktion des Strafmasses beim Unternehmen führt. Auch sollte das kooperative Verhalten der Unternehmungen im Rahmen der Untersuchung, das möglicherweise bis hin zu freiwillig selbstbelastenden Aussagen gehen kann, ebenso als klar strafmildernder Grund vorgesehen werden. Schliesslich wären auf technischen Fehlleistungen basierende Datenschutzverletzungen mit geringfügigen Auswirkungen auf den Datenschutz strafmildernd auszugestalten.

Sanktionenkatalog und Strafmass

Nach Ansicht von scienceindustries ist nicht nur das **strafrechtliche Bestimmtheitsgebot** in vielen vorgeschlagenen Strafbestimmungen oft **fraglich**, sondern der **Sanktionskatalog tendenziell überladen** und deshalb ist eine **Reduktion der Straftatbestände** zu prüfen. Im Umfang, wie wir uns in dieser Stellungnahme für eine Reduktion der Rechte der Datenschutzsubjekte und der Pflichten der Verantwortlichen aussprechen, führt dies entsprechend auch zur Aufhebung der damit verbundenen Sanktionierungen, denn wo keine Rechte verbrieft resp. keine Pflichten bestehen, können solche auch nicht verletzt werden und entsprechend keine Sanktionen greifen. Insbesondere sei an dieser Stelle wiederholt, dass die Strafbarkeit der Verletzung von Informationspflichten generell zu überdenken ist oder aber mindestens hierbei nur geringfügige Sanktionen festzulegen wären. Zudem halten wir fest, dass mit Blick auf die Fortführung eines mit Europa äquivalenten Datenschutzniveaus nach unserer Einschätzung gerade in diesem Bereich eine Orientierung am Übereinkommen SEV 108 des Europarates als genügend zu erachten ist.

Ersatzlos zu streichen ist sodann Art. 52 VE DSG, sind denn die angedrohten Freiheitsstrafen von bis zu drei Jahren zum einen absolut unverhältnismässig und diese Straftatbestände zum andern mit Blick auf ein

äquivalentes Datenschutzniveau mit Europa u.E. nicht erforderlich. **Generell ist von Freiheitsstrafen Abstand zu nehmen** und gänzlich auf deren Einführung zu verzichten, wurden denn auch keine solchen in den europäischen Regelwerken vorgesehen, welche ja allesamt wirksame und abschreckende, indes eben auch verhältnismässige Sanktionen verlangen. Offenbar wurde sowohl im Europarat als auch in den Institutionen der EU keine Notwendigkeit zur Einführung derart drastischer Sanktionen erkannt, was sachgerecht ist. Vielmehr erscheint die Strafandrohung von Freiheitsstrafe mit Blick auf den begangenen Rechtsbruch als unverhältnismässig kriminalisierend. Eine derart strenge Straffolge lähmte den Geschäftsverkehr übermässig und stellte einen beachtlichen Standortnachteil für die Schweiz dar.

scienceindustries **lehnt** des weitern jegliche **Strafbarkeit** für **fahrlässige Begehung** von Datenschutzverletzungen entschieden **ab**. Es sei erneut wiederholt, dass bei den vielfältigen Aktivitäten von Unternehmungen ein erhöhtes Risiko, ungewollt gegen die verschärften Datenschutzanforderungen zu verstossen, besteht. Diesem Umstand ist gebührend Rechnung zu tragen, dies nicht zuletzt auch in Anerkennung, dass die Unternehmen dem Schutz von Personendaten ohnehin einen hohen Stellenwert einräumen. Auch wenn heute schon grosse Anstrengungen zur Einhaltung der datenschutzrechtlichen Vorgaben getätigt werden, sind angesichts der zahlreichen Verarbeitungsaktivitäten sowie mit Blick auf die oft komplexen Prozesse unbeabsichtigte Datenschutzverletzungen auch bei Einhaltung hoher Standards in grossen wie in kleinen Unternehmen nicht immer zu vermeiden. Darin kann indes kein kriminelles Verhalten erkannt werden, weshalb die **Strafbarkeit von Datenschutzverstössen ausschliesslich auf deren vorsätzliche Begehung zu begrenzen** ist. Ein auf Vorsatz beschränkter Strafrahmen erscheint auch angesichts der typischerweise schwierigen sowie sehr aufwendigen Bewertungs- und Meldevorgängen bei der Aufklärung als auch Behebung von fahrlässigen Rechtsverstössen als angemessen und entsprechend geboten.

Stellung und Kompetenzen des Eidgenössischen Datenschutzbeauftragten

Vor dem Hintergrund der vorangegangen Ausführungen und in Anerkennung der internationalen Vorgaben, die neu im Bereich des Datenschutzes eine mit beachtlichen Kompetenzen ausgestattete (nationale) Aufsichtsbehörde fordern, schlägt scienceindustries ein vom VE DSG abweichendes Modell vor. Der **EDÖB** mit seiner beratenden, empfehlenden und letztlich anzeigenden Funktion hat sich im Grundsatz bewährt und wir würden es begrüssen, wenn an diesem **System unverändert festgehalten** wird. Nur schon mit Blick auf seine Bezeichnung als „Beauftragter" und seine organisatorische Einordnung bei der Bundeskanzlei, die von Bundesverfassung (BV) wegen als Stabsstelle des Bundesrates agiert (Art. 179 BV), drängt sich eine Beibehaltung des Systems auf. Im Übrigen wäre es auch fraglich, ob eine mit Verfügungsgewalt ausgestaltete Behörde von Verfassung wegen überhaupt der Bundeskanzlei angehören darf, sind doch die Exekutivgewalten in aller Regel den Departementen zugeordnet. Zudem orten wir Interessenskonflikte, wenn der mit umfassenden beratenden Funktionen ausgestattete Beauftragte des Bundes gleichzeitig auch Untersuchungsaufgaben - bis hin zur Kompetenz zur unangekündigten Hausdurchsuchung - erhält sowie weitere vorsorgliche Massnahmen verfügen kann. Abgesehen von solchen Konflikten führte dieser Umstand auch nicht zur notwendigen Vertrauensbasis, auf welcher beispielsweise das Konzept der guten Praxis wirksam greifen kann.

Wir regen deshalb an, dass der **EDÖB** unverändert als eine **bundesbeauftragte Stelle ohne Verfügungskompetenzen erhalten** bleibt und weiterhin alle im Zusammenhang mit der Umsetzung des DSG bestehenden Beratungs- und Empfehlungstätigkeiten wahrnimmt. So soll er auch inskünftig sowohl private Personen

wie auch Unternehmen in allen Belangen des Datenschutzes beraten, das Verzeichnis der Länder mit vergleichbarem Datenschutzniveau sowie das Verzeichnis der Firmen führen, die auf freiwilliger Basis einen internen unabhängigen Datenschutzbeauftragten gemeldet haben (vgl. Ausführungen auf Seite 12). Er würde im Rahmen der guten Praxis Empfehlungen ausarbeiten, wobei alleine schon aufgrund seiner Stellung nicht zu befürchten wäre, dass dabei eine „Schattengesetzgebung" entstünde, was mit Blick auf die Rechtssicherheit zentral ist. An ihn wären die meldepflichtigen Datenschutz-Folgenabschätzungen sowie weitere gesetzliche Meldepflichten zu richten und ebenso die meldepflichtigen Datenschutzverletzungen anzuzeigen. Zudem würde es in seiner Kompetenz liegen, Datenschutzverletzungen, von denen er Kenntnis erhalten hat, nach seinem Ermessen an eine **neu zu schaffende Bundesspruchbehörde** zu melden, die dann ihrerseits das Verwaltungsverfahren eröffnet, durchführt und allenfalls Verwaltungssanktionen ausspricht.

Entsprechend wäre somit eine **neue Bundesspruchbehörde** zu schaffen, die in einem Departement anzusiedeln wäre (wobei sich u.E. wohl das Eidgenössische Justiz- und Polizeidepartement [EJPD] als am geeignetsten erwiese) und die mit allen notwendigen Verfügungskompetenzen zur Durchführung eines Verwaltungsstrafverfahrens bis mit zur Verhängung von Verwaltungssanktionen auszustatten wäre. Damit würde die Schweiz die internationalen Vorgaben einer bestehenden **Aufsichtsbehörde mit Verfügungskompetenzen** samt jener zur **Verhängung von Verwaltungssanktionen** erfüllen, ohne dass sie das bewährte Institut des EDÖB aufgeben und diesen zudem mit Aufgaben und Kompetenzen ausstatten müsste, die zum einen zu Interessenkonflikten führen dürften und zum andern auch unter dem Aspekt der Gewaltenteilung fragwürdig sind. Zudem bestünde die Chance, eine zentrale Behörde zu etablieren, welche eine einheitliche Rechtsauslegung und -anwendung im Bereich der Sanktionierung gewährleisten könnte – dies im Unterschied zum im VE DSG vorgeschlagenen Ansatz über das ordentliche Strafrecht mit 26 kantonalen Vollzugsorganen. Sie wäre letztlich auch in der Lage, auf Datenschutz spezialisiertes und damit notwendigerweise versiertes Personal zu verpflichten, wie dies auf kantonaler Ebene unmöglich der Fall sein könnte. Dass damit beim Bund zusätzliche Kosten anfallen würden, ist nicht von der Hand zu weisen, doch muss dem auch entgegen gehalten werden, dass die zusätzliche Belastung der kantonalen Strafverfolgungsbehörden sowie deren Justiz vermutlich infolge der geringeren Professionalität volkswirtschaftlich betrachtet gar zu höheren Kosten führen dürfte. Wie bereits erwähnt, sprich sich scienceindustries auch dafür aus, gleichzeitig die Chance zu nutzen und **konkrete Verfahrensvorgaben zu machen, welche die Rechte der Verantwortlichen im Verwaltungsstrafverfahren in adäquater Weise garantieren**. Insbesondere wäre dabei an den Grundsatz des „nemo tenetur" zu denken und festzuschreiben, dass sich Verantwortliche auch dann im Verfahren nicht weiter selber belasten müssen, wenn sie vorgängig ihrer Pflicht zur Meldung der Datenschutzverletzung nachgekommen sind.

Ein solches System getrennter Kompetenzen – beratender EDÖB und Aufsichtsbehörde mit Verfügungs- und Sanktionskompetenzen – führte u.E. zu einer effektiveren Durchsetzung des Datenschutzes in der Schweiz und gleichzeitig könnten all die negativen Konsequenzen, die mit einer Sanktionierung von Datenschutzverletzungen über das ordentliche Strafrecht resultierten, weitgehend vermieden werden. Zudem könnte der EDÖB an sich nur so seine beratende und empfehlende Funktion glaubwürdig wahrnehmen, was in besonderem Mass auch für den Ansatz der guten Praxis gilt. Schliesslich würde die Schweiz damit eine dem Wortsinn der europäischen Regelwerke entsprechende Aufsichtsbehörde schaffen.

Wir sind uns bewusst, dass wir hiermit einen **neuartigen Vorschlag skizzieren**, den es im Detail zu vertiefen und konkret auszugestalten gälte. scienceindustries würde es begrüssen, wenn das **Bundesamt für Justiz**

diesen Ansatz aufnehmen und im Rahmen einer Arbeitsgruppe mit weiteren interessierten Kreisen einen **konkreten Vorschlag ausarbeiten** würde, wobei wir gerne unsere aktive Beteiligung anbieten.

Abschliessend halten wir fest, dass soweit vorliegende Stellungnahme sich nicht explizit zu weiteren Themen im Kontext der DSG-Revision äussert, wir auf die Stellungnahme von economiesuisse verweisen, die wir grundsätzlich unterstützen.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Dr. Beat Moser
Direktor

Jürg Granwehr
Leiter Pharma Schweiz

Kopie an:
economiesuisse, SwissHoldings
ASSGP, Intergenerika, Interpharma, vips

Seilbahnen Schweiz
Remontées Mécaniques Suisses
Funivie Svizzere
Pendiculares Svizras

ch-direct
Direkter Verkehr Schweiz
Service direct suisse
Servizio diretto svizzero
Servetsch direct Svizra

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Bern, 31. März 2017
Tel. +41 31 359 22 56, kai-leonie.tschan@voev.ch

Stellungnahme zum Vorentwurf des Bundesgesetzes über die Totalrevision des Datenschutzgesetzes

Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zur Stellungnahme zur Totalrevision des Datenschutzgesetzes (DSG). Anbei erhalten Sie die Stellungnahme des Verbandes für öffentlichen Verkehr (VöV) und Seilbahnen Schweiz (SBS) und des Vereins ch-direct (Geschäftsstelle des Direkten Verkehrs).

Einleitend möchten wir betonen, dass wir dem Schutz und dem vertrauenswürdigen Umgang mit den Kundendaten in der gesamten Branche des öffentlichen Verkehrs einen grossen Stellenwert beimessen. Die Bearbeitung der Kundendaten, welche selbstverständlich immer verhältnismässig sein muss, ist für den öV Schweiz allerdings von zentraler Bedeutung. Der Datenschutz und die Nutzung der Daten müssen deshalb in einem ausgeglichen Verhältnis zueinander stehen.

Um den Kunden und Kundinnen durchgehende und möglichst einfache Angebote anbieten zu können, ist der Austausch der Daten von zentraler Bedeutung. Dies gilt sowohl für den Datenaustausch im In- und Ausland. Grund dafür ist, dass die durchgehenden Reiseketten auch über die Landesgrenze hinausgehen sollen. Der VöV, SBS und ch-direct begrüssen deshalb die Anpassung des Schweizerischen Datenschutzrechtes an das Europäische Recht. Dies ist für den Austausch der Daten zwischen der Schweiz und der EU erforderlich. Für den öV Schweiz ist es allerdings von zentraler Bedeutung, dass die Regulierung nicht über das Schutzniveau der EU hinausgeht.

Die Branche braucht umsetzbare rechtliche Rahmenbedingungen, um den öV Schweiz weiterhin attraktiv gestalten und weiterentwickeln zu können. Insbesondere müssen die rechtlichen Rahmenbedingungen auch den zukünftigen Entwicklungen und der fortschreitenden Technologie Rechnung tragen. Der VöV, SBS und ch-direct sind der Meinung, dass einige Bestimmungen im Vorentwurf des DSG diesen Anforderungen nicht genügen. Die entsprechenden Bestimmungen wären für die Branche nur mit unverhältnismässigem Aufwand umsetzbar.

Dählhölzliweg 12
CH-3000 Bern 6
www.seilbahnen.org
info@seilbahnen.org
Tel +41 31 359 23 33
www.ch-direct.org
info@ch-direct.org
Tel +41 31 359 22 40
www.voev.ch
info@voev.ch
Tel +41 31 359 23 23

Zudem müssen die zukünftigen Bestimmungen genügend klar formuliert sein. Einige Bestimmungen sind für eine direkte Anwendung zu unbestimmt formuliert.

Die heutige Situation bezüglich der Aufsichtskompetenzen des EDÖB trägt dem Schutz der Daten Rechnung. Das Verhältnismässigkeitsprinzip wird gewahrt. Zudem behindern zu viele regulatorische Massnahmen den Markt und relativieren das Gesetz. Eine Stärkung der Aufsichtskompetenzen des EDÖB erachten der VöV, SBS und ch-direct als nicht verhältnismässig.

Nachfolgend finden Sie unsere Anliegen und Änderungswünsche in Bezug auf die Verhältnismässigkeit, die Umsetzbarkeit und den zukünftigen Entwicklungen und Herausforderungen des öffentlichen Verkehrs der Schweiz.

Wir danken Ihnen für die Kenntnisnahme unserer Stellungnahme und Berücksichtigung unser Anliegen und Änderungswünsche.

Freundliche Grüsse

i.A.

Ueli Stückelberger
Direktor VöV und SBS

Markus Thut
Leiter ch-direct

Anliegen und Änderungswünsche

Art. 3 lit. f DSG (Profiling)

Diese Definition geht über das EU-Recht hinaus und führt bei der Branche zu unverhältnismässigem Aufwand. Manuelle Auswertungen durch die Transportunternehmen (wie bspw. die manuelle Auswertung eines Kundendossiers oder eine Mitarbeiterauswertung) dürfen nicht als Profiling qualifiziert werden. Diese Auswertungen bedürfen nicht eines solch hohen Schutzes und die neue Definition würde zu unverhältnismässigem Aufwand führen.

Art. 3 DSG (Begriffe)

Unseres Erachtens sollte der Begriff des Beauftragten in dieser Bestimmung ausgeführt werden. Es ist nicht bei jeder Bestimmung in diesem Gesetz selbsterklärend, dass mit dem Begriff des Beauftragten der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragter bzw. –beauftragte gemeint ist. Diese Definition sollte in Art. 3 DSG nachgeschlagen werden können.

Art. 4 Abs. 5 DSG (Überprüfung der Richtigkeit)

Die Pflicht zur Korrektur und Ergänzung von Personendaten muss auch in Zukunft verhältnismässig sein. Der heutige Art. 5 Abs. 1 PBG sollte so beibehalten werden, da dieser sachgerechter und umsetzbarer ist als der neue Art. 4 Abs. 5 DSG.

Art. 6 Abs. 1 lit. a DSG (Bekanntgabe in Ausland)

Eine Einwilligung für jeden Einzelfall führt zu unverhältnismässig hohem Aufwand. Eine generelle Bekanntgabe der Daten der betroffenen Person ist genügend und verhältnismässig.

Art. 15 DSG (Automatisierte Einzelentscheidung)

Aus dieser Bestimmung wird nicht klar, was eine automatisierte Einzelentscheidung ist. Die aus dieser Bestimmung resultierenden Auswirkungen wären für den öV Schweiz aber erheblich, da sie Auswirkungen auf zukünftige Entwicklungen des gesamten öV Schweiz haben könnte. Hier bedarf es einer klaren Definition dieses Begriffs und des Anwendungsbereichs.

Art. 16 DSG (Datenschutz-Folgenabschätzung)

Datenschutz-Folgenabschätzungen sollten nur bei hohen oder sogar erheblichen Risiken für die Persönlichkeit oder der Grundrechte der betroffenen Person gefordert werden. Das erwähnte „erhöhte Risiko" in Art. 16 DSG sollte deshalb klar definiert werden. Andernfalls wären effiziente Verfahren in der Branche gefährdet und der Grundsatz der Verhältnismässigkeit fraglich.

Art. 17 DSG (Meldung von Verletzungen des Datenschutzes)

Die Pflicht zur Meldung von Verletzungen des Datenschutzes gegenüber dem Beauftragten sollte nur bei hohem bzw. erhöhtem Risiko für die Persönlichkeit oder die Grundrechte bestehen. Eine Meldung bei jeglichen Risiken wäre unverhältnismässig. Zudem ist eine Frist vorzugeben (entsprechend dem europäischen Recht).

Art. 19 lit. a DSG (Weitere Pflichten; Dokumentationspflicht)

Eine Dokumentation jeder Datenbearbeitung würde zu einem unverhältnismässigen Aufwand in der Branche führen. Eine Dokumentation über die Verarbeitungsaktivitäten würde das Ziel dieser Bestimmung ebenfalls erreichen. Die neu vorgesehene Dokumentationspflicht geht zudem über das europäische Recht hinaus.

Art. 20 DSG (Auskunftsrecht)

Das kostenlose Auskunftsrecht stellt für die schweizerischen öV-Unternehmen teilweise ein Missverhältnis zum grossen Aufwand dar. In diesen Fällen sollte der Auskunftsersuchende an den Kosten beteiligt werden können.

Art. 37 ff. DSG (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. –beauftragte)

Die heutige Situation bezüglich der Aufsichtskompetenzen des EDÖB trägt dem Schutz der Daten Rechnung. Das Verhältnismässigkeitsprinzip wird gewahrt. Zudem behindern zu viele regulatorische Massnahmen den Markt und relativieren das Gesetz. Eine Stärkung der Aufsichtskompetenzen des EDÖB erachten der VöV, SBS und ch-direct als nicht verhältnismässig.

Art. 50 ff. DSG (Strafbestimmungen)

Die Strafbarkeit bei Fahrlässigkeit (Art. 51 Abs. 2 PBG) wird in der Branche abgelehnt. Dies insbesondere deshalb, weil einige Bestimmungen (siehe Auflistung in Art. 51 Abs. 1 PBG) nicht genügend bestimmt sind. Wegen der Unklarheit dieser Bestimmungen führt dies in der Branche zu unkalkulierbaren Risiken. Für die Mitarbeitenden führt dies möglicherweise sogar zu unzumutbaren Risiken.

Verwaltungsbussen gegen das Unternehmen sind sinnvoll und verhältnismässig. Die strafrechtliche Verantwortlichkeit der handelnden Person (Mitarbeiter/in) ist allerdings nicht sachgerecht. Die Entlassung der natürlichen Person aus der strafrechtlichen Verantwortlichkeit sollte nicht mittels einer „Kann-Bestimmung" geregelt werden. Die Entlassung aus der strafrechtlichen Verantwortlichkeit sollte in jedem Fall, in dem eine Person für ein Unternehmen gehandelt hat, zwingend vorgesehen werden.

Art. 59 DSG (Übergangsbestimmungen)

Die unterschiedlichen Umsetzungsfristen sind nicht praxistauglich. Der Branche wäre gedient, wenn die Umsetzungsfristen einheitlich gestaltet würden.

VSA-AAS
Verein Schweizerischer Archivarinnen und Archivare
Association des archivistes suisses
Associazione degli archivisti svizzeri
Associaziun da las archivarias e dals archivaris svizzers
www.vsa-aas.ch

VSA-AAS
c/o Büro Pontri GmbH
Postfach
CH-3322 Urtenen-Schönbühl

t +41 (0)31 312 26 66
f +41 (0)31 312 26 68

info@vsa-aas.ch
www.vsa-aas.ch

Eidgenössisches Justiz- und Polizeidepartement
Vorsteherin
Bundesrätin Simonetta Sommaruga
jonas.amstutz@bj.admin.ch

Bern, 20. März 2017

Eingabe des Vereins Schweizerischer Archivarinnen und Archivare zum Vorentwurf Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Besten Dank für die Möglichkeit zur Stellungnahme im Rahmen der Vernehmlassung zur Totalrevision des DSG, von der wir gerne Gebrauch machen.

Die Archivierung macht Verwaltungshandeln für betroffene Personen und Dritte transparent und nachvollziehbar. Diese herausragende Bedeutung staatlicher, und ergänzend auch privater Archive innerhalb einer Demokratie, manifestiert sich immer wieder, zurzeit im Rahmen der Aufarbeitung fürsorgerischer Zwangsmassnahmen und Fremdplatzierungen vor 1981. Damit ermöglicht oftmals erst die sorgfältige und sichere Archivierung die Ausübung des Auskunftsrechts, einer der zentralen Ansprüche betroffener Personen im Datenschutzrecht.

Aufgrund seiner Vorbildfunktion für die anderen föderativen Ebenen, ist die Bundesgesetzgebung im Datenschutzrecht auch für kantonale und kommunale Archive wegweisend. Daher möchten wir in diesem Zusammenhang zwei Punkte gerne besonders positiv hervorheben.

Stärkung des Grundsatzes der Anbietepflicht bei Datenbearbeitung durch Behörden

Wir begrüssen, dass der Grundsatz der Anbietepflicht von Unterlagen an das Bundesarchiv in Art. 31 E-DSG, der bereits seit 2008 im DSG verankert ist, materiell unverändert übernommen wurde. Die umfassende Anbietepflicht von Personendaten stellt sicher, dass im Bereich der Datenbearbeitungen durch Bundesorgane auch weiterhin Daten zuerst dem Bundesarchiv angeboten werden und erst falls sie als nicht archivwürdig beurteilt werden, vernichtet werden dürfen. Entsprechend wichtig ist es, dass Art. 12 Abs. 5 E-DSG die unveränderte Geltung dieses Grundsatzes auch beim neu eingeführten Auskunftsrecht für Angehörige bereits verstorbener Personen durch den Vorbehalt anderer Bundesgesetze, wie dem Bundesgesetz über die Archivierung, hervorhebt.

VSA-AAS

Keine absolute Geltung des Rechts auf Vergessen

Des Weiteren unterstützt der VSA die im Entwurf vorgeschlagene Umsetzung des Rechts auf Vergessen, insbesondere die Betonung der nicht absoluten Geltung dieses Rechts in den Erläuterungen, vor allem im Hinblick auf gewichtige Interessen der Meinungs- und Informationsfreiheit und am Fortbestehen von Informationen, wie sie gerade Archive und andere Gedächtnisinstitutionen ermöglichen. Entsprechend begrüssen wir die explizite Aufnahme der öffentlichen Archive im Rahmen der Ausnahmebestimmungen zum Recht auf Vergessen in Art. 34 Abs. 4 E-DSG. Ebenso begrüssen wir die explizite Nennung von Archiven in den Erläuterungen zu Art. 25 E-DSG im Rahmen der Datenbearbeitung durch private Personen, deren Kernaufgabe es ist, Dokumente unverändert zu sammeln, zu erschliessen, zu erhalten und zu vermitteln.

Wir danken Ihnen für Ihre Kenntnisnahme unserer Ausführungen im Rahmen der Vernehmlassung. Selbstverständlich stehen wir Ihnen für Rückfragen gerne zur Verfügung. Bitte richten Sie Ihre Rückmeldungen an folgende Adresse: info@vsa-aas.ch.

Mit freundlichen Grüssen

Dr. Claudia Engler (Präsidentin)

Philippe Künzler (Delegierter)

Amstutz Jonas BJ

Von: Abouri Cornelia <Cornelia.Abouri@strom.ch>
Gesendet: Dienstag, 4. April 2017 15:47
An: Amstutz Jonas BJ
Cc: Beyeler Francis; Abouri Cornelia
Betreff: Stellungnahme VSE Datenschutzgesetz
Anlagen: Totalrevision-des-Datenschutzgesetzes_Stellungnahme_VSE_20170403.doc

Sehr geehrter Herr Amstutz

Ich lasse Ihnen anbei die Stellungnahme des VSE zur Totalrevision des Datenschutzgesetzes zukommen.

Freundliche Grüsse

Cornelia Abouri
Senior Expertin Public Affairs

Verband Schweizerischer Elektrizitätsunternehmen VSE
Hintere Bahnhofstrasse 10 | Postfach | 5001 Aarau
T +41 62 825 25 25 | direkt +41 62 825 25 15 | Fax +41 62 825 25 26

cornelia.abouri@strom.ch | www.strom.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Verband Schweizerischer Elektrizitätsunternehmen

Abkürzung der Firma / Organisation : VSE

Adresse : Hint. Bahnhofstrasse 10, 5001 Aarau

Kontaktperson : Francis Beyeler

Telefon : 062 825 25 40

E-Mail : francis.beyeler@strom.ch

Datum : 3. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Beyeler/VSE	Der VSE begrüsst die Anpassung des Datenschutzgesetzes an die neuen Technologien und die neuen europäischen Datenschutzbestimmungen. Damit dürfte der Zugang zum europäischen Markt auch weiterhin sichergestellt sein. Allerdings ist darauf zu achten, dass der administrative Aufwand für die betroffenen Unternehmen gering gehalten wird und nicht eine Legiferierung auf Vorrat erfolgt. Ein «Swiss Finish» ist weder notwendig noch wünschenswert. So dürfte sich die praktische Umsetzbarkeit der Vorlage in verschiedenen Punkten als schwierig erweisen bzw. zu einem unverhältnismässigen und nicht sachgerechten Zusatzaufwand führen. Zu nennen sind insbesondere - die deutlich erweiterte Informations- und Auskunftspflicht, welche zu weit greift. Es würde ausreichen, wenn die betroffenen Personen die Informationen auf Nachfrage hin erhalten würden. - die Regelungen im Bereich der Datenschutz-Folgeabschätzung mit der nicht-praktikablen Pflicht, sie dem EDÖB einzureichen und dessen Widerspruchsrecht innert dreier Monate abzuwarten. Mit dieser Regelung wären neue Business-Ideen während dreier Monate blockiert, was innovationshemmend wirkt. - die sehr weitgehenden Forderungen im Bereich der Datenschutzverletzungen (u.a. unverzügliche Meldung einer unbefugten Datenbearbeitung) und die überschiessenden Forderungen in Bereich der Strafbestimmungen.
Beyeler/VSE	Für die Strombranche ist das Datenschutzrecht insbesondere im Zusammenhang mit den neuen Bestimmungen im StromVG (gem. 1. Massnahmenpaket der Energiestrategie 2050, 13.074) relevant: Art. 17c StromVG Datenschutz 1 Auf die Datenbearbeitung im Zusammenhang mit intelligenten Mess-, Steuer- oder Regelsystemen findet das Bundesgesetz vom 19. Juni 1992 über den Datenschutz Anwendung. 2 Der Bundesrat erlässt die Ausführungsbestimmungen über die Bearbeitung der Daten. Er kann besondere Bestimmungen vorsehen, namentlich im Zusammenhang mit Lastgangmessungen. Grundsätzlich würde gestützt auf den aktuell vorliegenden Verordnungsentwurf mit Art. 8d „Umgang mit Daten aus intelligenten Mess-, Steuer- und Regelsystemen“ des revidierten StromVV eine ausreichende Rechtsgrundlage für die Branchenunternehmen im Kernbereich ihrer Tätigkeiten zur Anwendung kommen, doch könnten neue Geschäftsmodelle unter Umständen von dieser spezialgesetzlichen Bestimmung nicht erfasst sein,

	weshalb die Bestimmungen des revidierten Datenschutzgesetzes Anwendung finden würden. Je nach Art der Verwendung könnte diese Bearbeitung als Profiling i.S.v. Art. 3 lit. f rev. DSG qualifiziert werden. Dies hätte zur Folge, dass neben den bereits genannten Informations-, Auskunfts- und Risikoabschätzungspflichten auch die Pflicht bestehen würde, eine explizite Zustimmung des Kunden einzuholen. Dies wiederum würde einen grossen Mehraufwand bedeuten, ausser die explizite Zustimmung im Rahmen der AGB würde wie bis anhin als gesetzeskonform anerkannt.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Beyeler/VSE	DSG				Gemäss geltendem Datenschutzgesetz besteht die Möglichkeit, einen unternehmensinternen Datenschutzbeauftragten einzusetzen. Eine solche Funktion sieht auch das EU-Recht in Unternehmen unter gewissen Umständen ausdrücklich vor. Zudem ermöglicht sie den Unternehmen, die gesetzlichen Auflagen mit Unterstützung einer internen Fachperson zentral zu gewährleisten. Es ist nicht ersichtlich, weshalb auf diese Funktion künftig verzichtet werden soll. Antrag VSE: Art. 11a Abs. 5 lit. e und Art. 11 abs. 6 des geltenden Datenschutzgesetzes sind sinngemäss beizubehalten.
Beyeler/VSE	DSG	1			Juristische Personen werden vom neuen Art. 1 nicht mehr erfasst. Dies dürfte den Umgang mit Daten beispielsweise von Industriekunden erleichtern und ist zu begrüssen.
Beyeler/VSE	DSG	2	2	c	Der VSE erachtet die Einengung auf „unabhängige Justizbehörden“ als problematisch. Sie hebelt das Beweismittelrecht aus und wird zu mehr Auskunftsbegehren und damit zu höherem Aufwand für die Unternehmen führen. Es ist deshalb die Formulierung gemäss geltendem Datenschutzgesetz (Art. 2 Abs. 2 Bst. c) beizubehalten Änderungsantrag VSE: Art. 2 Geltungsbereich Es ist nicht anwendbar auf: c. ~~Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden~~ hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren; *(d.h. gem. geltendem Recht)*

Beyeler/VSE	DSG	3		d	Neu umfasst der gesetzlich definierte Begriff „Bearbeiten“ auch die Löschung von Daten. Dies führt zu unverhältismässigem Aufwand (Informationspflichten). Änderungsantrag VSE: Art. 3 Begriffe d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren~~, Löschen~~ oder Vernichten von Daten;
Beyeler/VSE	DSG	4	6		In Absatz 6 wird bei den Personendaten der neue Begriff „eindeutig“ eingeführt, welcher sich sprachlich zu wenig von „ausdrücklich“ bei den besonders schützenswerten Personendaten abgrenzt. Es ist zu befürchten, dass mit dem neuen Begriff „eindeutig“ konkludente Zustimmungen kaum mehr hinreichend sein werden. Das führt zu einem unnötigen administrativen Mehraufwand. Aus diesem Grund ist bei den Personendaten, die kein erhöhtes Sicherheitsniveau verlangen, die zusätzliche Zustimmung nicht notwendig. Änderungsantrag VSE: Art. 4 Grundsätze 6 Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und ~~eindeutig~~ ausdrücklich erfolgt. Für die Bearbeitung von besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.
Beyeler/VSE	DSG	5	3	d	Gemäss Abs. 3 lit. d dürfen Daten zwischen Mitgliedern einer Unternehmensgruppe nur übermittelt werden, wenn die unternehmensinternen Datenschutzvorschriften vorgängig durch den Beauftragten genehmigt wurden. Die Frist von 6 Monaten, welche dem Beauftragten für die Genehmigung eingeräumt wird, ist zu lange und es stellt einen zu grossen administrativen Aufwand dar. Der damit verbundene Zeitaufwand bedeutet einen volkswirtschaftlichen Nachteil. Das wäre nur gerechtfertigt, wenn es sich um besonders schützenswerte Daten handeln würde.

					Änderungsantrag VSE: Art. 5 Bekanntgabe ins Ausland 3 Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch: d. *Streichen*
Beyeler/VSE	DSG	5	5		Die Mitteilung unternehmensinterner Datenschutzvorschriften ist nicht notwendig. Die Vereinbarung muss dem EDÖB ohnehin vorgelegt werden und regelt den Datenschutz bereits. Zusätzliche Pflichten verursachen hohen administrativen Aufwand. Änderungsantrag VSE: Art. 5 Bekanntgabe ins Ausland 5 Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 1 ~~oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1~~ genehmigt sind oder nicht.
Beyeler/VSE	DSG	5	7		Abs. 7 regelt nicht, in welcher Frist und in welchem Umfang der Bundesrat eine entsprechende Liste derjenigen Staaten erstellt, die aus seiner Sicht einen angemessenen Schutz gewährleisten. Wenn die Liste derjenigen Staaten mit einem angemessenen Datenschutz einmal erstellt ist, dürfte ein Grossteil des administrativen Zusatzaufwands durch die revidierte Bestimmung zur Bekanntgabe von Personendaten ins Ausland entfallen Der Bundesrat ist deshalb zu verpflichten, die Liste, welche mindestens die europäischen Staaten (EWR und EU) umfassen sollte, so schnell wie möglich zu erstellen. Wünschenswert wäre ein Erlass mit Inkrafttreten, jedoch spätestens 3 Monaten nach Inkrafttreten. Änderungsantrag VSE: Art. 5 Bekanntgabe ins Ausland 7 Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet. <u>Innert drei Monaten ab Inkrafttreten dieses Gesetzes erstellt er eine Liste von Staaten.</u>

Beyeler/VSE	DSG	8	1		Das Empfehlungsrecht führt zu faktischen Verordnungen des EDÖB, was den ordentlichen Gesetzgebungsprozess aushöhlt und zu einer Unübersichtlichkeit bzw. zu Rechtsunsicherheit führt (vgl. hierzu auch die ElCom mit ihren „Mitteilungen“ bzw. die Weko mit ihren „Bekanntmachungen“). Falls das Empfehlungsrecht beibehalten wird, muss den Betroffenen das rechtliche Gehör gewährt werden, da eine solche Empfehlung materiell den Charakter eines Rechtssatzes geniesst. Zudem dürften solche Empfehlungen nur mit äusserster Zurückhaltung abgegeben werden und müssten wirtschaftlich vertretbar sein. Änderungsantrag VSE: Art. 8 Empfehlungen der guten Praxis 1 *Streichen*
Beyeler/VSE	DSG	8	2		S. Bemerkung zu Art. 8 Abs. 1 Die Empfehlungen sollen nur dort eingesetzt werden, wo es notwendig ist, um z.B eine einheitliche Praxis zu gewährleisten oder Prozesse zu standardisieren. Änderungsantrag VSE: Art. 8 Empfehlungen der guten Praxis 2 Der Verantwortliche, Wirtschaftsgruppen sowie interessierte Kreise können ~~die Empfehlungen des Beauftragten ergänzen oder~~ eigene Empfehlungen der guten Praxis ausarbeiten, wo dies notwendig erscheint. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie.
Beyeler/VSE	DSG	8	3		S. Bemerkung zu Art. 8 Abs. 1 Änderungsantrag VSE: Art. 8 Empfehlungen der guten Praxis 3 ~~Er~~ Der Beauftragte veröffentlicht ~~die von ihm erarbeiteten sowie~~ die von ihm genehmigten Empfehlungen der guten Praxis.

Beyeler/VSE	DSG	13-19			Generell gilt für Art. 13 bis 19 bzw. Kapitel 8.3.1 des erläuternden Berichts, dass die Bestimmungen über die Pflichten des Verantwortlichen nur bei der Bearbeitung von besonders schützenswerten Personendaten oder Profiling anzuwenden sind. Wenn die Pflichten für jedes Bearbeiten von Personendaten eingehalten werden müssen, dann führt das für die EVU zu einem unglaublichen, administrativen Aufwand, der nicht mehr tragbar ist.
Beyeler/VSE	DSG	13	1-3		Die Informationspflichten gehen viel zu weit und bringen den betroffenen Personen in der Regel keinen Mehrwert. Die Regelung sollte darauf beschränkt werden, dass die Informationen, wenn überhaupt nur auf Nachfrage geliefert werden müssen. S. zudem Bemerkung zu Art. 13-19. Änderungsantrag VSE: Art. 13 Informationspflicht bei der Beschaffung von besonders schützenswerten Personendaten oder Profiling 1 Der Verantwortliche informiert die betroffene Person auf Anfrage über die Beschaffung über die Beschaffung von besonders schützenswerten Personendaten oder Profiling; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. 2 Er teilt der betroffenen Person nach der Anfrage innert 30 Tagen diejenigen Informationen mit, die erforderlich sind, … b. die bearbeiteten besonders schützenswerten Personendaten oder die Kategorien der bearbeiteten besonders schützenswerten Personendaten; 3 Werden besonders schützenswerte Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person auf deren Anfrage zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.
Beyeler/VSE	DSG	13	4		Diese Pflicht, welche zusätzlich zu jener der Auftragsdatenvearbeitung gemäss Art. 7, besteht, ist unnötig, insbesondere wenn der Auftragsbearbeiter nicht im (vertraglichen) Verhältnis mit der betroffenen Person erscheint. Dies könnte die Geschäftsbeziehung erschweren. Wenn Abs. 4 aufrechterhalten wird, müsste diese auf jene Fälle beschränkt werden, in welchen der Auftragsbearbeiter klar und mit seiner eigenen Identität in der Beziehung zwischen dem Verantwortlichen

					und der betroffenen Person erscheint. Änderungsantrag VSE: Art. 13 4 *Streichen*
Beyeler/VSE	DSG	13	5		S. Bemerkung zu Art. 13-19 Änderungsantrag VSE: Art. 13 5 Werden die <u>besonders schützenswerten</u> Personendaten nicht bei der betroffenen Person beschafft, …
Beyeler/VSE	DSG	13	6 (neu)		Der Verantwortliche muss (wesentliche) Kosten für die Bearbeitung und Bekanntgabe von Daten auf den Antragsteller überwälzen können, es sei denn, es handelt sich um Anfragen im Zusammenhang mit einer Verletzung der Persönlichkeitsrechte. Änderungsantrag VSE: Art. 13 <u>6 Die Kosten für die Informationen dürfen den Betroffenen verursachergerecht überbunden werden.</u>
Beyeler/VSE	DSG	14	2+ 4	a	S. Bemerkung zu Art. 13-19 Änderungsantrag VSE: Art. 14 2 Werden die <u>besonders schützenswerten</u> Personendaten … 4 Darüber hinaus … a. … , falls überwiegende Interessen des Verantwortlichen dies erfordern und er <u>keine besonders schützenswerten</u> ~~die~~ Personendaten ~~nicht~~ <u>an</u> Dritt~~en~~ bekannt gibt;
Beyeler/VSE	DSG	15			S. Bemerkung zu Art. 13-19

					Änderungsantrag VSE: Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung betreffend besonders schützenswerte Personendaten oder bei Profiling 2 … und zu den bearbeiteten besonders schützenswerten Personendaten zu äussern.
Beyeler/VSE	DSG	16	1+2		Der Anwendungsbereich ist unklar und birgt die Gefahr, dass für sämtliche Arbeiten mit Daten eine Folgenabschätzung gemacht werden muss. Dies wäre ein massiv übertriebener Aufwand. Zudem würde die Regelung bedeuten, dass, die Einreichung der Folgenabschätzung beim EDÖB und das Abwarten dessen Widerspruchsrechts innert dreier Monate neue Business-Ideen während dreier Monate blockiert würden, was innovationshemmend wirkt. Art. 16 ist deshalb zu streichen. Änderungsantrag VSE: Art. 16 *Streichen* *Eventualantrag VSE:* Eventualiter muss die Massnahme auf grosse Risiken beschränkt werden, für welche sie allenfalls gerechtfertigt erscheint. Zudem weist der VSE darauf hin, dass Datenbearbeitungen keine Risiken für die „Persönlichkeit“ sind, sondern allenfalls Risiken für die Verletzung der Persönlichkeitsrechte. Wird an Art. 16 festgehalten, ist deshalb die gleiche Formulierung wie in Art. 18 Abs. 1 zu übernehmen. S. zudem Bemerkung zu Art. 13-19 Art. 16 Datenschutz-Folgenabschätzung bei besonders schützenswerten Personendaten oder bei Profiling 1 Führt die vorgesehene Datenbearbeitung von besonders schützenswerten Personendaten oder bei Profiling voraussichtlich zu einem ~~erhöhten~~ grossen Risiko ~~für die Persönlichkeit oder die~~ von Verletzungen der Persönlichkeit oder der Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen. 2 Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken ~~für die Persönlichkeit oder die~~ von Verletzungen der Persönlichkeit oder der Grundrechte der betroffenen Person …

Beyeler/VSE	DSG	16	5 (neu)		Prozesse und Zuständigkeiten sind klar zu definieren, damit der administrative Aufwand und die damit verbundenen Mehrkosten eingeschränkt werden können. Änderungsantrag VSE: <u>5 Der Bundesrat erlässt die Ausführungsbestimmungen, insbesondere zum Prozess und der Zuständigkeit.</u>
Beyeler/VSE	DSG	17			Diese Bestimmung ist in höchstem Masse unklar bezüglich Sinn und Zweck, Formulierung und Begriffswahl sowie Ausnahmeregelungen. Sie gibt daher viel zu grossen Interpretationsspielraum, so dass unter Umständen in sehr grossem Umfang Personen über Datenarbeiten informiert werden müssten. Unklar ist insbesondere, auf wen die Bestimmung abzielt, denn wenn der Verantwortliche weiss, dass eine beabsichtigte Datenbearbeitung den Datenschutz verletzt, darf er sie gar nicht erst durchführen. Da ist eine Meldung an den Beauftragten gem. Abs. 4 wenig sinnvoll. Ebenfalls schwierig zu beurteilen sein wird, wann ein Risiko einer Verletzung der Persönlichkeit vorliegt. Es muss bezweifelt werden, dass dies immer abgeschätzt werden kann. Der mit der Umsetzung dieser Bestimmung einhergehende Mehraufwand (Einführung neuer Prozesse) ist angesichts einer kaum möglichen wirksamen Umsetzung unverhältnismässig, weshalb Art. 17 zu streichen ist. Änderungsantrag VSE: Art. 17 *Streichen* *Eventualantrag VSE:* Eventualiter müsste die Bestimmung ausschliesslich dahingehend interpretiert werden, dass sie auf Dritte (Hacker, Vertragspartner, die trotz Verbot die Daten bearbeiten etc.) abzielt. S. zudem Bemerkungen zu Art. 13-19 sowie zu Art. 16 Art. 17 Meldung von Verletzungen des Datenschutzes <u>bei besonders schützenswerten Personendaten oder bei Profiling</u> 1 Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem <u>grossen</u> Risiko ~~für die Persönlichkeit oder die~~ <u>von Verletzungen der Persönlichkeit oder der</u> Grundrechte der

					betroffenen Person. 4 *Streichen*
Beyeler/VSE	DSG	18			Art. 18 ist ebenfalls unklar formuliert und mit immensen Kosten verbunden. Änderungsantrag VSE: Art. 18 *Streichen* *Eventualantrag VSE:* S. Bemerkungen zu Art. 13-19 sowie Art. 16. Art. 18 Meldung von Verletzungen des Datenschutzes bei besonders schützenswerten Personendaten oder bei Profiling durch Technik und datenschutzfreundliche Voreinstellungen 1 …, die ab dem Zeitpunkt der Planung der Datenbearbeitung das grosse Risiko von Verletzungen … 2 …, dass standardmässig nur diejenigen besonders schützenswerten Personendaten bearbeitet werden, …
Beyeler/VSE	DSG	19			Die Dokumentation sämtlicher Datenbearbeitungsschritte ist für ein EVU nicht praktikabel, da branchenspezifische Dienstleistungen zunehmend von spezialisierten externen Serviceanbietern erbracht werden („Cloud"-Software as a Service). Dieser Trend wird sich im Zuge der Marktliberalisierung verstärken. Für kleinere EVU, die diese Dienstleistungen aus Kostengründen nicht selber erbringen, ist es unmöglich, diese Vorgaben einzuhalten. Änderungsantrag VSE: Art. 19 *Streichen* *Eventualantrag VSE:* S. Bemerkung zu Art. 13-19 Art. 19 Weitere Pflichten bei der Bearbeitung von besonders schützenswerten Personendaten oder bei Profiling

					Der Verantwortliche … a. Sie dokumentieren ihre Datenbearbeitung bei besonders schützenswerten Personendaten oder Profiling;
Beyeler/VSE	DSG	24	1		Als Rechtfertigungsgrund muss auch das Verlangen einer befugten Behörde aufgeführt werden. Einhergehend mit den zunehmenden Kompetenzen von Behörden, z.B. der ElCom, oder im Zusammenhang mit den Bestimmungen über die Offenlegungspflichten kann der Verantwortliche gezwungen sein, persönliche Daten zur Verfügung zu stellen. Diese Fälle müssen durch das Gesetz abgedeckt sein. Änderungsantrag VSE: Art. 24 Rechtfertigungsgründe 1 Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse, auf Verlangen einer Behörde oder durch Gesetz gerechtfertigt ist.
Beyeler/VSE	DSG	50			Auch wenn eine gewisse Anpassung aufgrund der EU Kompatibilität notwendig ist, schiesst man hier weit über das Ziel hinaus. Dies kann durch zwei Beispiele eindrücklich illustriert werden: Vergleich 1: Ein fahrlässiger Verstoss gegen das DSG soll künftig gleich massiv geahndet werden, wie die fahrlässige Verletzung des Bankgeheimnisses. Vergleich 2: Die fahrlässige Verletzung des Amts-, Anwalts- oder Arztgeheimnisses ist nicht strafbar. Zudem ist der persönliche, strafrechtliche Charakter der Sanktionen unverhältnismässig und nicht zielführend. Speziell diejenigen Personen, die wie etwa betriebliche Datenschutzverantwortliche in ihrer Tätigkeit für den Datenschutz an sich geschützt und gestärkt werden sollten, werden durch die Schaffung eines persönlichen Strafbarkeitsrisikos unnötig unter Druck gesetzt und exponiert. Mitarbeiter in den Unternehmen werden sich hüten, bei strafrechtlich bedrohten Datenschutzfragen selbst Entscheide zu treffen, ohne sich über externen Rechtsrat durch Spezialisten abgesichert zu haben, was zu einer unnötigen Verteuerung der Datenbearbeitung führt und dazu, dass die Möglichkeiten des DSG zur Datenbearbeitung nicht ausgeschöpft werden. Hinzu kommt, dass die Mitarbeitenden mit unpraktikablen Informationspflichten (Art. 13 und 15), Meldepflichten (Art. 17), Dokumentationspflichten (Art. 19) bussbewehrt werden. Ebenfalls störend sind in diesem Zusammenhang die unhaltbaren Datensicherheitspflichten (Art. 11) und Privacy by

					Design (Art. 18). Die massive Bussenandrohung reduziert auch die Agilität der EVU und erhöht deren Kosten massiv. Die Entscheidungsträger (natürliche Personen) werden das nachvollziehbare Bedürfnis nach Absicherung haben. Änderungsantrag VSE: Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten 1 Mit Busse ~~bis zu 500 000 Franken~~ werden private Personen auf Antrag bestraft: a. … 2 Mit Busse ~~bis zu 500 000 Franken~~ werden private Personen bestraft, wer vorsätzlich: b. *Streichen* e. *Streichen* 3 *Streichen* 4 *Streichen* *Eventualantrag VSE:* Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten 1 Mit Busse bis zu ~~500 000~~ 100 000 Franken werden private Personen auf Antrag bestraft: a. … 2 Mit Busse bis zu ~~500 000~~ 100 000 Franken werden private Personen bestraft, wer vorsätzlich: a. … 3 Mit Busse bis zu ~~500 000~~ 100 000 Franken werden private Personen auf Antrag bestraft, die es vorsätzlich unterlassen: a. … 4 Wer fahrlässig handelt, wird mit einer Busse von höchstens ~~250 000~~ 50 000 Franken bestraft.
Beyeler/VSE	DSG	51			S. Bemerkung zu Art. 50 Änderungsantrag VSE: Art. 51 Verletzung der Sorgfaltspflichten 1 Mit Busse ~~bis zu 500‘000 Franken~~ werden private Personen auf Antrag bestraft, die vorsätzlich:

					a. … 2 *Streichen* *Eventualantrag VSE:* Art. 51 Verletzung der Sorgfaltspflichten 1 Mit Busse bis zu ~~500'000~~ 100 000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich: a. … 2 Wer fahrlässig handelt, wird mit einer Busse von höchstens ~~250 000~~ 50 000 Franken bestraft.
Beyeler/VSE	DSG	52			S. Bemerkung zu Art. 50 Änderungsantrag VSE: Art. 52 Verletzung der beruflichen Schweigepflicht 1 mit Busse ~~Freiheitsstrafe bis zu drei Jahren oder Geldstrafe~~ wird auf Antrag bestraft, wer vorsätzlich geheime Personendaten bekanntgibt: a. …
Beyeler/VSE	DSG	53			S. Bemerkung zu Art. 50 Änderungsantrag VSE: Art. 53 *Streichen* *Eventualantrag VSE:* Art. 53 Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse ~~500 000~~ 100 000 Franken nicht überschreitet …
Beyeler/VSE	DSG	59			Die Umsetzung der Datenschutzvorgaben erfordert die Anpassung diverser Systeme und eine bessere Implementierung von zugriffsberechtigungsregeln. Für diese Umstellungen sind zwei Jahre zu kurz. Es

					braucht mindestens fünf Jahre Übergangsfrist. Änderungsantrag VSE: Art. 59 ~~Zwei~~ Fünf Jahre nach Inkrafttreten dieses Gesetzes müssen …

Amstutz Jonas BJ

Von: Bucklar, Daniel <d.bucklar@eos-schweiz.com>
Gesendet: Freitag, 31. März 2017 17:19
An: Amstutz Jonas BJ
Betreff: Stellungnahme des Verbands Schweizerische Inkassotreuhandinstitute vsi zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)
Anlagen: 170331 VSI VE-DSG Totalrevision des Datenschutzgesetzes Formular für Stellungnahme de.docx

Sehr geehrter Herr Amstutz

Als Sekretär des Verbands Schweizerische Inkassotreuhandinstitute vsi beehre ich mich, Ihnen namens des Vorstandes unsere Stellungnahme zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) zuzustellen.

Ich wünsche Ihnen einen guten Empfang des Dokumentes.

Freundliche Grüsse

Daniel Bucklar
Sekretär Verband Schweizerische Inkassotreuhandinstitute vsi

Daniel Bucklar, lic. iur.
Corporate Legal Counsel

EOS Schweiz AG
Flughafenstrasse 90
CH-8302 Kloten
Phone +41 58 411 73 00 | d.bucklar@eos-schweiz.com
Mobile +41 79 227 59 63 | www.eos-schweiz.com

With head and heart in finance

Mitglied im VSI Verband Schweizerischer Inkassotreuhandinstitute

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Verband Schweizerischer Inkassotreuhandinstitute vsi

Abkürzung der Firma / Organisation : vsi

Adresse : c/o Advokaturbüro Küng und Hunziker - Lindenhofweg 9 - 3123 Belp

Kontaktperson : Bucklar Daniel

Telefon : +41 31 819 33 66

E-Mail : advokatur-kueng-hunziker@bluewin.ch

Datum : 31. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
vsi	Der vsi ist *der* Verband der Schweizerischen Inkassobranche. Nur die dem vsi angeschlossenen Mitglieder garantieren ein ethisch einwandfreies Inkasso. Der vsi bearbeitet 3,3 Millionen Inkassofälle mit einem Volumen von über 11 Milliarden Schweizer Franken. Damit leistet er einen wesentlichen Nutzen für die schweizerische Volkswirtschaft. Der VSI setzt sich für ein unternehmensfreundliches Umfeld und optimale wirtschaftliche Rahmenbedingungen ein. **Grundsätzliche Fragestellungen zum Vorentwurf DSG** Der Vorentwurf zum DSG zeugt insgesamt von einem ausgeprägten staatlichen Übereifer und ungenügender Reflexion. Er hebelt ohne Not diverse, ansonsten unbestrittene Rechtsgrundsätze aus (Vertragsfreiheit, Schutz von Geschäftsgeheimnissen, Abweichung vom Grundsatz, dass niemand sich selbst belasten muss, etc.). Die Vorlage wird von Seiten des vsi insgesamt als legislatorischer Overkill zurückgewiesen. Ein erheblicher Eingriff in die Vertragsfreiheit liegt v.a. in den völlig überschiessenden Begründungs-, Anhörungs- und Informationspflichten; zivilrechtlich muss der Nichtabschluss eines Vertrages grundsätzlich nicht begründet werden, nach DSG soll dies aber plötzlich erforderlich sein, wenn die Ablehnung auf einer automatisierten Datenbearbeitung basiert. Die stipulierte Pflicht zur Selbstanzeige widerspricht ebenfalls ansonsten unbestrittenen Rechtsgrundsätzen, schliesslich wurde dem Schutz von Geschäftsgeheimnissen offensichtlich nicht die notwendige Aufmerksamkeit geschenkt, etc. In welchen Punkten eine Anpassung an die DSGVO 2016/679 und/oder an die Konvention 108 wirklich erforderlich ist, und wie weit diese im Einzelfall gehen muss, bleibt im Dunklen. Der Erläuterungsbericht verweist meist einfach generell auf das Europarecht, was als Begründung aber offensichtlich nicht ausreicht. Teilweise werden in ausländischen Erlassen enthaltene Einschränkungen der Datenbearbeitung sogar noch ausgeweitet (die sattsam bekannte Neigung zum "Swiss Finish" ist auch hier festzustellen). Der tatsächliche Anpassungsbedarf wird auch in der Regulierungsfolgenabschätzung der PWC nicht beleuchtet. Zur Übungsanlage gehörte offenbar nicht, das Revisionsvorhaben kritisch zu diskutieren. Das Papier der PWC stellt vielmehr einseitig auf die Vorgaben der Politik ab. Entsprechend wohlwollend ist denn auch die Abschätzung der Folgen ausgefallen, die wir nicht teilen können. Die administrative Belastung für die KMU (Datenschutzverantwortlicher, Folgeabschätzungen, Informationspflichten unklaren Umfangs, Begründungspflichten für Entscheide, etc. etc.) wird offensichtlich unterschätzt. Selbst dort, wo die Botschaft im Interesse der Wirtschaft auf die Praktikabilität eingeht, spiegelt sich dies im Wortlaut der Vorlage häufig nicht (so etwa bei den Informationspflichten).

	Offenbar sind einige neue Regelungen wegen der Schengen-Richtlinie in den VE DSG aufgenommen worden, die jetzt auch auf Private ausgedehnt werden sollen (z.B. die weitgehenden Befugnisse des Beauftragten zum Erlass von Verfügungen). Dies wäre ggf. im Rahmen des Schengen-Acquis bzw. im öffentlich-rechtlichen Teil des DSG zu regeln. Ein ungelöstes Problem liegt in der fehlenden Regelung für eine Daten*sperre*. Eine Löschung reicht nicht unbedingt, um einen Eintrag dauernd aus einer Datenbank zu entfernen. Um zu gewährleisten, dass eine Person zu einem späteren Zeitpunkt nicht wieder in den Datenbestand gelangt, müssen deren Identifikationsmerkmale (idealerweise mit einem eindeutigen Personenidentifikator) gespeichert werden können. Der vsi hat stets die Auffassung vertreten, dass der Datenschutz für den öffentlichen und den Privatbereich in zwei separaten Gesetzen geregelt werden sollte. Die Vermischung von öffentlich- und privatrechtlichen Regelungen im gleichen Erlass führt zu einer Auflösung der - sinnvollen - Unterscheidung zwischen Privatrechtsverkehr einerseits, Regelungen zum Verhältnis zwischen Staat und rechtsunterworfenem Bürger anderseits. Ausserdem könnte dann auch die Umsetzung des Schengen-Acquis da erfolgen, wo sie hingehört, nämlich ins öffentliche Recht. Anstelle in vorauseilendem Gehorsam einer europäischen Institution zu folgen, wäre es angezeigt die gesamte Kodifizierung der SR 235.xyz vorzunehmen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
vsi	VE-DSG	1			Nicht nur die juristischen Personen, sondern auch die im HR eingetragenen Einzelunternehmen und Mitglieder von Personengesellschaften sind vom Schutz auszunehmen, den das DSG für von einer Datenbearbeitung betroffene Personen vorsieht. Die Abgrenzung der geschützten von den nicht geschützten Personenkategorien ist in dieser Form nicht sachgerecht. Im HR eingetragene Einzelfirmen oder Mitglieder von Personengesellschaften wären datenschutzrechtlich vielmehr gleich zu behandeln wie juristische Personen. Die strafrechtlichen Bestimmungen über den Schutz der Ehre und das Verbot des wirtschaftlichen Nachrichtendienstes sowie der Persönlichkeitsschutz gemäss Art. 28ff. ZGB (die für diese Kategorien auch weiterhin gelten würden), wären aus unserer Sicht ausreichend.
vsi	VE-DSG	2	2	c	Beibehaltung des geltenden Wortlauts. Der VE will nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erst- und zweitinstanzliche Gerichte soll die bisherige Einschränkung also nicht mehr gelten. Dies öffnet Missbräuchen Tür und Tor (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).
vsi	VE-DSG	3		c	Ziff.4: Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Bilder in Zeitungen wären damit ausgenommen (nach dem jetzigen Wortlaut würden sie unter den Begriff der "biometrischen Daten" fallen).
vsi	VE-DSG	3		c	Ziff. 5: Die Bestimmung ist in dieser allgemeinen Form problematisch. etwa wenn Vermögensdelikte zur Diskussion stehen, von denen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste.
vsi	VE-DSG	3		f	Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes "Daten". Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um "Personendaten". Die reflexartige Übernahme von Begriffen des ausländischen Rechts beinhaltet die Gefahr, dass auch die Anwendung sich primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und weder notwendig noch sachgerecht. Dies umso weniger, als der Begriff des "Profiling" gegenüber dem EU-Recht sogar ausgeweitet worden ist; die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise.

					Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Kautelen und Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Was damit gewonnen wäre, ist unerfindlich. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich höchst kontraproduktiv, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als "Voraussage" eines späteren Verhaltens interpretiert werden können. Die Revision schiesst hier weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen. ohne all die Kautelen einzuhalten, die der VE mit dem "Profiling" verknüpft; selbst die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind, würde plötzlich problematisch, etc. Der Begriff des "Profiling" ist zu unbestimmt und gefährdet damit die Rechtssicherheit. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem "Persönlichkeitsprofil" des geltenden Rechts absolut abzulehnen.
vsi	VE-DSG	3		h und i	Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), eventualiter zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem " Auftragsbearbeiter" ist verschwommen und führt zu unklaren - teilweise unsinnigen - Aufteilungen der Verantwortung und Doppelspurigkeiten. Offenbar wird zudem übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen *kann*. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für den "Verantwortlichen"?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den "Verantwortlichen?") geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den "Verantwortlichen"?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht. Unklar ist auch, ob Arbeitnehmer unter den Begriff des "Auftragsbearbeiters" fallen können, was dem Wortlaut und der Systematik entspräche, aber offensichtlich zu einer völlig ausufernden Verantwortlichkeit und gegebenenfalls zu Strafbarkeit führen würde.
vsi	VE-DSG	4	3		Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft nur neue Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern

					"klar erkennbar" ist. Die Botschaft argumentiert, es sei keine Änderung beabsichtigt. Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. Die Einführung kompatibler Bearbeitungszwecke ist zu begrüssen.
vsi	VE-DSG	4	4		Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt. Die Aufbewahrungsfrist von Daten soll dem allgemeinen Verjährungsrecht des OR zu unterstellen (10 oder 5 Jahre) sein. Es sei zudem an die Aufbewahrungsfrist von Geschäftsbüchern und **Belegen** im Sinne von Art. 958f OR erinnert.
vsi	VE-DSG	4	5		Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Seite 47 des Erläuterungsberichts sind hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten, sonst wird nur neue Unsicherheit geschaffen. Eventualiter: Beschränkung von Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind", Streichung des Restes dieses Passus'. Die zweite Hälfte des ersten Satzes sowie Satz 2 sind schon aus sachlogischen Gründen zu streichen. Wenn die Daten nicht "richtig" sind, so wird der Bearbeiter wohl in eigenem Interesse an einer Berichtigung interessiert sein. Bekanntlich fängt die "Bearbeitung" ja schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE). Eine fortdauernde Verpflichtung zur Nachführung wäre offensichtlich unerfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status' einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind!. Art. 4 Abs. 5 VE-DSG hat die Qualität einer Verordnungsbestimmung und nicht einer Gesetzesbestimmung.
vsi	VE-DSG	4	6		Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die in Art. 3 lit. f vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (s. auch die Bemerkungen zu Art. 3 lit. f VE)
vsi	VE-DSG	5	1		Der Begriff "schwerwiegend" ist auszulegen, eventualiter ist der Absatz zu streichen. Generell ist festzuhalten, dass in Art. 5 Gesetzesartikel werden mit Verordnungsbestimmungen vermischt. Es sind auch keine wichtigen Grundsätze vorgesehen und / oder die bestehenden Grundsätze sind teilweise redundant (vgl. z. B Art. 5 Abs. 2 mit Art. 5 Abs. lit. a VE-DSG. Der ganze Artikel ist typischer Ausfluss von Swiss-Finish, in dem er viel weiter geht als die europäische Schwesternorm DSGVO.
vsi	VE-DSG	5	3	d	Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG.

vsi	VE-DSG	5	4 - 6		Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt - wie aus dem Wort ersichtlich - nach den Weisungen des Verantwortlichen, dem - wiederum entsprechend seiner Bezeichnung - die Verantwortung für die Information des Beauftragten obliegt.
vsi	VE-DSG	6	1	b	Die Inkassotätigkeit im Ausland ist damit gefährdet, weil die Norm abschliessend und kumulativ zu verstehen ist.
vsi	VE-DSG	6	2		Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1, lit b, c und d ins Ausland bekanntgegeben wird; dies gilt erst recht, wenn - wie hier - neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Die Verantwortlichkeiten sind einmal mehr unklar geregelt. Die Bestimmung ist im Übrigen auch insofern heikel, als solche Meldungen z.T. sensible Geschäftsinterna betreffen werden (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetz auch für Dritte einsehbar werden. Dem Schutz von Geschäftsgeheimnissen ist im Rahmen des VE DSG generell nicht die nötige Aufmerksamkeit geschenkt worden.
vsi	VE-DSG	7	2		Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Der Auftragsbearbeiter ist auch hier zu streichen.
vsi	VE-DSG	7	3		Schaffung der Möglichkeit einer generellen Einwilligung.
vsi	VE-DSG	8			Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der "interessierten Kreise" - erfahrungsgemäss damit einseitig der politischen Linken - ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. U.a. ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen ohne diese zu hinterfragen zugrunde legen werden. Der Beauftragte wird im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich Recht setzen. Dies wiegt umso schwerer, als der Beauftragte noch nicht einmal Jurist zu sein braucht.
vsi	VE-DSG	9			Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zulasten des Datenbearbeiters führen.

vsi	VE-DSG	10	2		2. Satz: Die Berücksichtigung des internationalen Rechts ist zu streichen. Da der Bundesrat bekanntlich in vorauseilendem Gehorsam internationale Normen ohnehin übernimmt, ist ihm hier nicht noch legalen Raum zu bieten.
vsi	VE-DSG	12	2		Der Gesetzgeber unterlässt die Definition einer "faktischen Lebensgemeinschaft". Ab welchem Zeitpunkt ist eine Lebensgemeinschaft "faktisch"?
vsi	VE-DSG	12	4		Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Allfällige Änderungen wären im ZGB vorzunehmen. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und Löschungsrecht völlig ausreichen. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären, etc. Art. 4 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen.
vsi	VE-DSG				Vorbemerkungen zum 3. Abschnitt: **Vorbemerkungen**: - Es fehlt an Übergangsbestimmungen, die regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar. - die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention - und nicht die DSGVO - den Massstab für den " angemessenen" Datenschutz zu liefern haben.
vsi	VE-DSG	13	1 + 2		Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird festgehalten, es genüge eine "allgemeine Information" im beschriebenen Sinn (vgl. S. 55). Der Wortlaut von Art. 13 VE widerspricht dem allerdings. In der vorliegenden Form ist die Bestimmung völlig impraktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. In einem Wort: Ein kompletter Overkill (dies wurde sogar in der RFA der PWC richtig erkannt, wenn auch anscheinend nur von einer Minderheit; vgl. Ziff. 4.1.1.5 des genannten Dokuments). Dieser wäre umso gravierender,

					als dann je nach Tätigkeit des datenverarbeitenden Unternehmens jedermann auch noch sämtliche Empfänger und Empfängerinnen bekanntgegeben - und damit Geschäftsgeheimnisse offengelegt - werden müssten. Der Aufwand wäre schlicht jenseits von Gut und Böse. Es muss genügen, dass diese Informationen öffentlich zugänglich sind.
vsi	VE-DSG	13	3		Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist unakzeptabel. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, wo persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger auch noch der "unschuldigsten" Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen. Bemerkung: Die Weitergabe von Daten innerhalb eines Konzerns wird damit unnötig erschwert (Konzerngesellschaften gelten ja als Dritte).
vsi	VE-DSG	13	4		Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
vsi	VE-DSG	13	5		Ersatzlos streichen; eventualiter. Beschränkung der *aktiven* Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten. Die vorliegend stipulierte, uferlose Informationspflicht ist impraktikabel und völlig unverhältnismässig. Die Bestimmung ist im Übrigen strenger als die DSGVO, die immerhin noch einen Monat Frist gewährt (!). Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird.
vsi	VE-DSG	14			Wurde unnötigerweise enger als die CON108 gefasst.
vsi	VE-DSG	14	1		Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung), in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist.
vsi	VE-DSG	14	2		Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden.

					Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der Vorentwurf für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
vsi	VE-DSG	14	4	a	Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Bemerkung: Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns unnötig erschwert.
vsi	VE-DSG	15	1		**Streichen**, ev. um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a) DSGVO EU (2016/679) ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als überzogener und unreflektierter Versuch, Konsumenten vor jedweder Art von automatisierten Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise begründbar sein, und was eine "erhebliche Auswirkung ist, dürfte letztlich von der Sensibilität des Betroffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte Art. 22 DSGVO EU nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor - eine Abweichung wäre demnach zweifellos auch für die Schweiz zulässig. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Die Formulierung der "Auswirkungen" ist so breit, dass jeder kommerzielle Entscheid - z.B. über eine Lieferung von Ware gegen Rechnung - darunter fallen kann. Auch die Lieferung von Ware gegen Rechnung ist in keiner Weise zwingend, und die Verweigerung darf nicht begründungspflichtig werden. In der **Inkassobranche** werden automatisierte Entscheide immer wichtiger, um wirtschaftlich zu sein. Es kann nicht sein, dass automatisierte Mahnung oder Betreibungsbegehren gegenüber dem Schuldner oder Dritten begründbar wird.
vsi	VE-DSG	15	2		Streichen. Diese Bestimmung entlastet einmal mehr einseitig den Staat.
vsi	VE-DSG	16			Streichen. In den Wortlaut kann jeder hineindeuten, was er will. Im Ergebnis wird wohl jedes Unternehmen eine solche "Folgeabschätzung" vornehmen müssen, welches mehr tut, als die Daten seiner eigenen

					Kunden zu bearbeiten. Hier wird ein bürokratisches Monstrum in die Welt gesetzt, das in der Privatwirtschaft im Ergebnis nichts bringen wird (im öffentlichen Sektor mag es hingegen durchaus angebracht sein). Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier und Zeit dafür aufwenden müssen. Der Verweis auf die Grundrechte macht übrigens einmal mehr deutlich, dass ein Datenschutzgesetz, welches sowohl den privaten als auch den öffentlichen Sektor regeln will, zwangsläufig zu Regulierungen führt, die dem einen oder anderen Bereich unangemessen sind. Vor kurzem war der Tagespresse zu entnehmen, wie schwer der Bundesrat sich mit der Aufgabe der Regulierungsfolgeabschätzung tut. Dies sollte auch hier zur Vorsicht mahnen; im Gegensatz zu staatlichen Organen hat ein Rechtsunterworfener ja gravierende Konsequenzen bis hin zu seiner wirtschaftlichen Vernichtung zu befürchten für den Fall, dass er die Aufgabe der "Folgenabschätzung" nicht zur Zufriedenheit der Amtsstellen oder Gerichte löst, die sich mit ihm befassen wollen oder müssen. Siehe dazu auch die über das Ziel hinausschiessenden Strafbestimmungen (Art. 50 ff. VE-DSG).
vsi	VE-DSG	16	3 + 4		Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist wäre im Übrigen auch zu lang.
vsi	VE-DSG	17			Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien. Wieso dieser im Bereich des Datenschutzes plötzlich nicht mehr gelten soll, ist völlig unerfindlich; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Der Verantwortliche müsste sich m.a.W. nicht nur an das datenschutzrechtliche, sondern auch noch an das strafrechtliche Messer liefern. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der nachgerade horrenden Strafandrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer regelrechten Flut an Selbstanzeigen zu rechnen, die nur den Apparat des Beauftragten übermässig aufblähen würde. Es ist zudem nicht damit zu rechnen, dass dem Beauftragten angesichts der innenpolitischen Grosswetterlage weitere Stellen zugesagt werden, womit allgemein mit rechtsverzögernder respektive rechtsverweigernder Folgen zu rechnen ist.

vsi	VE-DSG	17	2		In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen.
vsi	VE-DSG	17	4		Vgl. den Antrag zu Art. 14 Abs. 4.
vsi	VE-DSG	18			Ersatzlos streichen. Die Bestimmung ist redundant, der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
vsi	VE-DSG	19			Ersatzlos streichen. Die Bestimmung ist nicht nur überflüssig, sondern teilweise gar nicht umsetzbar. Die stipulierte Dokumentationspflicht würde für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b. ist sodann von vornherein nicht umsetzbar bzw. nachgerade absurd. Was gewonnen sein soll, wenn alle früheren Empfänger von Daten über jede spätere Änderung, Löschung oder Vernichtung informiert werden, ist völlig unerfindlich. Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine - allfällige - Verletzung von Datenschutzgrundsätzen machen zu müssen oder über "Einschränkungen" der Datenbearbeitung gem. Art. 25 machen zu müssen (bei der obendrein nicht klar ist, was man sich darunter vorzustellen hätte). Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Zudem würde die Umsetzung der Bestimmung häufig ihrerseits zu Datenschutzverletzungen führen. Bezüger von Wirtschaftsauskünften haben häufig gar kein schützenswertes Interesse daran, von späteren Änderungen einer Auskunft Kenntnis zu erhalten; dies gilt z.B. immer dann wo die vertraglichen Beziehungen zum Betroffenen fertig abgewickelt sind. Sie über spätere Berichtigungen zu informieren, würde zweifellos einen Verstoss gegen das DSG bedeuten. Diese Pflichten würden beispielsweise zur absurden Situation führen, dass ein Domizilwechsel einer Unternehmung allen Personen, über die je Daten bearbeitet wurden, aktiv diese Änderung mitteilen müssten. Da mit einer exzessiven Auslegung zuungunsten der Datenbearbeiter zu rechnen ist, ist die ersatzlose Streichung des Artikels gerechtfertigt.
vsi	VE-DSG	20	2	e	Streichen - in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich, z.B. im Online-Handel, etc. Vgl. auch den Antrag zu Art. 15 hiervor.
vsi	VE-DSG	20	2	f	Streichen: Die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntzugeben, oder sie tangiert schützenswerte Interessen Dritter. Die

					Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen. Hier sind die Argumente zu Art. 13 Abs. 3 und 4 ebenfalls zu berücksichtigen.
vsi	VE-DSG	20	3		Streichen, ev. Beschränkung auf die Pflicht, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt - ein Vertrag wird geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, Geschäftsgeheimnisse offenlegen zu müssen, die ansonsten ausdrücklich strafrechtlich geschützt sind. Wieso es erforderlich sein soll, dem Betroffenen die Auswirkungen zu erläutern, ist sodann völlig unerfindlich. In aller Regel wird er absolut in der Lage sein, diese selber einzuschätzen. Dieser Absatz steht auch in einem unheilbaren Widerspruch zu Art. 1 OR, wonach (mit Einschränkung durch Art.. 261bis StGB [Strafbewehrung bei Verweigerung einer für die Allgemeinheit bestimmten Leistung aufgrund von Rasse, Ethnie oder Religion] Abschlussfreiheit]) gilt. Das DSG darf nicht dazu herhalten, dass z.B. ein ehemaliger Mitarbeiter Anrecht hat, über die DSG-Pflicht Informationen über von ihm betreute Kunden erhalten darf. Es ist bereits notorisch bekannt, dass Bankkunden unter Verweis auf die DSG-Regelungen kostenlos zu verlorenen Kontoauszügen kommen.
vsi	VE-DSG	23	1		Die Persönlichkeit darf nur nicht "widerrechtlich" bei der Datenbearbeitung verletzt werden. In Abs. 2 werden sodann Persönlichkeitsverletzungen nicht abschliessend aufgeführt. Es ist wohl mitgemeint, dass diese stets auch widerrechtlich sind.
vsi	VE-DSG	23	2	d	Streichen. Zum Profiling vgl. auch die Bemerkungen zu Art. 3 lit. f VE.
vsi	VE-DSG	23	3		Abs. 3 gaukelt eine scheinbare Sicherheit vor. Was über Facebook verbreitet worden ist, kann auch dann nicht wieder aus der Welt geschafft werden, wenn der Betroffene Facebook die (weitere) Verbreitung untersagt, wobei dazu gegenüber Onlineplattformen ein klagbarer Anspruch besteht. Der Artikel kann belassen werden, wobei die Formulierung "in der Regel" auf jeden Fall zu streichen ist. Das DSG kann nicht die über siebzigjährige Tradition des StGB ("voluntibus non fit iniuria") aushebeln.
vsi	VE-DSG	24	2		Erster Satz: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtsunsicherheit. Das neue DSG wimmelt nachgerade von Vorschriften, die einseitig auf die Einschränkung der Datenbearbeitung und auf eine Kriminalisierung datenbearbeitender Unternehmen ausgerichtet sind.

vsi	VE-DSG	24	2	a	Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft einmal mehr nicht gelöste Abgrenzungsfragen auf.
vsi	VE-DSG	24	2	c	Ziff. 3: Streichen. Die Volljährigkeit (respektive die Handlungsfähigkeit) ist häufig weder bekannt noch zu eruieren, die Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft. Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit 100 %-iger Sicherheit bestimmbar, geschweige denn sein Alter. Im Übrigen würde es klar zum Schutz Minderjähriger beitragen, wenn zumindest ihr Alter gespeichert und die Information aufbewahrt werden dürfte!
vsi	VE-DSG	25	1	a - c	müsste spezifiziert werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. ansonsten kann die Bestimmung nicht umgesetzt werden. Die Unternehmen würden unter Umständen ihrer Möglichkeit beraubt, bspw. einen Schuldner auf dem Rechtsweg für nicht bezahlte Forderungen zu belangen.
vsi	VE-DSG	25	2		Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", ev. Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich um bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis krause Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat.
vsi	VE-DSG	25	3		Streichen. Art. 25 Abs. 1 lit. a bis c reichen völlig, um dem Betroffenen Genüge zu tun. Auch die DGSVO EU sieht keine Mitteilung von Urteilen an Dritte vor.
vsi	VE-DSG				Vorbemerkungen zum 6. Abschnitt: Die nachfolgenden Bestimmungen zeigen ein Dilemma: Der EDÖB ist heute faktisch dem Bundesrat unterstellt. Die gesamte Gesetzesrevision ist deshalb sehr verwaltungsfreundlich. Es ist fraglich, ob sie das auch wäre, wenn der EDÖB in faktischer und rechtlicher Hinsicht von der Bundesverwaltung unabhängig. Vorgängig ist deshalb die unabhängige Stellung des EDÖB ist grundsätzlich zu diskutieren. Die Wirtschaft begrüsste eine starke Unabhängigkeit des EDÖB und eine Gleichbehandlung wie die Verwaltung. Diese ist offensichtlich nicht gegeben.
vsi	VE-DSG	28	1 + 2		Entweder streichen, oder die entsprechenden Möglichkeiten auch Privaten eröffnen. Hier kommt einmal mehr das einseitig etatistische Denken zum Ausdruck, das dem ganzen Erlass zugrunde liegt. Abs. 1

					steht im Widerspruch Abs. 1 lit. a. Der Artikel ist undemokratisch, weil dem Bundesrat eine Kompetenz zugestanden wird, die dem Parlament zusteht.
vsi	VE-DSG	29	2	lit. e	Die Inkassobranche muss und will regelmässig die Forderungsansprüche (auch im Ausland) rechtlich durchsetzen. Die Glaubhaftmachung muss dann gelten, wenn eine vernünftige Zweifel über die Identität des Schuldners ausschliessende Dokumentation (z. B. Rechnung) vorliegt. In der Praxis weichen Behörden oft von diesem Grundsatz ab.
vsi	VE-DSG	37	1		Dem Bundesrat soll nur ein Vorschlagsrecht zukommen, die Wahl muss durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Dauer von 4 Jahren gewählt". Ein blosses Recht des Parlaments, den Gewählten abzunicken, ist als Augenwischerei zurückzuweisen. Der Artikel ist in völliger Analogie zur Wahl des Bundesanwalts, welcher vom Parlament gewählt wird, auszuformulieren.
vsi	VE-DSG	37	4		Das Budget muss durch das Parlament genehmigt werden. Der EDÖB muss in Bezug auf das Budget der ganzen Finanzgesetzgebung unterworfen werden.
vsi	VE-DSG	37	5		Es ist nicht einsichtig, weshalb Art. 4 Abs. 3 BPG nicht gelten soll: Auch der Beauftragte soll für die Verhinderung von Willkür im Arbeitsverhältnis sorgen und seine Mitarbeitenden soll, weshalb der Absatz 5 zu streichen ist.
vsi	VE-DSG	38	2		Die automatische Wiederwahl ist zu streichen. Ein solches Institut existiert bei keiner anderen magistralen Position. Der gesamte Art. 38 atmet den Geist des alten Beamtengesetzes und ist einer modernen Gesetzgebung unzugänglich. Die Tatsache, dass auch hier der Bundesrat faktisch Wahlbehörde ist gefährdet die Unabhängigkeit des EDÖB in europarechtlich widriger Weise.
vsi	VE-DSG	39	2		Jede Nebenbeschäftigung muss offengelegt werden. Hier ist absolute Transparenz unabdingbar.
vsi	VE-DSG	41	1		Es muss ein begründeter Anfangsverdacht bestehen, ansonsten soll der Beauftragte weder von Amtes wegen noch auf Anzeige hin eine Untersuchung eröffnen dürfen.
vsi	VE-DSG	41	4		Streichen. Ein Tätigwerden des Beauftragten gegenüber Privaten ohne konkrete Hinweise auf eine Datenschutzverletzung ist strikte abzulehnen. Die Kosten solcher amtlicher Initiativen werden in der Praxis regelmässig den Privaten überbunden. Daher muss gelten: Keine "Überprüfung" ohne konkreten Anlass!" In

					welcher Form und ob überhaupt eine Beratungsdienstleistung des Beauftragten angefordert wird. erschliesst sich nicht.
vsi	VE-DSG	42			Streichen. Vorsorgliche Massnahmen sind - auch im Persönlichkeitsschutz - Sache der Gerichte. Hier soll einer Einzelperson, die nicht einmal Jurist sein muss, ohne Not eine völlige "carte blanche" erteilt werden! Dies ist rechtsstaatlich unhaltbar.
vsi	VE-DSG	43	1		Streichen. Der Beauftragte erhält hier Befugnisse zum Erlass hoheitlicher Verfügungen, die teilweise nicht wieder gutzumachende Folgen zeitigen (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 42 reicht zum Schutz Betroffener völlig aus. Keine Verfügungsbefugnisse für den Beauftragten, Verfügungen dürfen nur über ein anerkanntes staatliches Gericht erfolgen.
vsi	VE-DSG	44	3		: Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Wenn schon, wäre vorzusehen, dass die aufschiebende Wirkung auf **Antrag** durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt unsinnige Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
vsi	VE-DSG	45			Streichen. Ein *Recht* zur Anzeige wäre sachgerechter. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE). Der Beauftragte müsste **alle** Straftaten, also nicht nur jene nach dem DSG zur Anzeige bringen, auch wenn sie nichts mit dem vorliegenden Gesetz zu tun haben.
vsi	VE-DSG	46	2		Siehe Anmerkung zu Art. 45.
vsi	VE-DSG	47			Es ist einem ausländischen Staat in Analogie zu Art. 5 Abs. 2 VE-DSG nur dann Amtshilfe zu gewähren, wenn dieser mindestens gleichwertige Datenschutzgesetze kennt.
vsi	VE-DSG	49		b	Streichen. Es besteht die Gefahr, dass der Beauftragte zum verlängerten Arm ausländischer Behörden wird. Dies Gefahr besteht bereits mit Art. 47 Abs. 2.

vsi	VE-DSG	49		c + d	Wie soll eine "Sensibilisierung" der Bevölkerung, insbesondere der "schutzbedürftigen" Personen gestaltet sein? Es ist nicht einsichtig, weshalb allenfalls Steuergelder dafür aufzuwenden sind. Nach dem Legalitätsprinzip ist zu definieren, wer als "schutzbedürftige Person" gilt?
vsi	VE-DSG	50ff.			Vorbemerkungen: Die Strafbestimmungen sind vom Zeitgeist geprägt, der jedes angeblich "unwerte" Verhalten sofort in eine strafrechtliche Norm gegossen sehen will. Es ist dem vorherigen Autor beizupflichten, dass die Strafnormen jegliches Augenmass vermissen lässt. Die Straftatbestände sind ins Strafgesetzbuch zu verlagern und die entsprechenden Bestimmungen nochmals grundlegend zu überarbeiten. Der vorgesehene Strafrahmen ist völlig überrissen und nachgerade als zu horrend bezeichnen. Dies gilt sowohl für vorsätzliche als auch - erst recht - für fahrlässige Verstösse. Es wird **beantragt**, bei Fahrlässigkeit von einer strafrechtlichen Sanktionierung abzusehen, eventuell den Bussenrahmen auf eine maximale Höhe von CHF 5'000.00 bzw. - im Wiederholungsfall - CHF 10'000.00 zu begrenzen. Bei den Unternehmensbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen hergestellt werden, wie dies in der DSVGO EU ausdrücklich vorgesehen ist (Art. 83 Abs. 2 lit. geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen; die Umsatzrendite beträgt bei hiesigen KMU häufig weniger als 5 %). Die Strafbestimmungen stellen ein weiteres Beispiel dar, wie sehr der Politik das Augenmass abhandengekommen ist. Offenbar hat sich inzwischen der Glaube durchgesetzt, dass ein Gesetz nur dann von Gutem sein kann, wenn es Strafdrohungen im Phantasiebereich enthält und möglichst viele Akteure kriminalisiert. Theoretisch genügt EIN Betroffener, der sich falsch behandelt fühlt, um einen Datenbearbeiter als Kriminellen abzustempeln und wirtschaftlich in den Ruin zu treiben. Im "gewöhnlichen" Strafrecht beträgt die maximale Busse für eine Übertretung CHF 10'000.00 (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Rahmen. Die Erhöhung des Strafrahmens auf CHF 500‘000.00 ist absolut überrissen. Beispielsweise sieht das kantonalbernische Verwaltungsrecht im Baurecht bei schweren (!) Verstössen Höchstbussen von CHF 100'000.00 vor (Art. 50 Abs. 3). Gemäss Art. 14ff. VStrR können bei Leistungs- und Abgabebetrug, Urkundenfälschung und Erschleichung einer Falschbeurkundung sowie Begünstigung Höchstbussen von CHF 30'000.00 festgelegt werden. Gemäss DBG können bei Verstössen wie Mithilfe bei der Steuerhinterziehung Bussen von 10‘000.00 bis max. CHF 50‘000.00 (in schweren Fällen oder bei Wiederholungsfall) gesprochen werden. Bei Steuerbetrug beträgt die Busse max. 30‘000.00. Bei Verstössen gegen das DSG handelt es sich mi Ausnahme von Art. 52 VE - der eine Freiheitsstrafe als Höchststrafe vorsieht - nicht um Vergehen oder Verbrechen, sondern um Übertretungen. Es existiert kein

					nachvollziehbarer Grund den für vergleichbare Verstösse übliche Bussenrahmen im DSG, um das Zehnfache oder mehr zu überschreiten. Eine Persönlichkeitsverletzung, die dies rechtfertigen würde, ist nicht vorstellbar. Eine solche Pönalisierung von DSG-Verstössen kommt einer schweren Kriminalisierung der Fehlbaren gleich und ist komplett unverhältnismässig. U.a. übersteigt der im VE DSG gesteckte Rahmen auch Schmerzensgelder bei weitem, die nach hiesiger Rechtsprechung bei Körperschäden zugesprochen werden. Als Vergleich noch einige Beispiele aus der deutschen Rechtsprechung für die Bemessung von Schmerzensgeld wegen Persönlichkeitsverletzung (Mobbing und ähnliches): - Mobbing durch nicht gerechtfertigte Aufgabenentziehung durch den Arbeitgeber, Schikanieren und Degradierung des Arbeitnehmers: 53.000 Euro (ArbG Leipzig, 2012) - vielfältige persönliche Herabsetzung des Arbeitnehmers, rund € 26.500, ArbG Ludwigshafen am Rhein, 2000 - Beleidigungen, Auftragsentziehung, Verbot des Kundenkontakts, Gehaltskürzung durch den Arbeitgeber, € 24.000 , LAG Hannover, 2005 - systematische Persönlichkeitsverletzungen des Arbeitnehmers in 34 Fällen über 1 Jahr, € 17.500, ArbG Eisenach, 2005 - schikanöse und entwürdigende Handlungen, € 7.000, ArbG Siegburg, 2012 - Demütigung wegen der ethnischen Herkunft durch ein Rap-Video bei YouTube, € 5.000, LG Bonn, 2013 - Cybermobbing via Facebook mit Unterstellung der Homosexualität und Pädophilie, € 1.500, LG Memmingen, 2015 Quelle: http://www.schmerzensgeldtabelle.net/mobbing/#tabelle
vsi	VE-DSG	50	2		Bei Art. 50 Abs. 2 ist zu beachten, dass es sich offensichtlich um ein Offizialdelikt handelt, das von Amtes wegen verfolgt wird.
vsi	VE-DSG	50	4		Ist zu streichen.
vsi	VE-DSG	51	2		Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen. Vorsatzstrafen: S. Bemerkungen zu Art. 50.
vsi	VE-DSG	52			Streichen. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht (vgl. Art. 321 StGB) sind völlig ausreichend. Unklar, wer hier neu zum Träger eines Berufsgeheimnisses gemacht werden soll, ebenso unklar, was "geheime Personendaten" im vorliegenden Zusammenhang genau bedeuten würde.

					Wenn schon die blosse kommerzielle Bearbeitung von Daten als Aufhänger für die Strafdrohung genügen soll, würde wohl nahezu jeder Datenbearbeiter zum Träger einer strafbewehrten Schweigepflicht gemacht. Es ist nicht einsichtig, weshalb hier plötzliche von "geheimen" Daten die Rede ist, während sonst von "besonders schützenswerten" Daten die Regel ist. Es ist dem vorherigen Autor zuzustimmen, dass das StGB respektive in anderen Gesetzen aufgeführte strafbewehrte Geheimhaltungspflichten ausreichen. Vgl. dazu auch BSK StGB Niklaus Oberholzer N13 zu Art. 321 StGB: "…Andererseits genügt aber nicht bereits jede Offenbarung eines Geheimnisses, sondern nur die **unbefugte Bekanntgabe besonders schützenswerter Personendaten** (Hervorhebung durch d. V.).
vsi	VE-DSG	53			Die Frage stellt sich, weshalb es einer Unternehmung nur bis 100 000 Franken möglich sein soll, eine Strafe zu übernehmen. Nach dem jetzigen Text würde die Übernahme einer Busse > 100 000 Franken durch den Geschäftsbetrieb (typischerweise in der Regel der Arbeitgeber) wohl eine Begünstigung im Sinne von Art. 305 Abs. 1 StGB darstellen.
vsi	VE-DSG	55			Reduktion der Verjährungsfrist auf 3 Jahre. Dies entspricht Art. 109 StGB und wäre völlig ausreichend und sachgerecht.
vsi	VE-DSG	56			**Titel fehlt!** Die Genehmigung des Parlamentes ist zwingend einzuholen.
vsi	VE-DSG	59			Die Übergangsbestimmungen sind ziemlich mager, für alle ausserhalb Art. 16, 18 und 19 VE-DSG stehenden Normen ist keine Übergangsfrist vorgesehen.
vsi	VE-DSG				**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Wo das Gesetz in Abweichung von den normalen Regeln von der Erhebung von Gerichtskosten absieht, geht es üblicherweise um Vertragsstreitigkeiten (Miete, Arbeitsvertrag, auch Gleichstellungsfragen pflegen sich jeweils im Zusammenhang mit einem Arbeitsverhältnis zu stellen). Wegleitend ist dabei die Annahme des Gesetzgebers, dass eine Partei besonders geschützt werden muss, weil sie in einem Abhängigkeitsverhältnis zur anderen steht. Im Datenschutzbereich werden oft keinerlei vertragliche oder persönliche Beziehungen zwischen Datenbearbeiter und Betroffenem bestehen. In dieser Konstellation ist nachgerade mit einer Flut von - durchaus auch mutwilligen - Klagen zu rechnen, wenn das Prozessieren gratis ist. Es besteht kein Anlass, die üblichen, zivilprozessualen Regeln hier zu ändern. Einem bedürftigen Kläger

					steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll - wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist - seine Kostenrisiken abwägen müssen. Der vsi spricht sich auch dagegen aus, alle Streitigkeiten ins vereinfachte Verfahren zu weisen. Dies beschränkt die beklagte Partei wesentlich in ihren Verfahrensrechten.
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht	

gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")		
Name/Firma	**Kapitel-Nr.**	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"		
Name/Firma	**Art.**	**Bemerkung/Anregung**
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Eidgenössisches Justizdepartement
EJPD
Herr Jonas Amstutz
Bundeshaus West
CH-3003 Bern

jonas.amstutz@bj.admin.ch

Datum 4. April 2017
Kontaktperson Lukas Aebi
Direktwahl 061 206 66 26
E-Mail l.aebi@vskb.ch

Stellungnahme der Kantonalbanken zur Revision des Datenschutzgesetzes

Sehr geehrte Damen und Herren

Sehr geehrter Herr Amstutz

Am 21. Dezember 2016 hat der Bundesrat die Vernehmlassung zur Revision des Datenschutzgesetzes eröffnet. Wir bedanken uns für die Gelegenheit, unsere Position und Überlegungen zum Revisionsentwurf im Rahmen des Vernehmlassungsprozesses einbringen zu können.

Zusammenfassung

Eine moderne, international kompatible und auf bewährten schweizerischen Regulierungsgrundsätzen aufbauende Datenschutzgesetzgebung ist im Sinne des Finanzplatzes Schweiz und der Kantonalbanken. Wir begrüssen daher das Revisionsvorhaben im Grundsatz. Dabei ist jedoch zentral, dass unverhältnismässige Belastungen für die Rechtsunterworfenen, die in keinem Verhältnis zum Schutzzweck des Gesetzes stehen, unbedingt vermieden werden.

Mit Blick auf den vorliegenden Revisionsentwurf besteht diesbezüglich noch viel Anpassungsbedarf. Die folgenden Kernanliegen, die in unserer Stellungnahme noch eingehender ausgeführt werden, sind für die Kantonalbanken von zentraler Bedeutung:

- Der Vorentwurf zum Datenschutzgesetz sollte sich an der revidierten Konvention 108 des Europarats und der Datenschutzgrundverordnung der Europäischen Union orientieren. Ein darüber hinaus gehender **«Swiss Finish» ist unnötig und schädlich** für den Wirtschaftsstandort Schweiz. So ist beispielsweise die Definition des sogenannten **«Profiling»** wesentlich breiter gefasst als die analoge Definition im Europäischen Recht. Dies ist nicht zielführend für eine Vereinheitlichung des Datenraumes in Europa und widerspricht damit der eigentlichen Absicht der Revision. Es gibt zahlreiche weitere Beispiele für unnötige und kontraproduktive Swiss finishes (vgl. dazu im Detail die nachfolgende Stellungnahme).
- Die zahlreichen verschärften und zusätzlichen Begründungs-, Anhörungs- und Informationspflichten führen für Unternehmen zu einer Flut von Meldungen an den Datenschutzbeauftragten und damit zu einem enormen, unverhältnismässigen und unnötigen Aufwand. Dies wirkt sich zudem wettbewerbs- und innovationsbehindernd aus.
- Sehr problematisch und **dezidiert abzulehnen sind die in Art. 50 ff. VE-DSG enthaltenen Strafbestimmungen**. **Diese setzen die Mitarbeiter von Bankinstituten einem enormen Haftungsrisiko bei der Datenbearbeitung aus.** Aus rechtsstaatlicher Sicht ebenso bedenklich sind die sehr offen formulierten Tatbestände, die einer Abkehr von den bewährten Grundsätzen der schweizerischen Strafrechtsdogmatik gleichkommen («nulla poena sine lege»). Auf die Strafbestimmungen ist daher zu verzichten, stattdessen sollten **angemessene verwaltungsrechtliche Sanktionskompetenzen** etabliert werden.
- Es gilt zu bedenken, dass Art. 19 des Bundesgesetzes über den internationalen automatischen Informationsaustausch in Steuersachen (AIAG) den meldepflichtigen Personen die Rechte nach DSG einräumt. Wenn nun im Rahmen der Datenschutzgesetzrevision die juristischen Personen explizit ausgenommen werden, stellt sich berechtigterweise die Frage**, ob damit juristische Personen nicht ihrer prozessualen Rechte beraubt werden.** Dies sehen wir kritisch.

- Der VSKB fordert ausserdem Mechanismen zur Verhinderung des Missbrauchs des Auskunftsrechts. **Im Sinne eines wirksamen Datenschutzes ist dieses so auszugestalten, dass es einzig zur Verfolgung von Datenschutzinteressen und nicht zur Beweismittelbeschaffung in Zivil- und Strafverfahren verwendet werden kann.** Es ist unserer Ansicht nach zudem falsch, das Auskunftsrecht kostenlos auszugestalten.
- Bei den angedachten Grundsätzen zur Bearbeitung von Personendaten ist darauf zu achten, **dass zentrale Bestimmungen des Geldwäschereigesetzes**, die eine Bank etwa dazu verpflichten, Informationen des Kunden und auffällige Transaktionen genau zu dokumentieren und aufzubewahren, **nicht unterlaufen werden**.

In der folgenden tabellarischen Übersicht sind unsere detaillierten Bemerkungen und Anliegen festgehalten:

Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Detaillierte Bemerkungen zum Vorentwurf Datenschutzgesetz (VE-DSG)

Gesetz	Art.	Abs.	Bst.	Bemerkungen
DSG				**Vorbemerkung I:** Die Totalrevision des DSG sollte zwei Ziele verfolgen: • Anpassung an die revidierte Konvention 108 des Europarats (ERK 108) und • Beibehaltung der Anerkennung durch EU-Kommission, dass die Schweiz über einen angemessenen Datenschutz (Angemessenheitserklärung) verfügt. Letztere verlangt keine pauschale Übernahme der europäischen Datenschutz-Grundverordnung (EU-DSGVO). Für die Angemessenheitserklärung genügt es, grundlegende Garantien einzuhalten, beispielsweise die Rechtsstaatlichkeit oder die Existenz unabhängiger Aufsichtsbehörden. Die EU-DSGVO hält deshalb ausdrücklich fest, dass die Umsetzung der ERK 108 bei der Angemessenheitsbeurteilung ein wesentlicher Faktor ist. Illustriert wird dies dadurch, dass aus Sicht der EU-Kommission die Einhaltung der wenigen Regeln des US-EU Privacy Shields bekanntlich genügt, um einen angemessenen Datenschutz sicherzustellen. Vor diesem Hintergrund muss sich der **VE-DSG primär an der ERK 108 orientieren**. Darüber hinausgehende Regelungen können nur insofern sinnvoll sein, als sie helfen, einen einheitlichen Standard nach Massgabe der EU-DSGVO zu fördern. Damit wären Implementierungs- sowie Unterhaltskosten für

				Unternehmen, die in den Geltungsbereich beider Rechtsgrundlagen fallen und sämtliche Regelungen umsetzen müssen, auf ein verkraftbares Ausmass beschränkt. Dagegen wäre eine Verschärfung gegenüber der ERK 108 und der EU-DSGVO konzeptionell falsch, nicht notwendig und überdies **kontraproduktiv**, weil ein solcher **«Swiss Finish»** einen einheitlichen internationalen «Datenraum» zu Lasten der Schweiz verhindern und zulasten Schweizerischer Unternehmen wettbewerbsverzerrend wirken würde. Ein «Swiss Finish» kann daher zum Vornherein höchstens nur punktuell in Frage kommen, wo er eine wesentliche Erleichterung mit sich bringt.
DSG				**Vorbemerkung II:** Wir begrüssen, dass unter dem VE-DSG **Unternehmen keinen Datenschutz** mehr beanspruchen können. Damit wird Gleichlauf und somit Äquivalenz mit der EU-DSGVO hergestellt. Zu berücksichtigen ist allerdings die Tatsache, dass Unternehmen als rechtliche Fiktionen naturgemäss **zwingend durch natürliche Personen handeln** müssen. Bei jeder Datenbearbeitung durch Unternehmen entstehen deshalb per definitionem auch Daten von Mitarbeitenden des betreffenden Unternehmens, z.B. als Verfasser eines im Namen der Unternehmung erstellten Dokuments. Sämtliche solcher Daten von Mitarbeitenden dem Datenschutz zu unterstellen, wäre sachlogisch falsch und ein Widerspruch zur Tatsache, dass Unternehmen keinen Datenschutz mehr geniessen sollen. Deshalb ist **im Gesetz eine klare Abgrenzung** vorzunehmen. Diese muss statuieren, dass sämtliche Daten, welche über Mitarbeitende bei Ausübung oder bei Gelegenheit der geschäftlichen Tätigkeit für das Unternehmen entstehen, dem VE-DSG nicht unterstehen (vgl. Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 12 DSG N 24). Dementsprechend ist auch der künftig nicht mehr nötige Verweis in Art. 328b OR auf das DSG im gleichen Sinn anzupassen bzw. einzuschränken. Es gilt allerdings zu bedenken, dass Art. 19 des Bundesgesetzes über den internationalen automatischen Informationsaustausch in Steuersachen (AIAG) in Art. 19 den meldepflichtigen Personen die Rechte nach DSG einräumt. Wenn nun im Rahmen der Datenschutzgesetzesrevision juristische Personen explizit ausgenommen werden, stellt sich berechtigterweise die Frage, ob damit juristischen Personen nicht das Beschreiten des Rechtsweges im Rahmen des internationalen automatischen Informationsaustausches verwehrt wird. Aus Gründen der Adäquanz mit den europäischen Datenschutzregelungen ist die beste Lösung, nicht den Datenschutz wieder auf Unternehmen auszudehnen, sondern unter AIA Rechtsschutzmechanismen für Unternehmen ausserhalb des Datenschutzgesetzes zu etablieren.

DSG				**Vorbemerkung III:** Der VE-DSG sieht **zahlreiche verschärfte Prüf- und Meldepflichten** für Datenbearbeiter vor, die überdies einen erheblichen Eingriff in die Vertragsfreiheit bedeuten. Zu nennen sind insbesondere die Prüfung der Richtigkeit der Daten (Art. 4 Abs. 5 VE-DSG), die Meldepflichten bei Weitergabe von Daten ins Ausland (Art. 5 Abs. 3 Bst. c u. d i.V.m. Abs. 5 VE-DSG u. Art. 6 Abs. 2 i.V.m. Art. 6 Abs. 1 Bst. b-d VE-DSG), Informationspflichten, sofern Daten über einen Dritten beschafft werden (Art. 13 Abs. 5 VE-DSG), die Datenschutz-Folgeabschätzungen samt Meldepflicht (Art. 16 VE-DSG), umgehende Meldepflicht sämtlicher Datenschutzverletzungen (Art. 17 VE-DSG), Dokumentationspflichten (Art. 19a VE-DSG) und Pflicht zum Monitoring samt engem Zeitraum für allfällige Berichtigungen (Art. 19b VE-DSG). Das Gesamtpaket dieser Pflichten möge für spezifische Marketing-Dienstleister und Data-Miner angemessen sein, da sie im Rahmen eines eng begrenzten Geschäftsmodells typischerweise besonders sensible Datenbearbeitungen vornehmen. Für Datenbearbeiter, welche wie z.B. Banken ständig und in enormem Volumen Daten in Zusammenhang mit der Ausführung von Kundenaufträgen und aufgrund regulatorischer Vorgaben an zahllose Empfänger weitergeben müssen, ist die pauschale Anwendung solch strenger Regeln unbesehen der Sensibilität der betroffenen Daten nicht sachgerecht. Sie führen nicht zu besserem Datenschutz, sondern lediglich zu **enormem unnötigem Aufwand** und zu einer Flut von Meldungen an den Eidgenössischen Datenschutzbeauftragten (EDÖB). Ein derart intensives Paket von Pflichten ist umso bedenklicher, als es überdies auch noch weitgehenden strafrechtlichen Sanktionen unterstehen soll, welche erst noch entgegen etablierten Strafrechtsgrundsätzen sehr offen formuliert sind (vgl. Art. 50 ff. VE-DSG). Pflichten dieser Art sind deshalb nochmals in grundsätzlicher Form im Sinne einer Liberalisierung mit konsequentem Fokus auf die spezifischen **Bedürfnisse verschiedener Branchen** wie z.B. der Banken zu überarbeiten, damit die Wirtschaft nicht am Datenschutz «erstickt». Das neue DSG durchbricht gemäss VE ausserdem rechtsstaatliche Grundsätze, indem die gleiche Behörde Recht setzen und sprechen kann. Schliesslich enthält das Gesetz einige Auflagen, die in der Praxis nicht umsetzbar sind, was von einer mangelnden Prüfung auf die Umsetzbarkeit des Gesetzes zeugt.
DSG	1			**Kernanliegen: Berücksichtigung gesamtwirtschaftlicher sowie gesellschaftlicher Interessen bei der Bearbeitung von Personendaten**

				Die Bearbeitung von Personendaten ist Bestandteil und Voraussetzung nicht nur der erfolgreichen Digitalisierung der schweizerischen Wirtschaft und Gesellschaft, sondern überhaupt jeder wirtschaftlichen Tätigkeit. Infolgedessen muss das neue DSG bei der Bearbeitung von Personendaten auch gesamtwirtschaftliche und gesellschaftliche Interessen berücksichtigen. Dies würde auch der Zielsetzung der EU-DSGVO (Art. 1 Gegenstand und Zweck) entsprechen. Diese sieht neben dem Schutz natürlicher Personen auch den freien Verkehr von Personendaten als Zweck ausdrücklich vor. Zudem stünde die Berücksichtigung gesamtwirtschaftlicher sowie gesellschaftlicher Interessen im Einklang mit der Strategie des Bundesrates für eine digitale Schweiz. Demnach soll die Schweiz «Chancen der Digitalisierung in allen Lebensbereichen konsequent nutzen», von der „zunehmenden Digitalisierung profitieren», sich «als innovative Volkswirtschaft noch dynamischer entwickeln» und die «Wirtschaft soll sich im digitalen Raum möglichst frei entfalten können» (vgl. Medienmitteilung vom 20.04.2016 zur Strategie des Bundesrates für eine digitale Schweiz). Wir schlagen daher folgende Anpassung von Art. 1 VE-DSG (Zweck) vor: *Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden, und die Förderung des freien Verkehrs von Personendaten*
DSG	2	2	e	Zur Eindämmung des Missbrauchs und um die verfahrensrechtlichen Regeln gemäss den einschlägigen Verfahrensordnungen wie z.B. der ZPO nicht zu verwässern, fordern wir die **Wiedereinführung der Regel von Art. 2 Abs. 2 Bst. c DSG** mit Bezug auf sämtliche Zivil- und Strafverfahren (Nichtanwendbarkeit des DSG auf hängige Prozesse und anderer Verfahren) (vgl. im Einzelnen hinten zu Art. 20 Abs. 1 VE-DSG). Wäre dies nicht der Fall, so könnten über das DSG Daten beschafft werden, die im Rahmen der prozessualen Editionspflicht nicht herausgegeben werden müssten.
DSG	2	3		Es ist nicht einsehbar, weshalb die wichtige und richtige Regel von Art. 2 Abs. 3 VE-DSG nur für bundesrechtliche Verfahren gelten soll. In hängigen Verfahren müssen insbesondere auch kantonale (Vor-) Instanzen gleichermassen rechtlich geschützt sein.
DSG	3		a	Definition der Personendaten: Nach heutiger Definition umfassen Personendaten alles, was irgendwie auf eine Person schliessen lässt. Im Rahmen des Bankgeschäfts sind somit sämtliche Belege, jeder Ausweis, jede Adressmutation etc. als Personendaten zu qualifizieren. Es ist zu beachten, dass die

				Pflichten zur Datenbearbeitung (beispielsweise Information bei Beschaffung oder Vernichtung von Daten) massiv ausgeweitet wurden. Mit der hier gewählten Definition ist es Banken unmöglich, den Pflichten dieses Gesetzes nachzukommen. Entsprechend wäre in der Definition zu unterscheiden, ob es sich um Personendaten grundsätzlicher Art handelt oder nicht. Eine Präzisierung der Begrifflichkeiten ist anzustreben. Wünschenswert wäre eine Unterscheidung, ob es sich um Personendaten grundsätzlicher Art handelt oder nicht.
DSG	3		c Ziff. 4	Die besonders schützenswerten biometrischen Daten sollten dahingehend präzisiert (eingeschränkt) werden, dass «zum Zweck» der Identifizierung ergänzt wird.
DSG	3		f	**Kernanliegen: Streichung des gegenüber der EU-DSGVO überschiessenden Swiss Finish und Beschränkung auf Personendaten sowie automatisierte Bearbeitung** Die Definition von «Profiling» ist zu breit und geht massiv weiter als die Definition gemäss der EU-DSGVO. Bereits eine «von Hand» bearbeitete Mitarbeiterbeurteilung würde als «Profiling» nach Art. 23 Abs. 2 Bst. d VE DSG und damit per se als Persönlichkeitsverletzung gelten. Konsequenterweise müsste ein Bearbeiter vor jeder Bearbeitung einen Rechtfertigungsgrund ausweisen können, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden wäre. Dies stellt einen partiellen Paradigmenwechsel im schweizerischen Datenschutzrecht dar, für den es keinen Grund gibt. Zudem umfasst «Profiling» gemäss VE-DSG auch das Bearbeiten von **nicht-personenbezogenen Daten**, was eine unzulässige Ausweitung des Geltungsbereichs des DSG darstellen und im Widerspruch zu Art. 2 Abs. 1 VE-DSG stehen würde. Richtigerweise darf «Profiling» nur diejenigen Daten erfassen, welche tatsächlich Rückschlüsse auf konkrete Personen zulassen, mithin nur Personendaten. Schliesslich ist eine Analyse bzw. Auswertung noch keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte der betroffenen Personen auswirkt. Richtigerweise ist der Begriff «Auswertung» durch «Bewertung» zu ersetzen, denn erst diese stellt einen schützenswerten Eingriff in die Persönlichkeitsrechte der betroffenen Personen dar. «Bewertung» umfasst eine Entscheidung mit Bezug auf eine einzelne betroffene Person, die sich auf eine Analyse bzw. Auswertung stützt. Die Anknüpfung an die Auswertung greift demnach zu weit. Art. 3 Bst. f ist deshalb wie folgt zu ändern (Ergänzungen unterstrichen):

				Profiling: automatisierte ~~jede Auswertung~~ Bewertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität Der generelle Einbezug von Datenauswertungen im Zusammenhang der Voraussage von Entwicklungen auch mit der wirtschaftlichen Lage ist aus Banksicht heikel.
DSG	4	3		**Kernanliegen: Keine Verschärfung der bewährten aktuellen Regelung** Gemäss Erläuterungsbericht soll die Regelung des Grundsatzes von Treu und Glauben gemäss Art. 4 VE-DSG materiell keine Änderungen gegenüber der aktuellen Fassung gemäss Art. 4 DSG enthalten (vgl. Erläuterungsbericht, S. 45 f.). Entgegen dieser Aussage wird nun aber in Abs. 3 der Grundsatz der «Erkennbarkeit» mit dem Zusatz «klarer» Erkennbarkeit verschärft. Der Hinweis auf terminologische Anpassung an die EU-DSGVO (vgl. Erläuterungsbericht, S. 46) ist schon deshalb verfehlt, weil die EU-DSGVO einem grundsätzlich anderen Grundkonzept als das Schweizer DSG folgt. Das Schweizerische DSG fusst auf dem bewährten Fundament der – aus dem Grundsatz von Treu und Glauben abgeleiteten – Erkennbarkeit der Datenbearbeitung im Rahmen einer klaren Zweckbindung. Ausnahmen stellen Persönlichkeitsverletzungen dar, ausser es werden überzeugende Rechtfertigungsgründe geltend gemacht, welche in einer Interessenabwägung obsiegen, und mittels angemessener Information der betroffenen Person mitgeteilt (vgl. Rosenthal/Jöhri, a.a.O., Art. 4 DSG N 2 ff.). Das zusätzliche Adjektiv «klar» macht die Regel keineswegs klarer, sondern im Gegenteil auslegungsbedürftiger und produziert damit gegenüber der bestehenden bewährten Fassung von Art. 4 Abs. 3 DSG unnötigerweise Rechts*un*sicherheit. Der Begriff «klar» ist deshalb ersatzlos zu streichen.
DSG	4	5		**Kernanliegen: Keine Verschärfung der bewährten aktuellen Regelung** Entgegen dem Erläuterungsbericht (S. 47) erfolgt nicht nur die Übernahme der bewährten Grundsätze gemäss bestehendem Art. 5 DSG. Vielmehr führt die gewählte Formulierung von Art. 4 Abs. 5 VE-DSG zu einer unnötigen **Verschärfung des Pflichtenhefts**. Die vorgeschlagenen Regeln sind überschiessend. Statt der Pflicht zur Überprüfung der Richtigkeit der Daten würde z.B. die Pflicht genügen, geeignete Massnahmen zu ergreifen, um die Richtigkeit der Daten sicherzustellen. Teilweise entstehen aus den überschiessenden Pflichten auch unnötige Rechts*un*sicherheit und Abgrenzungsprobleme zu anderweitigen bestehenden gesetzlichen Regeln. Beispielsweise wird ein allgemeiner Löschungsanspruch

				statuiert, welcher im Einzelfall mit anderweitigen gesetzlichen Dokumentations- und Aufbewahrungspflichten kollidieren kann. Die Formulierung von Art. 5 DSG ist wesentlich besser gelungen, weshalb diese Regelung als neue Formulierung von Art. 4 Abs. 5 VE-DSG zu übernehmen ist. Sollte wider Erwarten gleichwohl am neuen Vorschlag gemäss VE-DSG festgehalten werden, müsste zumindest der Satzteil «und wenn nötig nachgeführt wurde» gestrichen werden, da diese Aussage unklar und überflüssig ist. Zudem ist in den **Erläuterungen** klarzustellen, dass **keine Vernichtungspflicht** besteht, soweit gesetzliche oder regulatorische (aufsichtsrechtliche) Aufbewahrungspflichten dem entgegenstehen. Dies betrifft z.B. die Bestimmungen des Geldwäschereigesetzes, die eine Bank verpflichten, alle Informationen aufzubewahren, die mit der Information des Kunden oder mit aussergewöhnlichen Transaktionen zusammenhängen. Es gilt hier ganz grundsätzlich zu bedenken, dass eine Bank mit den hier angedachten auferlegten Pflichten im Tagesgeschäft rasch an ihre Grenzen stösst. Es ist einer Bank nur sehr schwer möglich, ein eingereichtes Ausweisdokument und die darauf verzeichneten Daten auf ihre Echtheit zu überprüfen.
DSG	4	6		**Kernanliegen: Keine Verschärfung durch strengere Formvorschriften** Wie unter Abs. 3 wurde auch unter Abs. 6 eine unnötige vermeintliche Präzisierung eingefügt, indem die ausdrückliche Einwilligung nicht nur nach angemessener Information freiwillig, sondern neu zusätzlich «eindeutig» sein soll. Diese Neuformulierung ist verunglückt, da sie entgegen der Absicht gemäss Erläuterungsbericht (S. 45 ff.) eine Verschärfung und damit verbunden Rechts*un*sicherheit beinhaltet. Unklar bleibt insbesondere, ob das im Massengeschäft und insbesondere beim elektronischen Auftritt unumgängliche Abstellen auf Allgemeine Geschäftsbedingungen (AGB) weiterhin zulässig sein soll. Diese Frage muss klar mit ja beantwortet werden. Im Erläuterungsbericht (S. 47) wird zu Unrecht gefordert, dass die betroffene Person nicht gänzlich untätig bleiben darf, damit von einer «Einwilligung» ausgegangen werden kann. Mit dieser Auslegung wird de facto eine Formvorschrift aufgestellt, welche zahlreiche aus dem modernen Geschäftsleben nicht mehr wegzudenkende und datenschutzrechtlich unproblematische Anwendungen, welchen z.B. Regelungen in AGB zugrunde liegen, künftig verunmöglichen würde. Richtigerweise ist auf den Zweck der Datenbearbeitung abzustellen (Art. 4 Abs. 3 DSG). Soweit dieser für die betroffene Person erkennbar ist, muss die Einwilligung formunabhängig erfolgen

				können. Die bestehende Fassung von Art. 4 Abs. 5 DSG ist klarer und in sich stimmiger formuliert. Demzufolge sollte diese Fassung auch in Art. 4 Abs. 6 VE-DSG übernommen werden. Im Eventualfall ist aus systematischen Gründen zumindest das Profiling aus der Regelung zu entfernen. Der Umgang mit Profiling ist anderweitig im VE-DSG bereits detailliert geregelt (bzw. gemäss nachfolgenden Anträgen zu regeln), insb. in Art. 3 Bst. f. und in Art. 15 VE-DSG. Die zusätzliche Regelung auch in Art. 4 Abs. 6 VE-DSG produziert unnötige Doppelspurigkeiten mit der Folge von Abgrenzungsproblemen und Rechts*un*sicherheiten, und dies alles bei Themen, welche sogar unter Strafe gestellt sind (Art. 50 ff. VE-DSG).
DSG	5			**Kernanliegen: Informations- und Genehmigungspflichten setzen komplizierte sowie ressourcenintensive, interne Prozesse voraus und sind zu streichen, eventuell auf höchstens vier Wochen zu reduzieren**
DSG	5	1		Art. 5 Abs. 1 wiederholt lediglich einen anderweitig – u.a. in Art. 4 Abs. 1 VE-DSG – bereits statuierten Grundsatz und ist im Kontext von Art. 5 VE-DSG verwirrend, überflüssig und bietet der betroffenen Person keinen Mehrwert. Die konkrete anwendbare Regelung ergibt sich abschliessend aus den folgenden Absätzen von Art. 5 VE-DSG. Ein konkreter Anwendungsbereich von Abs. 1 ist nicht erkennbar, weshalb er ersatzlos zu streichen ist.
DSG	5	2 u. 3		Die Einschränkung, dass für eine Datenbekanntgabe ins Ausland eine **vorgängige Feststellung des Bundesrats** über die Angemessenheit des Datenschutzes im betreffenden Land notwendig ist, schränkt ungerechtfertigt und unnötig ein. Es ist durchaus denkbar, dass ein **Verantwortlicher gestützt auf eigene Abklärungen bzw. Kenntnisse** z.B. in Form einer «Legal Opinion» weiss, dass vor Ort ein angemessenes Datenschutzniveau gilt. Solche eigenen Abklärungen müssen zulässig sein. Umgekehrt kann dem Verantwortlichen nicht zugemutet werden, trotz Bedarf an Datenflüssen in ein bestimmtes Land darauf warten zu müssen, bis in unbestimmter Zukunft eine Einschätzung des Bundesrats vorliegt oder – mangels einer solchen – trotz besseren eigenen Kenntnissen bis zum Vorliegen der Einschätzung des Bundesrats immer die strengeren Voraussetzungen gemäss Abs. 3 einhalten zu müssen. Demzufolge ist Abs. 3 von Art. 5 VE-DSG wie folgt zu ergänzen (Ergänzungen unterstrichen):

				Liegt kein Entscheid des Bundesrats vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn der Verantwortliche selbst festgestellt hat, dass ein angemessener Schutz gewährleistet ist oder wenn ein geeigneter Schutz gewährleistet ist durch: …
DSG	5	3 u. 5	3 c u. d	Die Regelung, wonach standardisierte Garantien und sog. «Binding Corporate Rules» (BCR) einer **Genehmigungspflicht von sechs Monaten** unterliegen, ist weder sachgerecht noch praktikabel (Art. 5 Abs. 3 Bst. c u. d i.V.m. Abs. 5 VE-DSG). Einerseits stellen standardisierte Garantien ebenso wie BCR blosse Unterkategorien der «spezifischen Garantien» i.S.v. Art. 5 Abs. 3 Bst. b VE-DSG dar und für letztere ist lediglich eine Informationspflicht vorgesehen (eine Genehmigung durch den EDÖB ist nicht erforderlich). Ferner ist eine Frist von sechs Monaten abzulehnen. Dasselbe gilt für die Möglichkeit des EDÖB, Informationen nachzuverlangen, was die sechsmonatige Frist erneuern würde. Eine solche Regelung würde jeden unternehmerischen Handlungsbedarf im Keim ersticken und typische Bankgeschäfte mit internationalem Konnex verhindern (vgl. unten zu Art. 6 Abs. 1 Bst. a u. b VE-DSG). Im Ergebnis würden die bewährten Instrumente standardisierte Garantien und BCR gar nicht mehr verwendet.
DSG	5	6		Die pauschale Informationspflicht bietet weder der betroffenen Person noch dem EDÖB einen Mehrwert. Dementsprechend kennt auch die EU-DSGVO keine entsprechende Informationspflicht. Art. 5 Abs. 6 VE-DSG ist deshalb ersatzlos zu streichen.
DSG	6			**Kernanliegen: Berücksichtigung der Bedürfnisse der Praxis bei Festlegung der Ausnahmetatbestände**
DSG	6	1	a	Die Anforderung, dass die betroffene Person «im Einzelfall» einwilligen muss, ist eine allzu strenge Einschränkung. Nach allgemeinen Grundregeln des Vertragsrechts genügt es, wenn die betroffene Person mit Bezug auf bestimmte wiederkehrende Sachverhalte generell gültig zustimmen kann, mithin nicht nur für einen aktuellen Einzelfall, sondern auch mit Wirkung für analoge künftige Fälle. Dies ist bereits heute unter geltendem DSG von Lehre und Praxis anerkannt. Andernfalls würde ein enormer unnötiger Aufwand generiert, welchen die betroffene Person selbst nicht mehr verstehen würde. Im Interesse einer immer mehr arbeitsteilig und international vernetzt organisierten Wirtschaft z.B. ist der Verzicht auf das Erfordernis der Einwilligung im Einzelfall zwingend nötig. Eine generelle Information, welche den betroffenen Personen den wiederkehrenden Sachverhalt und die damit verbundenen typischen Risiken

				erläutert, muss genügen. Viele Massengeschäfte mit notwendigerweise internationalem Konnex wären andernfalls gar nicht mehr durchführbar mit der Folge von starken Wettbewerbsverzerrungen zu Lasten von Schweizer Unternehmen und zum Nachteil schweizerischer Kunden (welchen in der Schweiz nur noch eine laufend eingeschränkte Produktepalette zu immer höheren Preisen zur Verfügung stünde). Gegen das Zustimmungserfordernis im Einzelfall sprechen auch die typischerweise engen zeitlichen Verhältnisse. Zu denken ist z.B. an Kauf und Verkauf von Effekten für Kunden im Ausland, Verwahrung von Effekten im Ausland, etc. Das Erfordernis der Zustimmung im Einzelfall würde auch die einschlägige Regulierung der FINMA torpedieren, welche das internationale Bankgeschäft und die damit notwendigerweise zusammenhängenden Informationsflüsse u.a. mit Blick auf die typischerweise knappen zeitlichen Verhältnisse gerade ermöglichen und sicherstellen will (vgl. Art. 42c FINMAG u. dazu FINMA-RS 2017/6 Direktübermittlung). Demzufolge ist die Einschränkung **«im Einzelfall» ersatzlos zu streichen**.
DSG	6	1	b	Art. 6 Abs. 1 Bst. b VE-DSG muss aus Gründen der Rechtssicherheit und Äquivalenz mit der Regelung der EU-DSGVO in Übereinstimmung gebracht werden. Demnach sollte eine Bekanntgabe im Sinne eines Ausnahmefalls auch dann zulässig sein, wenn die betroffene Person nicht Vertragspartei ist, aber der fragliche Vertrag in ihrem Interesse oder zu ihren Gunsten abgeschlossen wurde. Diese Präzisierung ist z.B. im Bankenbereich für zahlreiche Konstellationen nötig. Bei internationalen Transaktionen des Handels und der Verwahrung von Wertschriften z.B. tritt die Bank nach bewährter Praxis in eigenem Namen und bloss im Interesse der betroffenen Kunden auf. Andere Lösungen wären in Massengeschäften dieser Art gegenüber ausländischen Vertragspartnern der Bank nicht durchsetzbar und – selbst wenn – mit Blick auf den immensen Aufwand für den einzelnen Kunden extrem kontraproduktiv, weil der einzelne Kunde mit wesentlich höheren Gebühren konfrontiert wäre. Solche bewährten Strukturen liegen somit im klaren Interesse der betroffenen Kunden. Art. 6 Abs. 1 Bst. b ist daher wie folgt anzupassen (Ergänzungen unterstrichen): *die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt <u>oder einer Person, zu deren Gunsten oder in deren Interesse der Vertrag abgeschlossen wird</u>;*
DSG	6	1	c Ziff. 2	Um schwierige Abgrenzungsfragen im Voraus auszuschliessen, sollten in Art. 6 Abs. 1 Bst. c Ziff. 2 VE-DSG die Begriffe «Gericht» sowie «Verwaltungsbehörde» ersatzlos gestrichen werden. Massgebend

				ist, dass die Datenbearbeitung zur «Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen» erfolgt. Die hierfür zuständigen ausländischen Behörden können aus historischen Gründen unterschiedlich organisiert sein sowie verschiedene Bezeichnungen tragen und sich nicht in eine der beiden Kategorien zuordnen lassen. Da es sich um ausländische Stellen und Verfahren handelt, dürfen deshalb nicht allein Schweizerische Traditionen massgebend sein. Vielmehr ist die Klausel offen zu formulieren, um auch wesentlich von Schweizer Traditionen abweichende Verfahrensformen zur Rechtsdurchsetzung zu erfassen (vgl. Werner Wyss, in: Nicolas Passadelis/David Rosenthal/Hanspeter Thür (Hrsg.), Handbücher für die Anwaltspraxis, Datenschutzrecht, Basel 2015, N 11.92 ff.). Demzufolge ist die Einschränkung «vor einem Gericht oder einer Verwaltungsbehörde» ersatzlos zu streichen. Art. 6 Abs. 1 Bst. c Ziff. 2 ist daher wie folgt anzupassen: *die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen ~~vor einem Gericht oder einer Verwaltungsbehörde~~;*
DSG	6	1	d	Vgl. Ausführungen zu Art. 6. Abs. 1 Bst. a VE-DSG. Anpassungsvorschlag: *die Bekanntgabe ~~im Einzelfall~~ notwendig ist, um das Leben oder die körperliche*
DSG	6	2		Art. 6 Abs. 2 VE-DSG ist **ersatzlos zu streichen**. Erstens ist eine Verpflichtung, den EDÖB trotz Ausnahmetatbestand zu informieren, unverhältnismässig. Typischerweise dürfte dies auch kontraproduktiv sein, da Ausnahmetatbestände i.d.R. zeitkritisch sind und keinen Aufschub dulden. Zweitens würde diese bereits (für Verantwortliche und Auftragsdatenbearbeiter) geltende Pflicht zu einer «*Meldeflut*» führen, welche der EDÖB gar nicht wird bewältigen können. Drittens würde der EDÖB über heikle Verfahren und (Geschäfts-) Geheimnisse informiert, ohne dass ein (sachlich gerechtfertigter) Grund dafür vorliegt und ohne Mehrwert für betroffene Personen. Zudem ist diese Pflicht dem EU Recht (inkl. ERK 108) fremd und somit ein kontraproduktiver Swiss Finish. Deshalb ist Abs. 2 ersatzlos zu streichen.
DSG	7	2		Art. 7 Abs. 2 VE-DSG führt Pflichten auf, welche gemäss Gesamtgefüge des VE-DSG ohnehin bereits bestehen. Diese Regelung ist demzufolge **ebenso wenig notwendig wie zusätzliche Präzisierungen in der Verordnung**. Letztere könnten **sogar kontraproduktiv** sein, da jedes Projekt eigene spezifische Datenschutzthemen generiert. Ein allgemeiner starrer Anforderungskatalog kann diesen Projekt-spezifi-

				schen Herausforderungen nicht gerecht werden. Vielmehr würde der Katalog Herausforderungen bestimmter Projekte gar nicht aufführen oder umgekehrt die Verantwortlichen zwingen, bestimmte Themen generell in jedem Projekt detailliert zu klären, obwohl diese je nach Projekt gar keine Rolle spielen. Allgemeine Präzisierungen würden somit einerseits per definitionem unvollständig bleiben und andererseits zu unnötigem Zusatzaufwand führen. Solche Detailregulierungen widersprechen sodann auch dem bewährten **prinzipienbasierten Ansatz** des DSG, an welchem der VE-DSG erklärtermassen festhalten will. Abs. 2 von Art. 7 VE-DSG ist demzufolge **ersatzlos zu streichen**. Soweit sich zu diesem Themenkreis wider Erwarten gleichwohl Präzisierungsbedarf ergeben sollte, ist der **Bundesrat** ohnehin generell – auch **ohne ausdrückliche spezifische Ermächtigung im Gesetz – befugt, die notwendigen Präzisierungen auf Verordnungsstufe zu erlassen**. Der Unterschied liegt darin, dass der Bundesrat gestützt auf eine ausdrückliche Anordnung, wie Art. 7 Abs. 2 VE-DSG sie vorsieht, zum Erlass von Verordnungsbestimmungen nicht nur berechtigt, sondern verpflichtet ist. Eine solche Notwendigkeit zum Erlass von Verordnungsbestimmungen besteht aber wie dargelegt aus heutiger Sicht nicht.
DSG	8 u. 9			Das vorgeschlagene **Konzept zur Erstellung von Empfehlungen der guten Praxis** ist im Kern zu begrüssen. Es lehnt sich an das bereits bestehende **Konzept von Selbstregulierungen der Branche** an, wie es sich z.B. im Bereich der Finanzwirtschaft bestens bewährt hat und von der Aufsichtsbehörde FINMA, dem EFD und den Schweizerischen Gerichten anerkannt ist (vgl. insbes. zahlreiche, äusserst hilfreiche Selbstregulierungen von SBVg und SFAMA). Der wesentliche Vorteil liegt darin, dass qua Selbstregulierung entweder **sehr knappe oder aber sehr komplexe gesetzliche Regelungen praxisnah und operativ umsetzbar präzisiert** werden können. Mit solchen Selbstregulierungen, neudeutsch auch «Codes of Conduct» genannt, werden **Mindeststandards** geschaffen, welche nach dem Prinzip «comply or explain» funktionieren. Datenschutzrechtlich gesprochen entspricht dies einer **«Safe Harbor»-Regelung**. Zur Erreichung dieses Ziels muss einerseits sichergestellt sein, dass die themenspezifischen Wünsche der Branche tatsächlich in die Regelung einfliessen. Andererseits muss die Regelung trotz grundsätzlich klärendem Ansatz einen ausreichenden Grad an **Prinzipienbasiertheit** aufweisen, damit jede betroffene Unternehmung **entsprechend individueller Grösse, Komplexität, Struktur und Risikoprofil ihres Geschäftsmodells eine angemessene Umsetzung** (so die bewährte Standardumschreibung der FINMA) des betreffenden Themas vornehmen kann.

				Diese Anforderungen sind durch spezifische Umformulierung von Art. 8 und 9 VE-DSG zu realisieren.
DSG	8			Der Wortlaut von Art. 8 VE-DSG lässt zu, dass der EDÖB Empfehlungen der guten Praxis mit einem Inhalt erlässt, welcher dem erklärten Willen der betroffenen Branchenvertreter widerspricht. Damit würde dieses Institut seinem Zweck nicht gerecht und würde sich ins Gegenteil verkehren (vgl. oben zu Art. 8 u. 9 VE-DSG). Richtigerweise muss (i) die **Initiative zum Erlass von Empfehlungen der guten Praxis zwingend von Branchenverbänden ausgehen**. (ii) Wenn die Vorschläge die einschlägigen **Datenschutzvorschriften einhalten, genehmigt der EDÖB** die Vorschläge in Form von Empfehlungen der guten Praxis. (iii) Führen die Verhandlungen zwischen Branchenvertreter und EDÖB nicht zu einer Regelung, welche dem von der Branche gewünschten Konzept entspricht, muss den **Branchenverbänden das Recht zustehen, die Vorschläge ohne Weiteres zurückzuziehen** und auf einschlägige Empfehlungen zu verzichten. (iv) Erlässt der EDÖB gleichwohl Empfehlungen der guten Praxis mit anderem Inhalt als von den Branchenverbänden gewünscht, muss dies in Form einer **von den Branchenverbänden anfechtbaren Verfügung** geschehen. (v) Der **EDÖB publiziert genehmigte Vorschläge der Branche** als Empfehlungen der guten Praxis. Art. 8 und 9 VE-DSG sind im vorstehenden Sinn umzuformulieren. Diese Lösung stellt auch die **Rechtstaatlichkeit der Regelung** sicher. Andernfalls stünde nämlich dem EDÖB eine kritische da allzu grosse Machtfülle zu, notfalls sogar gegen die Meinung der betroffenen Branchen Empfehlungen der guten Praxis zu erlassen. Entgegen etablierten rechtsstaatlichen und demokratischen Prinzipien würde er so de facto zum Gesetzgeber in Datenschutzthemen. Daraus ergäben sich auch zusätzliche Risiken einer nicht mehr in sich stimmigen Rechtsordnung. Im Extremfall könnte der EDÖB z.B. entgegen der Bankenbranche Empfehlungen der guten Praxis erlassen, welche etablierten von Bankaufsichtsgesetzgebung und FINMA-Praxis statuierten Regeln widersprächen. Damit wäre es den Banken verboten, die Empfehlungen des EDÖB einzuhalten, womit sich letztere ins Gegenteil verkehren würde: Statt einer erwünschten «Safe Harbor»-Regelung würde de facto eine Verbotsregelung geschaffen, indem es den Banken verunmöglicht würde, in einem bestimmten Bereich überhaupt tätig zu werden. Eine derartige Machtfülle darf dem EDÖB nicht von Gesetzes wegen zugestanden werden.

DSG	9	1		Art. 9 Abs. 1 VE-DSG geht sehr weit und stellt mit der gewählten Formulierung eine **unumstössliche Fiktion** auf. Mit Blick auf die Vielfalt des operativen Alltags sind innerhalb der von Empfehlungen der guten Praxis geregelten Materie aber Konstellationen denkbar, welche von den Empfehlungen nur unvollständig und unzureichend geregelt werden. Unter einer unumstösslichen Fiktion sind die erfassten Konstellationen eng auszulegen. Dies würde dazu führen, dass trotz Existenz von Empfehlungen zahlreiche Konstellationen vom «Safe Harbor» nicht profitieren. Damit verlören zahlreiche Empfehlungen ihren Wert. Stellen die Empfehlungen demgegenüber bloss eine Vermutung der Richtigkeit dar, besteht auslegungstechnisch mehr Spielraum, (zahlreiche) zusätzliche Konstellationen zu erfassen. Somit ist es zielführender, in Art. 9 Abs. 1 VE-DSG statt einer unumstösslichen Fiktion nur, aber immerhin die **Vermutung der Richtigkeit** zu statuieren. Diese Regelung wird auch der beabsichtigten Qualität der Empfehlungen als «Safe Harbor»-Regelung besser gerecht (vgl. oben zu Art. 8 u. 9 VE-DSG).
DSG	12			**Kernanliegen: Ersatzlose Streichung des ganzen Artikels** **Der Schutz und die Rechte verstorbener Personen gehören ins ZGB.** Die Regelung von Art. 12 VE-DSG ist schwer verständlich und erscheint im VE-DSG als Fremdkörper. Soweit es sich bei Personendaten auch um Geschäftsdaten handelt, was die Regel ist, bestehen gemäss diversen anderen einschlägigen Gesetzen (wie z.B. Buchführungsrecht gemäss OR, Steuerrecht, spezialgesetzliche Regelungen wie z.B. im Finanzmarktrecht zur Sicherstellung von Anlegerschutz, etc.) weitreichende legitime Dokumentations- und Archivierungspflichten, welche dem Kerngehalt von Art. 12 VE-DSG zuwiderlaufen. Nur schon deshalb bringt Art. 12 VE-DSG in dieser pauschalen Formulierung mit Wirkung für sämtliche Branchen und Konstellationen nichts und ist demzufolge ersatzlos zu streichen. Bei genauerem Betrachten fokussiert die Regelung wohl auf Daten einer verstorbenen Person auf **Social-Media-Plattformen**. Dann sollte dies aber wenn schon in der Regelung auch explizit so eingeschränkt werden. Allerdings bringt die Regelung auch im Bereich Social Media keinen erkennbaren Mehrwert. Effektiv gehen beim Tod einer Person dessen Rechte qua **erbrechtlicher Universalsukzession** ohne Weiteres auf die Erben über (Art. 560 Abs. 1 ZGB). Gestützt auf diesen erbrechtlichen Übergang sämtlicher Rechte von Gesetzes wegen sind die Erben bereits ausreichend legitimiert, geeignete Massnahmen vorzukehren und z.B. die Löschung von Daten des Erblassers auf einer Social-Media-Plattform zu verlangen. Die Regelung von Art. 12 VE-DSG ist somit weder nötig noch sinnvoll. Umgekehrt können

				die Erben per definitionem auch nicht mehr Rechte haben, als der Erblasser sie hatte. Art. 12 VE-DSG ist sogar kontraproduktiv, weil er eine Regelung aufstellt, welche zumindest nicht deckungsgleich ist mit etabliertem Erbrecht. Gleiches gilt mit Bezug auf Regelungen von Amts- und Berufsgeheimnissen in bereits bestehenden gesetzlichen Regelungen, für Banken z.B. nach Art. 47 BankG. Die pauschale Regelung, dass unter Art. 12 Abs. 3 VE-DSG Amts- und Berufsgeheimnisse generell nicht geltend gemacht werden können, kann so jedenfalls nicht stimmen. Tritt z.B. gemäss Vereinbarung der Erbengemeinschaft nur ein einzelner Erbe in die Rechtsstellung des Erblassers z.B. einer bestimmten Bank gegenüber ein, stehen nur diesem Erben sämtliche Rechte des Erblassers zu, während gegenüber allen anderen Erben das Bankkundengeheimnis uneingeschränkt gilt. Art. 12 VE-DSG ist auch unklar abgegrenzt zur im Rahmen der pendenten Erbrechtsreform geplanten Regelung des Auskunftsrechts von Erben nach neuem Art. 601a nZGB. Nach alldem ist Art. 12 VE-DSG jedenfalls geeignet, statt der – heute nach Erbrecht bereits bestehenden – Rechtssicherheit eher **Widersprüche zu bereits bestehenden gesetzlichen Regelungen** zu produzieren. Nicht berücksichtigt sind ausserdem die Rechte und Pflichten des Datenverantwortlichen (zum Beispiel Forderung auf Datenvernichtung im Zusammenhang mit der Weiterführung einer Hypothek, Aktenaufbewahrung etc.). Aufgrund all dieser Argumente fordern wir die **ersatzlose Streichung von Art. 12 VE-DSG**. Stattdessen ist soweit sinnvoll zu überlegen, inwieweit gezielte spezialgesetzliche Regelungen z.B. in Ergänzung von Art. 28 ff. ZGB sinnvoll erscheinen. Nach dem Gesagten eher nicht. Sollte dieser ersatzlosen Streichung wider Erwarten nicht gefolgt werden, müsste in der Regelung von Art. 12 Abs. 1 Bst. a zumindest der Begriff «kostenlos» ersatzlos gestrichen werden.
DSG	13			**Kernanliegen: Reduktion der Informationspflichten auf das Wesentliche. Die Information über die Beschaffung von Personendaten muss auch in allgemeiner Form möglich sein. Die Informationspflichten sind zusätzlich zu präzisieren.**
DSG	13	1		Sinnvollerweise wird die Informationspflicht ausdrücklich auf **besonders schützenswerte Daten** und überdies auf **Datenbearbeitungen ausserhalb des (objektivierten) Erkennbarkeitshorizonts** i.S.v. Art. 4 DSG der betroffenen Person eingeschränkt. Dies folgt aus dem naheliegenden Grundsatz, dass alle anderen Daten entsprechend den Grundsätzen von Art. 4 VE-DSG für die betroffene Person erkennbar sind und demzufolge keiner (zusätzlichen) Information bedürfen.

				Klarzustellen im Gesetz ist, dass die Information sich jedenfalls auf den Zeitpunkt der Datenbeschaffung bezieht und sich auch die Richtigkeit und Vollständigkeit der Daten an diesem Zeitpunkt misst. Für spätere Änderungen kann keine Informationspflicht bestehen. Zudem hat Art. 13 VE-DSG aus Klarheitsgründen in sich konsequent dieselbe Terminologie zu verwenden. Es muss z.B. konsequent von «Dritten» gesprochen werden (wie in Abs. 1) und nicht von «Empfängern» (wie in Abs. 3 u. 4) und statt von «Identität» vom «Namen» des Verantwortlichen. Sofern eine Pflicht zur Beschaffung von Informationen im Gesetz angelegt ist, ist der Betroffene nicht noch separat zu informieren. Der Artikel sollte folglich dahingehend präzisiert werden, da insbesondere im Geldwäschereigesetz für Banken bereits Datenbeschaffungspflichten bestehen.
DSG	13	3		Die Informationspflicht wird auf **alle Personendaten** ausgeweitet, was zu erheblichem **Mehraufwand** für die Unternehmen führen wird. In den Erläuterungen sollte präzisiert werden, dass bei allfälligen Änderungen keine Nachinformation erfolgen muss. Art. 13 Abs. 3 VE-DSG verwendet die Begriffe «Dritter» und «Empfängerinnen und Empfänger», ohne diese genau zu definieren. Wir fordern deshalb, die Schlüsselbegriffe zu definieren, idealerweise in Form eines Glossars am Anfang des Gesetzes oder als Anhang, um die Begriffe entlang des ganzen Gesetzes durchgängig gleichförmig zu verwenden. Der gesamte Absatz ist unklar formuliert, was insbesondere die Abgrenzung der Pflichten des Verantwortlichen und des Auftragsdatenbearbeiters betrifft. Abs. 3 sollte deshalb **ersatzlos gestrichen** werden.
DSG	13	4		Die **Mitteilung der Identität und Kontaktdaten sämtlicher Auftragsdatenbearbeiter ist überschiessend** und weder sinnvoll noch nötig. Solche Pflichten kennt auch die **EU-DSGVO nicht**. Diese Anforderung ist somit kontraproduktiver **Swiss Finish**, der für die notwendige Äquivalenz nicht notwendig ist. Wenn schon, dann wäre von «Name» statt «Identität» zu sprechen. Zahlreiche Auftragsdatenbearbeiter sind zudem bloss für untergeordnete Tätigkeiten mandatiert. Die Offenlegung sämtlicher Auftragsdatenbearbeiter widerspricht deshalb auch dem datenschutzrechtlichen Verhältnismässigkeitsprinzip («need to know»). Auch gesetzliche Pflichten des Verantwortlichen müssen selbstverständlich widerspruchsfrei in das übrige datenschutzrechtliche Gesamtkonzept des Gesetzes, wozu u.a. Art. 18 Abs. 2 VE-DSG («need to know») gehört, eingebettet sein.

				Überdies greift die Offenlegung von Identität und Kontaktdaten sämtlicher Auftragsdatenbearbeiter massiv in berechtigte eigene Datenschutzinteressen und überdies in Geschäftsgeheimnisse des Unternehmens ein, welche gesetzlich geschützt sind (Art. 162 StGB). Es steht dem VE-DSG nicht an, in anderen Gesetzen geregelte Geheimnispflichten einfach zu missachten. Schliesslich würde die Liste sämtlicher Auftragsdatenbearbeiter kaum einen informativen Mehrwert produzieren. Zumindest innerhalb derselben Branche würde sich vermutlich zeigen, dass sehr viele Marktteilnehmer zur Unterstützung auf dieselben Auftragsdatenbearbeiter abstellen. Damit würde den betroffenen Personen de facto auch jedes Wahlrecht genommen, je nach Inhalt der Liste z.B. die Bank zu wechseln. Aufgrund all dieser Argumente kommt der Offenlegung von Identität und Kontaktdaten unter keinem vernünftigen Titel, nicht einmal unter den datenschutzrechtlichen Gründen i.e.S., ein sinnvoller Zweck zu. Im Gegenteil würde eine solche Offenlegung zur Verletzung berechtigter Datenschutzbedürfnisse des Unternehmens führen. Dies alles muss dazu führen, dass diese unnötigen Zusatzanforderungen **ersatzlos gestrichen werden**.
DSG	13	5		Diese Pflicht zur Weitergabe von Informationen **sprengt den Rahmen von Datenschutz i.e.S.** Die Regel fordert maximale Transparenz zum Preis eines hohen, unverhältnismässigen Aufwands. Da die Bestimmung die Datenbeschaffung durch Dritte regeln will, sind die relevanten Eckpfeiler wie insbesondere «erstmalige Speicherung» regelmässig gar nicht bekannt. Der dafür eingesetzte Dritte kennt diese Modalitäten naturgemäss viel besser. Wird der Verantwortliche direkt verpflichtet, müsste er deshalb aus Gründen seiner Sorgfaltspflicht immer zuerst den Dritten anfragen, bevor er gestützt auf dessen Angaben die betroffenen Personen informieren könnte. Dies ist im operativen Alltag weder sinnvoll noch zielführend. Solche direkten Informationspflichten sind aber auch gar nicht nötig. Wenn überhaupt, dann wäre eher zu überlegen, inwiefern eine Verpflichtung des Dritten zur indirekten Weitergabe implementiert werden soll. Dies wäre nach dem Gesagten jedenfalls sachlich näherliegend und wesentlich einfacher bzw. weniger aufwendig. Auch mit dieser Umsetzung bliebe die Regel aber infolge ihres schlechten Aufwand/Ertrags-Verhältnisses mehr als fraglich. Im Gesamtgefüge des VE-DSG muss eine allgemeine vorgängige Information an die betroffenen Kunden genügen, wonach bestimmte Daten zu bestimmten Zwecken an bestimme Kategorien von Dritten

				beschafft und gegebenenfalls auch bearbeitet werden (vgl. Art. 13 Abs. 1-3 VE-DSG). Der Abs. 5 bringt dazu keinen Mehrwert, sondern nur unnötigen Mehraufwand. Dieser Absatz ist deshalb **ersatzlos zu streichen**.
DSG	14	1		Der Bankkunde erteilt bereits durch das Anvertrauen der Gelder oder der Beanspruchung eines Kredites seine stillschweigende Zustimmung zur Datenbeschaffung. Eine explizite Informationspflicht ist im Bankwesen daher nicht notwendig. Art. 14 VE-DSG sollte eine solche Ausnahme daher vorsehen und wäre wie folgt zu ergänzen (Ergänzungen unterstrichen): *Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person ihre stillschweigende Zustimmung zur Datenbeschaffung- ~~etwa im Rahmen eines Bankgeschäftes~~ erteilt hat.*
DSG	14	4	a	Wir schlagen vor, die Bestimmung wie folgt zu formulieren (siehe hierzu die Ausführungen in Art. 21 VE-DSG): *a) wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern ~~und er die Personendaten nicht Dritten bekannt gibt;~~*
DSG	14	6 (neu)		In der EU-DSGVO ist eine Bestimmung eingefügt, welche offenkundig unbegründete oder exzessive Anträge regelt. Der Schweizer Gesetzgeber muss eine vergleichbare Regelung aufnehmen. Nur so können «gleich lange Spiesse» erzielt und den wichtigen Anliegen der Verhinderung unnötigen Aufwands Rechnung getragen werden. Wir schlagen vor, den folgenden neuen Absatz zu ergänzen: *a) Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person, kann der Verantwortliche entweder ein angemessenes Entgelt verlangen, bei dem die Kosten für den Aufwand von Unterrichtung, die Mitteilung oder Durchführung der beantragten Massnahme berücksichtigt werden, oder* *b) sich weigern, aufgrund des Antrags tätig zu werden.*
DSG	15			**Kernanliegen: Ersatzlose Streichung des Äusserungsrechts (Art. 15 Abs. 2 VE-DSG)**

				Ein zentraler Punkt der Digitalisierung ist die Automatisierung. Gerade durch Automatisierung lassen sich Effizienzgewinne und damit einhergehend Aufwandreduktionen erzielen, welche im heutigen wirtschaftlichen Umfeld unabdingbar geworden sind. Zudem wirken sie sich auch positiv bei den Kunden aus, z.B. durch attraktive Preisgestaltung.
DSG	15	2		Das in Art. 15 Abs. 2 VE-DSG neu vorgeschlagene Recht einer betroffenen Person, sich zu einer automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern («Anhörungspflicht»), stufen wir als **wettbewerbs- und innovationshemmend** ein. Darüber hinaus ist dieses Recht aber auch schlicht unnötig, insbesondere angesichts der ebenfalls neu eingeführten Pflicht, die betroffene Person darüber zu informieren, wenn eine automatisierte Einzelentscheidung gefällt wurde (Art. 15 Abs. 1 VE-DSG). Unabhängig davon gewissermassen «auf Vorrat» zu informieren produziert demnach keine zusätzliche Transparenz, sondern generiert lediglich unnötigen zusätzlichen Administrativaufwand. Weder die ERK 108 noch die EU-DSGVO sehen ein entsprechendes Äusserungsrecht vor. Die Regelung von Art. 15 Abs. 2 VE-DSG ist demzufolge ein kontraproduktiver und im Hinblick auf die Äquivalenz unnötiger Swiss Finish. **Automatisierte Entscheide** bringen gegenüber manuellen Entscheidungsprozessen auch erhebliche **Vorteile** für Anbieter und Kunden mit sich (Objektivität der Entscheidung, geringere Kosten, schnellere Prozesse). Es ist deshalb nicht einzusehen, warum vollautomatisierte Entscheide durch die Datenschutzgesetzgebung faktisch verboten werden sollten. Es ist ausserdem auch nach Konsultation der Botschaft weitgehend unklar, wann genau eine automatisierte Einzelentscheidung vorliegt. Die Kunden können selbst entscheiden, ob sie zu einem Anbieter wollen, der vollautomatisierte Entscheide trifft oder zu einem Anbieter, der zusätzlich oder vollständig auf die Arbeitskraft natürlicher Personen setzt. Diese Grundentscheidung mit Bezug auf das Geschäftsmodell spiegelt sich regelmässig auch in unterschiedlichen Preisen wieder. Der Kunde wird darüber gemäss Art. 15 Abs. 1 VE-DSG bereits ausreichend informiert (z.B. mit einem Piktogramm). Eine Regel wie sie in Art. 15 Abs. 2 VE-DSG vorgeschlagen wird, würde daher den Kunden und Konsumenten unnötigerweise bevormunden. Zudem gehört die Information darüber, wie bestimmte Entscheide zustande kommen, zum Geschäftsgeheimnis eines Unternehmens, und ist demnach, insbesondere in der aktuell vorgesehen, detaillierten Form gemäss Art. 20 Abs. 3 VE-DSG klar unverhältnismässig. So ist zum Beispiel im Finanzbereich die

				Einschätzung von Ausfallrisiken bei der Kreditvergabe eine wichtige, differenzierende Kompetenz eines Finanzdienstleisters. Die Auskunft über die für diese Einschätzung genutzten Daten und deren Gewichtung führt zu einer Replizierbarkeit dieser Einschätzung und damit zur Aufgabe dieses Geschäftsgeheimnisses. Offenlegungspflichten solcher Art würden im Ergebnis die Innovationskraft der Wirtschaft erheblich beeinträchtigen, da der dafür eingesetzte Aufwand nicht angemessen geschützt werden könnte. Die Ausnahmebestimmung von Art. 21 Abs. 1 VE-DSG dürfte daher mehr die Regel als die Ausnahme bilden. Schliesslich ist die Befürchtung nicht von der Hand zu weisen, dass die Einführung einer Pflicht zur «Äusserung» in der Praxis zu einer **Begründungspflicht** führt und letztlich die Vertragsfreiheit eines Unternehmens erheblich einschränkt. Die Relevanz bestimmter Daten für die Richtigkeit von Entscheidungen und der Grad der Wichtigkeit von automatisierten Entscheidungen i.S.v. Art. 15 VE-DSG kann von Branche zu Branche sehr unterschiedlich sein. Daraus ergibt sich, dass eine generelle Regelung für die gesamte Wirtschaft jedenfalls über das Ziel hinausschiesst. Nicht grundsätzlich abwegig ist es demgegenüber, soweit nötig für einzelne branchenspezifische Datennutzungen in einschlägigen Spezialgesetzen eine angemessene Regelung zu treffen, welche den Besonderheiten der betreffenden Branche gebührend Rechnung trägt. Aufgrund all dieser Argumente fordern wir dezidiert die **ersatzlose Streichung der Äusserungsrechts von Art. 15 Abs. 2 VE-DSG**.
DSG	15 u. 20			**Folgen** der ersatzlosen Streichung des Äusserungsrechts in Art. 15 Abs. 2 VE-DSG: Folgerichtig ist **auch der entsprechende thematische Abschnitt in Art. 20 Abs. 3 VE-DSG ebenfalls zu streichen**. Sollte dem Streichantrag wider Erwarten nicht gefolgt werden, müsste jedenfalls vorab Art. 20 Abs. 3 VE-DSG als dort - unter dem allgemeinen Auskunftsrecht - sachfremde Regelung gestrichen und mit Art. 15 VE-DSG zu einer in sich stimmigen Gesamtlösung verbunden werden. Dabei wäre die Regelung - entsprechend dem richtigen Ansatz der EU-DSGVO, mit welchem der VE-DSG äquivalent zu sein hat - auf schwere Fälle zu begrenzen, d.h. auf solche mit erheblichen Auswirkungen auf die betroffene Person. Sodann wäre klarzustellen, dass jedenfalls eine einmalige angemessene Information ohne ausdrückliche Einwilligung im Sinne der Gesetzessystematik ausreichend ist. Dadurch wird auch das in Art. 20 Abs. 3 VE-DSG vorgesehene Auskunftsrecht über automatisierte Einzelfallentscheidungen obsolet.

DSG	16			Die Regelung der Datenschutz-Folgenabschätzung (DSFA) im Vorentwurf erachten wir im Grundsatz als überflüssig. Die Forderung von Art. 8bis der revidierten ERK 108, bei geplanten Datenbearbeitung die Risiken einzuschätzen, wird durch Art. 11 VE-DSG (Datensicherheit) bereits erfüllt. Wir erachten diese Regelung im vorliegenden Kontext für verzichtbar, zumal die Folgeabschätzungen stark interpretationsbedürftig bleiben und zu einem grossen, nicht absehbaren Aufwand führen, ohne dass ein Datenschutzmissbrauch letztlich verhindert werden könnte. Wir fordern daher ihre **Streichung**. Sofern an einer eigenen gesetzlichen Regelung der DSFA festgehalten wird, ist folgendes zwingend zu beachten. Die Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen, ist im vorliegenden VE-DSG viel zu weit gefasst. Der Natur der Sache nach muss sich die Regelung **auf hohe Risiken beschränken**, wobei die Erheblichkeit – entsprechend der Regelung gemäss EU-DSGVO – aufgrund des gemäss DSFA erreichten Endresultats zu beurteilen ist. Mithin liegen erhebliche Risiken nur vor, soweit **selbst nach Implementierung geeigneter Massnahmen** weiterhin hohe Risiken verbleiben. Im aktuellen Entwurf würde die Regel ohne Notwendigkeit enormen Aufwand produzieren, welcher überdies sogar einen klaren, für die Äquivalenz unnötigen **Swiss Finish** darstellen würde. Überdies bestehen zahlreiche Spezialregeln, welche bestimmte Datenflüsse bereits einer anderweitigen Überwachung unterstellen. Im Bankenbereich wird z.B. der notwendige niederschwellige Datenfluss an ausländische Stellen (welche nicht Behörden sein müssen) gemäss Art. 42c FINMAG durch die FINMA überwacht (vgl. neues FINMA-RS 2017/6 «Direktübermittlung»). Solche «doppelten» Überwachungen sind aus Effizienzgründen und zur Vermeidung von Widersprüchen zu vermeiden. Wie dieses Beispiel zeigt würde eine zusätzliche Überwachung durch den EDÖB dem Zweck der Regelung von Art. 42c FINMAG und des einschlägigen FINMA-RS 2017/6 offensichtlich zuwiderlaufen, im Interesse von teilweise sehr kurzen Fristen für notwendige Datenflüsse klare und rechtssichere Regeln für eine rasche Lösung der Thematik im Einzelfall zur Verfügung zu stellen. Andernfalls wären Banken international von zahlreichen wichtigen Geschäftssparten faktisch ausgeschlossen. Sofern an einer Regelung festgehalten wird, wäre Art. 16 VE-DSG aus den genannten Gründen wie folgt neu zu fassen (Ergänzungen unterstrichen, vgl. dazu im **Einzelnen die nachfolgenden Begründungen unten**):

				[1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen~~erhöhten~~ Risiko für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen. *[2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit ~~oder der Grundrechte~~ der betroffenen Person zu verringern.* *[3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen, sofern trotz der vorgesehenen Massnahmen hohe Restrisiken für eine Verletzung der Persönlichkeit der betroffenen Person vorauszusehen sind.* *[4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von ~~drei Monaten~~ einem Monat nach Erhalt aller erforderlichen Informationen mit.*
DSG	16	1		Der Ausdruck «erhöhtes Risiko» in Abs. 1 ist zu unbestimmt. Er geht zudem über die europäischen Vorgaben hinaus: **Art. 35 f. EU-DSGVO und Art. 27 Ziff. 1 der Schengen-Richtlinie verlangen eine Datenschutz-Folgenabschätzung jeweils nur bei einem «hohen» Risiko**. Der VE DSG ist entsprechend anzupassen. Ohne eine solche Anpassung müsste jede Bearbeitung, die in irgendeiner Hinsicht ein Risiko mit sich bringt (schon jede Übermittlung ins Ausland) zu einer Datenschutz-Folgenabschätzung und einer Meldung an den EDÖB führen (schon wegen des Sanktionsrisikos). Dies würde hohe Kosten verursachen, denen kein angemessener Mehrwert gegenübersteht.
DSG	16	2		**Es ist zudem falsch, von einem Risiko für «die Grundrechte» der betroffenen Personen zu sprechen.** Das entspricht zwar mehr oder weniger der Regelung der EU-DSGVO. Das europäische Recht kennt aber eine direkte Drittwirkung der Grundrechte, die dem schweizerischen Recht fremd ist. Wenn Art. 16 VE DSG vom Risiko für Grundrechte spricht, würde dies eine konzeptionelle Änderung bedeuten. Das ist abzulehnen: Es ist nicht Aufgabe privater Datenbearbeiter, die Grundrechte betroffener Personen zu schützen, soweit diese Grundrechte nicht in den einzelnen Anforderungen des DSG Ausdruck gefunden haben. Dazu kommt, dass völlig unklar ist, um welche Grundrechte es geht und welche Risiken dabei relevant wären.

				Schliesslich spricht Art. 16 Abs. 1 VE DSG davon, dass «der Verantwortliche *oder* der Auftragsbearbeiter» verpflichtet sind, die Datenschutz-Folgenabschätzung durchzuführen. Diese Formulierung kann nur bedeuten, **dass die Pflicht den Verantwortlichen trifft, dieser aber befugt ist, die Durchführung der Datenschutz-Folgenabschätzung dem Auftragsbearbeiter zu übertragen**. Die Formulierung ist aber missverständlich und daher zu präzisieren (vgl. oben).
DSG	16	3		**Viel zu weit geht auch die Meldepflicht an den EDÖB.** Nach der vorgeschlagenen Regelung ist der EDÖB über jede Datenschutz-Folgenabschätzung zu informieren. Das ist strikt abzulehnen: - Jede Datenschutz-Folgenabschätzung melden zu müssen, stellt einen massiven Eingriff in die Geheimsphäre der Unternehmen dar. - Den Unternehmen würde durch eine solche Meldepflicht ein Anreiz gesetzt, im Zweifel keine Datenschutz-Folgenabschätzung durchzuführen. Das wäre kontraproduktiv. - Wenn jede Datenschutz-Folgenabschätzung meldepflichtig ist, wird der EDÖB von Meldungen überflutet. Er kann auf die zahlreichen Meldungen von Datenschutz-Folgenabschätzung nicht reagieren. Eine unterschiedslose Meldepflicht führt nur zu bürokratischen Leerläufen ohne Nutzen. Denn auch dieser sehr grosse, nicht absehbare Aufwand könnte letztlich einen Datenmissbrauch nicht verhindern. - Selbst das europäische Recht verlangt nicht, die Aufsichtsbehörden von jeder Datenschutz-Folgenabschätzung zu informieren. Art. 36 Abs. 1 EU-DSGVO verlangt eine Meldung im Gegenteil nur dann, wenn die Datenschutz-Folgenabschätzung ergibt, dass trotz der vorgesehenen Massnahmen ein hohes Risiko verbleibt. Art. 36 Abs. 1 EU-DSGVO ist zwar unklar formuliert, doch ergibt sich dies eindeutig aus den Erwägungsgründen der EU-DSGVO.
DSG	16	4		**Auch die Reaktionszeit des EDÖB von drei Monaten ist viel zu lang**. Wenn Unternehmen drei Monate auf eine Antwort des EDÖB warten müssen, führt dies zu erheblichen Verzögerungen und wirkt massiv innovationshemmend. Im Fall einer Meldung hat der EDÖB ausschliesslich zu prüfen, ob die vorgeschlagenen Massnahmen ausreichend sind. Dafür genügt ein Monat. Dies insbesondere deshalb, weil der EDÖB diese Frist durch Nachfragen laufend verlängern kann.
DSG	17			Diese Pflicht wird ohne **gezielte Eingrenzung in qualitativer und quantitativer Weise** uferlos. Entsprechend würden die Verantwortlichen, um dem Vorwurf einer strafbaren Handlung zu entgehen (vgl.

				Art. 50 Abs. 2 Bst. e VE-DSG), jeden noch so geringfügigen Verstoss melden. Der Beauftragte wäre ausser Stande, innerhalb dieser Papierflut wirklich wichtige Meldungen zeitgerecht zu erkennen und geeignete Massnahmen einzuleiten. In solchen Fällen sähe er sich selbst mit dem Vorwurf konfrontiert, trotz erhaltener Meldung nicht gehandelt zu haben. Insgesamt verkäme das Institut zum reinen Formalismus, welcher allerdings für alle Beteiligten äussert aufwendig wäre. Die Regelung krankt überdies am Ansatz, dass der Verantwortliche sich mit Erfüllung der Meldepflicht in Bezug auf die Verfehlungen, welche zur Datenschutzverletzung geführt haben, de facto gleich selbst anzeigen muss. Damit wird das strafrechtliche Grundprinzip, dass niemand sich selbst anzeigen muss (nemo tenetur), verletzt. Befolgt er die Meldepflicht nicht, wird er gleichwohl durch Nichteinhaltung derselben strafbar (Art. 50 Abs. 2 Bst. e VE-DSG). Umso schlimmer ist diese Regelung, wenn man davon ausgeht, dass seriöse Datenbearbeiter der Meldepflicht wohl nachkommen werden und gestützt darauf «als Dank» für ihre Versäumnisse sanktioniert werden. Demgegenüber werden die wirklich «schwarzen Schafe» die Meldepflicht nicht ausüben und – in vielen Fällen zu Recht – darauf vertrauen, dass der Skandal nicht erkannt wird und «unter dem Deckel» gehalten werden kann. Mit solchen Regelungen werden mithin schlicht die falschen Anreize gesetzt. Dies ist selbstredend zu verhindern. Das Dilemma könnte dadurch gelöst werden, dass der VE-DSG dem die Meldepflicht ausübenden Verantwortlichen einen «Bonus» oder gar Straffreiheit in Aussicht stellt, wie dies z.B. auch gemäss Kartellgesetz (KG) der Fall ist. Dies spricht übrigens auch dafür, dass – ebenfalls analog zum KG – die Sanktionskompetenz der Verwaltungsbehörde unter VE-DSG dem EDÖB zustehen soll und nicht den Strafbehörden und -gerichten (vgl. unten zu Art. 50 ff. VE-DSG). Ohnehin muss die aus einer allzu weit gefassten Papierflut resultierende kontraproduktive Papierflut eingedämmt werden. Dies geschieht am besten dadurch, dass – **wie dies die EU-DSGVO vorsieht** – **in qualitativer Hinsicht** nur **grobe Datenschutzverstösse** zu melden sind. Letztlich muss es um solche Fälle gehen, in welchen der Verantwortliche wegen der Dimension der Datenschutzverletzung nicht mehr aus eigener Kraft in der Lage ist, sämtliche geeignete Massnahmen einzuleiten und deshalb zur zielgerichteten Unterstützung an den EDÖB gelangt. Das qualitative Element der groben Datenschutzverletzung ist sodann mit einem **quantitativen Element** zu konkretisieren, wonach z.B. nur Fälle, in welchen Daten von **mindestens 100’000 Personen betroffen** sind, eine Meldepflicht auslösen.

				In zeitlicher Hinsicht ist sodann eine unverzügliche Meldung, wie sie Art. 17 Abs. 1 VE-DSG vorsieht, **nicht zielführend**. Massgebend muss der Zeitpunkt sein, in welchem dem Verantwortlichen **hinreichende Informationen** zur Beurteilung vorliegen, ob überhaupt eine Datenschutzverletzung stattgefunden hat und gegebenenfalls, ob sie eine meldepflichtige Dimension aufweist. Erst solche Klarheit über den Sachverhalt kann eine Meldepflicht auslösen. Es müssen mithin analoge Grundsätze zur Anwendung kommen, wie sie im Zivilrecht z.B. für die Beurteilung massgebend sind, ob eine Verjährungs- oder Verwirkungsfrist zu laufen beginnt. Erst eine mit solchen qualitativen, quantitativen und zeitlichen Einschränkungen versehene Meldepflicht für (grobe) Datenschutzverstösse ist zielführend und macht Sinn. Mit Blick auf den bereits stark reglementierten und beaufsichtigten Finanzbereich geben wir schliesslich zu bedenken, dass weitere Meldepflichten zu erheblichen Kompetenzproblemen zwischen Behörden führen können. In diesem Fall ist zu erwägen, ob Meldungen an den EDÖB nicht notwendig sein sollten, wenn der Datenschutzverantwortliche einer anderen Bundesaufsicht untersteht und allfällige Meldungen (beispielsweise aufgrund einer Verletzung eines Bankkundengeheimnisses) an diese zu richten hat (im Beispiel an die FINMA).
DSG	18			Mit dieser Bestimmung werden allgemeine Grundprinzipen des Datenschutzes wie z.B. im Abs. 2 der Grundsatz «need to know» kodifiziert. Aus Gründen der besseren Systematik und Übersichtlichkeit sollten diese in Art. 11 VE-DSG integriert und hier gestrichen werden.
DSG	19			Der VE-DSG weist bereits zahlreiche Informations- und Dokumentationspflichten auf. Durch Wiederholung in verändertem Wortlaut wie z.B. in Art. 19 VE-DSG entstehen bloss kontraproduktive Auslegungs- und Abgrenzungsprobleme, welche die notwendige Rechtssicherheit beeinträchtigen. Aus nachstehenden Ausführungen zu Bst. a und b von Art. 19 VE-DSG ergibt sich, dass diese Bestimmung hier zu streichen ist und der Inhalt, soweit notwendig, in andere Bestimmungen des VE-DSG integriert wird.
DSG	19		a	In Würdigung vorstehender Erwägungen und aus Gründen der notwendigen **Äquivalenz mit der EU-DSGVO** fordern wir, die in Bst. a von Art. 19 VE-DSG geregelte allgemeine Dokumentationspflicht durch die griffigere Anforderung zu ersetzen, dass ein **«Verzeichnis» als Dokumentation der Datenbearbeitungen** zu erstellen ist. Erst damit erhält die Bestimmung Art. 19 Bst. a VE-DSG eine gegen-

				über den zahlreichen anderweitig gemäss VE-DSG bestehenden Dokumentationspflichten klar fassbare, eigenständige Bedeutung. Aus Gründen der leichteren Auffindbarkeit und im Interesse der besseren Verständlichkeit des VE-DSG ist die im vorstehenden Sinn präzisierte Regelung von Art. 19 Bst. a VE-DSG systematisch **besser bei Art. 11 VE-DSG zu integrieren**. Wir geben zudem zu bedenken, dass die Dokumentation jeder Datenbearbeitung in einer Unternehmung einen grossen Aufwand verursachen und abschliessend (bei Strafandrohung) gar nicht möglich sein dürfte. So bearbeitet bspw. eine Bank täglich tausende von Daten ihrer Kunden, die personenbezogen sind. Diesem Umstand muss besser Rechnung getragen werden.
DSG	19		b	Diese Pflicht geht sehr weit, ohne dass ein klarer datenschutzrechtlicher Mehrwert erkennbar ist. Selbst die EU-DSGVO kennt solche Pflichten nicht. Nur schon aus Gründen der notwendigen **Äquivalenz** sollte deshalb darauf verzichtet werden. Kommt dazu, dass weder der Verantwortliche noch dessen Auftragsdatenbearbeiter selbst umfassend beurteilen können, welche Daten für welche Empfänger überhaupt (noch) von Interesse sind. Nur mit Bezug auf solche Daten würde sich aber eine Information überhaupt rechtfertigen. Die betroffene Person selbst kann dies viel besser beurteilen als Verpflichteter und Auftragsdatenbearbeiter. Pauschale «Massen»-Informationen an alle möglichen Adressaten würden nur unnötigen Aufwand beim Abwesenden und Unklarheiten bei den zahlreichen Empfängern generieren und wären überdies **kontraproduktiv**, da gesetzlich normierter klarer Verstoss gegen das datenschutzrechtliche Prinzip der Verhältnismässigkeit (Grundsatz «need to know»). Dahingehende Ansprüche der betroffenen Personen bestehen bereits nach **Art. 25 VE-DSG** (vgl. insb. Abs. 1 Bst. c). Insbesondere erscheint es nicht praktikabel, wenn Kunden informiert werden müssten, nachdem die Geschäftsbeziehung längst beendet ist. Nach alledem bleibt es besser den betroffenen Personen überlassen, die aus eigener, besserer Wahrnehmung wichtigen und richtigen Ansprüche gestützt auf Art. 25 Abs. 1 Bst. c VE-DSG geltend zu machen. Art. 19 Bst. b VE-DSG verbessert diesen Schutz wie dargelegt nicht und ist am besten zu **streichen**. Schliesslich muss es möglich bleiben, während der Kundenbeziehung Daten zu vernichten, ohne den Kunden zu informieren, sowie auch Kundendaten jederzeit zu löschen bzw. zu vernichten, sofern diese nicht aufbewahrt werden müssen (bspw. Massendaten wie Kontoauszüge).

DSG	20 u. 21			**Kernanliegen: Einführung von Mechanismen zur Verhinderung des Missbrauchs des Auskunftsrechts**
DSG	20			Das allgemeine Auskunftsrecht ist im Kern unbestritten. Die Ausweitung des Auskunftsrechts auf **sämtliche Datenbearbeitungen** und überdies auf hängige Verfahren (vgl. Art. 2 Abs. 3 VE-DSG) ist aber unverhältnismässig. Dies gilt umso mehr, als gemäss geltender Schweizer Rechtsprechung kein Auskunftsersuchen je rechtsmissbräuchlich sein kann, weil selbst ein untergeordnetes Datenschutzinteresse ausreicht, um einen Auskunftsanspruch zu bejahen. Die Anknüpfung am bisher bewährten System der Datensammlung wäre sachgerechter und würde den betroffenen Personen ausreichenden Schutz bieten.
DSG	20	1		Dem zunehmenden **Missbrauch des Auskunftsrechts** für datenschutzfremde Zwecke ist ein Riegel zu schieben. Die Vergangenheit hat leider gezeigt, dass einerseits datenschutzrechtliche Begründungen viel zu leicht vorgeschoben werden können, um eine kostenlose Beschaffung von Beweismitteln durchzusetzen. Andererseits hat die Anzahl querulatorischer, kosten- und ressourcenintensiver Fälle zu reinen Schikanezwecken ebenfalls stark zugenommen. Aus diesen Gründen ist der Ansatz falsch, das **Auskunftsrecht generell kostenlos** auszugestalten. Damit wird ein Grundprinzip verletzt, welches ansonsten in der Rechtsordnung generell gilt. Dementsprechend ordnet auch die EU-DSGVO keine allgemeine Kostenlosigkeit an (Art. 12 Ab. 5 EU-DSGVO). Die von Art. 20 Abs. 1 VE-DSG angeordnete pauschale Kostenlosigkeit der Auskunft ist deshalb **nicht äquivalent** und demzufolge ersatzlos zu streichen. Stattdessen ist ein angemessener Unkostenbeitrag vorzusehen. Zur effizienten Bekämpfung von Rechtsmissbrauch ist die Regelung überdies dahingehend auszugestalten, dass – innerhalb des Anwendungsbereichs von Rechtsmissbrauch – bei besonders aufwendigen Verfahren nach vorgängiger Abmahnung der betroffenen Person kein maximales Kostendach mehr gilt, sondern über den angemessenen Unkostenbeitrag hinaus die effektiven Kosten geltend gemacht werden dürfen. Dies ist mit rechtsstaatlichen Grundsätzen durchaus vereinbar, muss es doch darum gehen, den Auskunftspflichtigen vor uferlosem Aufwand aufgrund von klarem Rechtsmissbrauch zu schützen. In der Formulierung von Art. 20 Abs. 1 VE-DSG ist deshalb das Wort «**kostenlos» ersatzlos zu streichen** (vgl. im Übrigen zu Art. 21 VE-DSG).

				Alternativ wäre analog Art. 12 Abs. 5 Bst. a EU-DSGVO dem Bundesrat die Kompetenz einzuräumen, die Ausnahmen der Kostenlosigkeit auf Verordnungsstufe festlegen zu können. Ohne diese Ermächtigung können keine Ausnahmebestimmungen Eingang in die Verordnung finden (vgl. zum Rechtsmissbrauch und den Verfahrenskosten ferner unten zu Art. 21 VE-DSG). Der **Missbrauch des Auskunftsrechts**, namentlich die **zweckentfremdete Nutzung zur Beweismittelausforschung,** ist heute an der Tagesordnung und belastet die Unternehmen. Da der Herausgabeanspruch nach VE-DSG neu auch während Gerichtsverfahren gelten soll, dürfte der Trend zu Missbräuchen noch weiter zunehmen. Deshalb ist das Auskunftsrecht so anzupassen, dass es für die (datenschutzfremde) Beweismittelausforschung nicht mehr interessant ist, z.B. indem der Auskunftspflichtige wählen kann, die Auskunft nicht mehr in Form einer Kopie an den Auskunftssuchenden zu erstatten, sondern an eine **dritte Stelle**, welche die Verletzung des Datenschutzes stellvertretend prüft oder wo die Unterlagen eingesehen, aber nicht mitgenommen werden können. Alternativ wäre auch möglich, dass die betroffene Person ihr Interesse bei der Auskunftsanfrage darlegen muss oder die Schwelle zur Annahme eines Missbrauchs des Anfragenden gesenkt wird. Schliesslich fordern wir zur Eindämmung des Missbrauchs und um die verfahrensrechtlichen Regeln gemäss den einschlägigen Verfahrensordnungen wie z.B. der ZPO nicht zu verwässern, die **Wiedereinführung der Regel von Art. 2 Abs. 2 Bst. c DSG** (Nichtanwendbarkeit des DSG auf hängige Zivilprozesse und andere Verfahren). Ohne diese Regelung stünde das neue DSG im Widerspruch zum austarierten System der Mitwirkungspflichten und Verweigerungsrechte der Zivil- und Strafprozessordnung (vgl. Art. 160 ff. ZPO und Art. 157 ff. StPO). Während eines hängigen Zivil- und Strafverfahrens darf kein Auskunftsrecht bestehen. Vgl. dazu schon vorne zu Art. 2 Abs. 3 VE-DSG.
DSG	20	2	a	Aus systematischen Gründen ist – wie bereits bei Art. 13 Abs. 2 Bst. a bzw. Abs. 4 VE-DSG erwähnt – statt von «Identität» besser von «Name» und Kontaktdaten des Verantwortlichen bzw. des Auftragsdatenbearbeiters zu sprechen.
DSG	20	2	b	Wir empfehlen entsprechend bewährtem Auskunftsmechanismus die Präzisierung, dass die Information nur die Kategorien der bearbeiteten Personendaten beinhaltet. Dies entspricht Art. 15 Bst. b EU-DSGVO. Darüber hinauszugehen hiesse, einen mit Blick auf das gesetzgeberische Ziel der Äquivalenz unnötigen und kontraproduktiven Swiss Finish zu setzen. Anpassungsvorschlag (Ergänzung unterstrichen):

				Die Kategorien der bearbeiteten Personendaten
DSG	20	2	e	Die geforderte Information über das Vorliegen einer automatischen Einzelfallentscheidung darf hier, im Rahmen der allgemeinen Auskunftspflicht, nicht eine detaillierte Auflistung aller in der Vergangenheit ausgeführten automatischen Einzelfallentscheidungen beinhalten. Vielmehr ist hier bloss ein allgemeiner Hinweis notwendig, in welchen Bereichen bzw. zu welchen Themen gegebenenfalls automatische Einzelfallentscheidungen erfolgen. Andernfalls ergäbe sich im Rahmen von Art. 20 eine unübersichtliche Vermischung des allgemeinen Auskunftsanspruchs mit individueller Information zu einem konkreten Fall. Letzteres hätte, wenn überhaupt, losgelöst vom allgemeinen Auskunftsrechts unter Art. 15 VE-DSG zu geschehen (vgl. nachstehend zu Art. 20 Abs. 3 VE-DSG u. oben zu Art. 15 u. 20 VE-DSG).
DSG	20	2	f	Wir erachten es als ausreichend, wenn die Herkunft der Personendaten dann angegeben werden muss, wenn die Daten nicht bei der betroffenen Person selbst erhoben wurden. Dies entspricht Art. 15 Abs. 1 Bst. g EU-DSGVO. Anpassungsvorschlag (Ergänzungen unterstrichen): *Die verfügbaren Informationen über die Herkunft der Personendaten**,** falls diese nicht bei der betroffenen Person erhoben wurden*
DSG	20	2	g	«Empfänger» der Daten schliesst auch Auftragsdatenbearbeiter ein. Es ist nicht praktikabel und kann operativ nicht sichergestellt werden, sämtliche Auftragsdatenbearbeiter inkl. Identität und Kontaktdaten zu nennen (vgl. auch EU-DSGVO, wonach in Art. 15.1.b nur die Angabe von Kategorien von Empfängern verlangt wird). Anpassungsvorschlag: *Gegebenenfalls die Informationen nach Art. 13 Abs. 2 Buchstabe d (neu) und Abs. 3 ~~und 4~~*.
DSG	20	3		Der von Art. 20 Abs. 3 Halbsatz 2 VE-DSG geforderte Umfang des Auskunftsrechts (Informationen über Ergebnis, Zustandekommen und Auswirkungen der Entscheidung) ist mit Blick auf die anderweitig im VE-DSG bereits bestehenden weitreichenden Informationspflichten weder sinnvoll noch nötig und produziert ohne Mehrwert (z.B. in Form von mehr Transparenz) lediglich einen **unnötigen zusätzlichen**

				Administrativaufwand. Eine derart weitgehende Begründungs- bzw. Rechtfertigungspflicht ist datenschutzrechtlich nicht zu rechtfertigen. Sie würde ausserdem zwangsläufig zu einer Offenlegung von Geschäftsgeheimnissen z.B. in Form von internen Entscheid- und Ablaufverfahren führen. Die Regelung würde auch zu Unrecht eine **Vermischung des allgemeinen Auskunftsrechts mit individuellen Auskünften zu Einzelfallentscheidungen** produzieren. Eine gestützt auf Art. 20 VE-DSG erteilte allgemeine Auskunft hat in allgemeiner, übersichtlicher und leicht verständlichen Form den Anforderungen an die Auskunftspflicht zu genügen. Solche allgemeinen Auskünfte dürfen deshalb nicht mit einer Auflistung sämtlicher in der Vergangenheit durchgeführten individuellen Entscheidungen wie z.B. automatisierten Einzelfallentscheidungen ergänzt werden. Dies würde den Rahmen einer vernünftigen Auskunftserteilung sprengen und wäre auch für den Adressaten nicht mehr leicht verständlich, sondern im Gegenteil verwirrend. Deshalb ist Abs. 3 von Art. 20 VE-DSG hier systematisch falsch zugeordnet und gehört – wenn schon – zur gesamtheitlichen Regelung von Art. 15 VE-DSG. Darüber hinaus ist aber ein vom allgemeinen Auskunftsrecht losgelöstes individuelles Auskunftsrecht mit Bezug auf Ergebnis, Zustandekommen und Auswirkungen jeder Entscheidung generell abzulehnen. Die Auskunftspflicht würde damit erheblich ausgeweitet, wäre entsprechend massiv aufwendiger als bisher, ohne dass damit ein besserer Schutz der betroffenen Personen erreicht würde. Sehr viele Entscheidungen liegen im Rahmen dessen, was für die betroffenen Personen ohne weiteres erkennbar ist (vgl. Art. 4 Abs. 3 VE-DSG). Soweit eine Informationspflicht vorgeschrieben ist, muss diese auch genügen. Gestützt auf eine **angemessene Information** kann jede Person eigenverantwortlich entscheiden, ob sie die vorgeschlagene Form der Entscheidung akzeptieren will oder nicht. Die vom VE-DSG vorgeschlagene Regelung geht sodann klar über den von den EU-Anforderungen gesetzten Rahmen hinaus (vgl. Art. 15 Abs. 1 Bst. h EU-DSGVO). Dies stellt einen mit Blick auf die Äquivalenz unnötigen und kontraproduktiven Swiss Finish dar, der abzulehnen ist. Zusammenfassend ist die Regelung von Art. 20 Abs. 3 VE-DSG zu streichen und stattdessen in die Regelung von Art. 15 DSG zu integrieren. Auch diese Integration muss sich aber an die vorstehend und überdies zu Art. 15 VE-DSG skizzierten Grundsätze halten und sich insbesondere auf eine sehr generelle Darlegung der Funktionsweise automatisierter Einzelentscheide beschränken.
DSG	20	5		Vgl. die Ausführungen zu Art. 7 VE-DSG. Anpassungsvorschlag:

				Lässt der Verantwortliche Personendaten von einem Auftragsdatenbearbeiter bearbeiten, so bleibt er auskunftspflichtig. ~~Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat.~~
DSG	20	6		Wir empfehlen, an dieser Stelle ausdrücklich zu erwähnen, dass es sich beim Auskunftsrecht um ein subjektives höchstpersönliches Recht handelt.
DSG	20^{bis} (neu)			Die Ausnahmetatbestände von Art. 21 VE-DSG sind zu eng formuliert und inkonsistent. Die müssen in nachfolgendem Sinn **präzisiert und erweitert werden**: So ist beispielsweise nicht einzusehen, weshalb die Informationspflicht bei Unmöglichkeit und Unzumutbarkeit nur entfallen soll, soweit der Verantwortliche die betreffenden Daten nicht Dritten bekannt gibt (Art. 14 Abs. 4 Bst. a VE-DSG). Gleichwohl ist die Informationspflicht aber dann nicht nachzuholen, wenn dies nicht unmöglich oder unzumutbar ist (Art. 14 Abs. 5 VE-DSG). Richtigerweise muss die Informationspflicht immer entfallen, wenn die Information nicht möglich oder unzumutbar ist, wie es auch die EU-DSGVO vorsieht (Art. 12 Abs. 5 Bst. b EU-DSGVO). Dies gilt umso mehr, als das Auskunftsrecht neu bei jeder Datenbearbeitung greift. Insbesondere wird es keine Beschränkung mehr auf Datensammlungen geben. Nicht nachvollziehbar ist auch, weshalb die Informationspflicht nach gesetzlicher Vorschrift nur bei indirekter Beschaffung durch Dritte entfallen soll (Art. 14 Abs. 2 Bst. a VE-DSG). Umso mehr muss die Informationspflicht bei direkter Beschaffung entfallen. Dem Auskunftsverpflichteten muss sodann nach allgemeinen Rechtsgrundsätzen generell das Recht zustehen, das Auskunftsrecht unter Berufung überwiegender eigener Interessen einzuschränken oder sogar zu verweigern. Um dieser Regel griffige Konturen zu verleihen, sind – ohne Anspruch auf Vollständigkeit – typische Fallgruppen direkt im Gesetz aufzuführen. Das datenschutzrechtliche Auskunftsrecht dient der **Beseitigung eines allfälligen Informationsgefälles** zwischen betroffener Person und Auskunftspflichtigem. Die datenschutzrechtliche Begründung für das Auskunftsrecht fokussiert somit auf diejenigen Daten, welche die betroffene Person gar nicht kennt und aufgrund aller Umstände, z.B. mangels Erkennbarkeit (vgl. Art. 4 Abs. 3 u. Art. 20 Abs. 2 Satz 1 VE-DSG), vernünftigerweise auch gar nicht kennen kann. Naturgemäss nicht im Fokus sind demzufolge Daten, welche die betroffene Person bereits kennt bzw. erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen aller Art. Dies ist schon deshalb richtig, weil es nicht Aufgabe des

				Auskunftspflichtigen sein kann, einer betroffenen Partei wiederholt immer wieder und sogar unter Strafandrohung dieselben Daten liefern zu müssen, nur weil die betroffene Person z.B. den Aufwand sparen will, diese bereits erhaltenen Daten z.B. in Form von Verträgen bei sich selbst in vernünftiger Form aufzubewahren (Werner Wyss, a.a.O., N 11.46). Ebenfalls nicht herauszugeben sind Daten, welche aufgrund gesetzlicher Pflichten zu erheben und/oder aus bestimmten Gründen der betroffenen Person nicht bekannt gegeben werden dürfen, z.B. wegen Vereitelungs- oder Kollusionsgefahr in Zusammenhang mit Abklärungen zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption. Selbstredend darf das datenschutzrechtliche Auskunftsrecht auch nicht dazu führen, dass – ebenfalls rechtlich geschützte – Geschäftsgeheimnisse (vgl. Art. 162 StGB) herausgegeben werden müssen. Nicht herausgabepflichtig sind überdies rein intern bearbeitete Daten. Ein Auskunftsbegehren erfasst sachlogisch immer nur Daten über die antragstellende betroffene Person selbst. Nicht herauszugeben sind deshalb sämtliche Daten, welche Drittpersonen betreffen. Andernfalls würden mit der Datenherausgabe datenschutzrechtliche Ansprüche Dritter verletzt. Können solche Daten über Dritte nicht von den Daten über die betroffene Person getrennt werden, sind erstere z.B. mittels Schwärzung unkenntlich zu machen. Der Auskunftsverpflichtete ist auch vor Auskunftsbegehren zu schützen, welchen klarer Rechtsmissbrauch zu Grunde liegt (vgl. bereits oben zu Art. 20 Abs. 1 VE-DSG). Typische Fallgruppen klar rechtsmissbräuchlicher Geltendmachung des Auskunftsrechts sind aus Gründen der Rechtssicherheit direkt im Gesetzestext aufzuführen, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder die exzessive Geltendmachung des Auskunftsrechts mit häufiger Wiederholung, welche sachlich nicht nachvollziehbar ist. Es existiert im Vorentwurf kein pauschales Recht, die Herausgabe der Kommunikation zwischen der Bank und einem extern mandatierten Anwalt zu verweigern. Wichtig ist in diesem Zusammenhang, dass das Unternehmen aus rechtsstaatlichen Gründen nicht verpflichtet werden darf, interne Abklärungen zur Risikolage und zu den Prozesschancen im Vorfeld eines Prozesses herausgeben zu müssen, gehören solche Abklärungen doch zum Geschäftsgeheimnis eines jeden Unternehmens. Dies betrifft im Bankbe-

				reich etwa die Korrespondenz zwischen Banken und Rechtsanwälten oder Steuer- und Unternehmensberatern. Mit dieser Ausnahmeregelung werden verpönte «fishing expeditions» verhindert. Dies ist rechtsstaatlich mit allen Mitteln zu fördern so auch im Datenschutzrecht. Unter dem Geschäftsgeheimnis verstehen wir Tatsachen, die weder offenkundig noch allgemein zugänglich sind. Die Bank muss sodann ein Interesse und den Willen haben, diese Tatsachen geheim zu halten. Zielführend ist es deshalb, direkt in einem neuen Art. 20bis VE-DSG aufzuführen, dass solche Daten der vorstehend skizzierten Art nicht herauszugeben sind. Auch in der EU-DSGVO finden sich solche Ausnahmen und Einschränkungen. Zusammenfassend handelt es sich insbesondere um nachfolgend aufgeführte Daten: Formulierungsvorschlag für Art. 20bis VE-DSG (neu): *Nicht der Herausgabepflicht unterstehen folgende Datenkategorien:* *a) Daten, welche die betroffene Person bereits erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen;* *b) Aufgrund einer gesetzlichen Pflicht bearbeitete Daten, z.B. zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption;* *c) Daten, welche vom Auskunftspflichtigen als Geschäftsgeheimnisse qualifiziert werden;* *d) Rein intern bearbeitete Daten;* *e) Daten über Drittpersonen;* *f) Unter rechtsmissbräuchlichen Umständen herausverlangte Daten, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder mit häufiger, sachlich nicht nachvollziehbarer Wiederholung.* *g) Unterlagen aus dem Verkehr des Verantwortlichen mit einem Anwalt oder einem anderen beauftragten Dienstleister wie etwa Steuer- oder Unternehmensberater.*
DSG	21			Unter dem Vorentwurf (Art. 21 Abs. 1 i. V. m. Art. 14 Abs. 4 Bst. a VE-DSG) wie auch dem geltenden Recht (Art. 9 Abs. 4 DSG) ist es beispielsweise nicht möglich, die Auskunft bei einem überwiegenden

				Interesse der Bank zu verweigern, wenn die Personendaten einem Dritten (z.B. FINMA oder mandatierter Rechtsanwalt) weitergegeben wurden. Die fehlende Datenweitergabe an Dritte darf nicht Voraussetzung für die Auskunftsverweigerung sein, sondern ist in Art. 14 Abs. 4 Bst. a VE-DSG zu streichen. Dies betrifft etwa Fälle von Streitigkeiten zwischen Bank und einem Kunden. Wenn in solchen Fällen die Bank einen externen Rechtsanwalt mandatiert ein Gutachten zu erstellen, muss sie dieses Gutachten allenfalls in einem späteren Zivilprozess publik machen, denn dabei wurden ja klarerweise Daten an Dritte weitergegeben.
DSG	21	3 (neu)		Mit Blick auf die oben dargelegten Risiken des Missbrauchs des Auskunftsrechts, namentlich die **zweckentfremdete Nutzung zur Beweismittelausforschung**, muss ein effektiver **Mechanismus gegen solchen Missbrauch** vorgesehen werden, welcher das Auskunftsrecht für die (datenschutzfremde) Beweismittelausforschung nicht mehr interessant macht. Wir empfehlen, eine in der Praxis bewährte Vorgehensweise aus dem Bereich der Strafverfolgung anzuwenden (vgl. Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI); SR 361): Demnach kann der Verantwortliche bei begründetem Verdacht auf Missbrauch die herauszugebenden Personendaten einem Dritten (bspw. dem EDÖB) übergeben. Dieser würde anstelle des Gesuchstellers die Einhaltung bzw. Verletzung des Datenschutzes prüfen und sein Prüfergebnis in Form einer anfechtbaren Verfügung vorlegen (vgl. analoge Regelung in Art. 8 Abs. 2 BPI). Formulierungsvorschlag für Art. 21 Abs. 3 (neu): *Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche* *a) entweder ein angemessenes Entgelt verlangen, bei dem die Aufwandkosten für den Aufwand von Unterrichtung, Mitteilung oder Durchführung der beantragten Massnahme berücksichtigt werden, oder* *b) sich weigern, aufgrund des Antrags tätig zu werden.* (Eine analoge Formulierung drängt sich überdies auch bei Art. 14 in einem neuen Abs. 6 auf, vgl. oben). Alternativ könnte eine Kostenregelung eingeführt werden, die sich bspw. am Rechtsschutzinteresse des Gesuchstellers orientiert. Falls datenschutzfremde Interessen überwiegen, könnte eine höhere Gebühr verlangt werden; im umgekehrten Fall wäre eine tiefere Gebühr angezeigt (vgl. zu den Kosten einer Auskunft ferner oben zu Art. 20 Abs. 1 VE-DSG).

DSG	23	1	d	Aufgrund der richtigen Neukonzeption ist nur das **elektronische Profiling gesamtheitlich in Art. 15 VE-DSG** zu regeln. Demzufolge ist hier Abs. 1 Bst. d von Art. 23 VE-DSG ersatzlos zu streichen (vgl. oben zu Art. 3 Bst. f. u. Art. 15 VE-DSG).
DSG	23	2	d	Die Relevanz von Profiling sollte wie in der EU-DSGVO auf automatisierte Einzelentscheidungen beschränkt werden. Zudem ist das elektronische Profiling gesamtheitlich in Art. 15 VE-DSG zu regeln. Wir beantragen die **ersatzlose Streichung dieses Swiss Finish.**
DSG	24	1		Die Rechtfertigung durch «Gesetz» ist weiter zu definieren; andernfalls besteht ein Ungleichgewicht zwischen datenschutzrechtlichen und sonstigen rechtlichen Pflichten, welche auf derselben Stufe stehen müssen. Anpassungsvorschlag (Ergänzungen unterstrichen): *Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse ~~oder durch Gesetz~~ gerechtfertigt ist <u>oder auf rechtlichen Pflichten beruht</u>.*
DSG	24	2		Der Begriff «möglicherweise» ist mangels Aussagekraft und Mehrwert unnötig, demzufolge in Gesetzestexten auch gänzlich unüblich und deshalb ersatzlos zu streichen.
DSG	24	2	a	Zur Herstellung eines in sich stimmigen Gesamtkonzepts ist hier dieselbe Ergänzung anzubringen («*oder einer Person, zu deren Gunsten oder in deren Interesse der Vertrag abgeschlossen wird*»), wie sie auch unter Art. 6 Abs. 1 Bst. b VE-DSG notwendig ist (vgl. zur Begründung im Einzelnen dort).
DSG	24	2	c	Die Einschränkung gemäss Art. 24 Abs. 2 Bst. c Ziff. 1 VE-DSG ist nicht sachgerecht und sollte gestrichen werden. Sie verkennt, dass bspw. Massnahmen der sozialen Hilfe (Art. 3 Bst. c Ziff. 6 VE-DSG) von zentraler Bedeutung für die Beurteilung der Kreditwürdigkeit sein können. Ein Verzicht darauf würde zu Fehlbewertungen führen, was nicht im Interesse der betroffenen Person sein kann.
DSG	24	2	g (neu)	Schliesslich ist mit Art. 24 Abs. 2 Bst. g (neu) VE-DSG ein Rechtfertigungsgrund zu ergänzen, welcher den Einsatz neuer Technologien (insbesondere Profiling) zur Steigerung der Sicherheit bzw. der Prävention von Straftaten gegen das Vermögen der betroffenen Person ermöglichen würde.

				Formulierungsvorschlag für Art. 24 Abs. 2 Bst. g VE-DSG (neu): *die Daten zur Erhöhung der Sicherheit und Vermeidung von erheblichen Nachteilen für die betroffene Person bearbeitet werden, wofür sie auch Profiling durchführen kann.*
DSG	25	1	c	Wie bereits oben im Zusammenhang mit Art. 4 Abs. 4 und 5 VE-DSG (Grundsätze) erwähnt, können zwingende gesetzliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter der Vernichtung oder Löschung von Personendaten entgegenstehen (vgl. obenstehende Ausführungen zu Art. 4 VE-DSG). Anpassungsvorschlag (Ergänzungen unterstrichen): *Personendaten berichtigt werden; ~~, gelöscht oder vernichtet werden~~.*
DSG	25	1	d (neu)	Vgl. die Ausführungen zu Art. 25 Abs. 1 Bst. c. Formulierungsvorschlag für Art. 25 Abs. 1 Bst. d VE-DSG (neu): *Personendaten gelöscht oder vernichtet werden, sofern zwingende gesetzliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter dem nicht entgegenstehen*
DSG	25	3		Vgl. Ausführungen zu Art. 25 Abs. 1 Bst. c. Anpassungsvorschlag (Ergänzungen unterstrichen): *Die klagende Partei kann zudem verlangen, dass die Vernichtung, sofern zwingende gesetzliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter dem nicht entgegenstehen, die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.*
DSG	38	1		Eine Amtszeitbeschränkung ist eine in der Schweiz unübliche Praxis mit fragwürdigem Nutzen. Wir beantragen die ersatzlose Streichung dieser Bestimmung.

DSG	39	1		Es wird beantragt, die Formulierung «*Mitglied (…) der Verwaltung*» durch «*Mitglied (…) des Verwaltungsrats*» zu ersetzen. Damit wird sichergestellt, dass unter Mitglied der Verwaltung nicht die Verwaltung als Institution, sondern das oberste Exekutivorgan einer Gesellschaft verstanden wird. Anpassungsvorschlag (Ergänzungen unterstrichen): *Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, ~~der Verwaltung~~ des Verwaltungsrats, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig werden*
DSG	40 ff.			Die Regeln über die Rechtsprechung sind entsprechend unseren Ausführungen zu Art. 50 ff. VE-DSG (Sanktionen) anzupassen. Die Kompetenzen des EDÖB sind auf die derzeitigen Kompetenzen gemäss geltendem DSG zu beschränken. Weitergehende Kompetenzen müssen die von uns unter Art. 50 ff. VE-DSG vorgeschlagenen zusätzlichen Verwaltungsbehörde übertragen werden.
DSG	41	1		Unabhängig vom von uns vorgeschlagenen Konzept der verwaltungsinternen Gewaltenteilung (vgl. unten zu Art. 50 ff. VE-DSG) gehen die vorgesehenen Eingriffsrechte des EDÖB viel zu weit. Es darf keine Überprüfung ohne konkreten Anlass bzw. vorsorgliche Massnahmen geben. Der generelle Entzug einer aufschiebenden Wirkung oder einer Löschungsanordnung muss Sache der Gerichte bleiben. Die Einschränkung des geltenden DSG, wonach der EDÖB nur dann eine Untersuchung von sich aus durchführen kann, wenn eine grössere Zahl von Personen betroffen ist, müsste in Art. 41 Abs. 1 VE-DSG wiederaufgenommen werden. Das Verfahren vor dem Beauftragten ist ein öffentlich-rechtliches und daher auch nicht geeignet und auch nicht dazu vorgesehen, um Ansprüche aus der Persönlichkeitsverletzung geltend zu machen. Dafür muss der zivilrechtliche Weg beschritten werden. Folglich ist es auch nicht sachgerecht, dass jede Datenschutzverletzung untersucht wird. Dies würde sowohl beim EDÖB als auch beim Untersuchten unnötig wertvolle Ressourcen binden. Im Sinne der Verhältnismässigkeit sollte daher eine Untersuchung nur in schweren Fällen stattfinden. Anpassungsvorschlag (Ergänzungen unterstrichen):

				Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung ~~gegen die Datenschutzvorschriften verstossen~~ die Persönlichkeit einer grösseren Anzahl von Personen verletzen könnte (Systemfehler)
DSG	41	3		Im Unterschied zur EU-DSGVO räumt der VE-DSG dem Beauftragen umfangreiche Ermittlungs- und Eingriffsbefugnisse ein. Dieser Swiss Finish ist abzulehnen. Diese Zwangsmassnahmen führen ausserdem zu Kompetenzkonflikten, wenn gleichzeitig eine Strafuntersuchung stattfindet. Aus der Sicht der Verhältnismässigkeit sollte daher nur derjenige über Zwangsmittel verfügen, der das Strafverfahren führt. Im Übrigen unterscheidet sich die Untersuchung gemäss DSG genau darin von jener gemäss KG. Im Kartellrecht ist es die Verwaltungsbehörde, welche das «Strafverfahren» führt und die Sanktionen ausspricht. Im reinen Verwaltungsverfahren besteht aber für spezialgesetzliche Untersuchungsbefugnisse kein Raum. Es ist ferner nicht einzusehen, weshalb für das Verfahren beim EDÖB nicht einfach wie im Verwaltungsrecht üblich, das VwVG anwendbar sein soll, wie das in Art. 44 ohnehin vorgesehen ist. Zudem ist fraglich, ob die Bestimmung im Einklang mit strafrechtlichen, untersuchungsrechtlichen und staatsrechtlichen Grundsätzen steht. Insbesondere ist unklar, wie vorzugehen ist, wenn ein gesetzliches/regulatorisches Mitwirkungsverweigerungsrecht und/oder Recht auf Aussageverweigerung besteht. Bei der Inspizierung von Räumlichkeiten müssten dieselben Voraussetzungen eingehalten werden, wie dies heute bei Hausdurchsuchungen der Fall ist. Anpassungsvorschlag (Ergänzungen unterstrichen): *Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte trotz angesetzter angemessener Frist die notwendigen ~~vergeblich versucht,~~ Auskünfte und Unterlagen nicht erhalten ~~einzuholen~~, so kann der Beauftragte im Rahmen einer Untersuchung, nach Erlass einer entsprechenden anfechtbaren Verfügung:* *a. ~~ohne Vorankündigung~~ Räumlichkeiten inspizieren;*
DSG	41	4		Diese Regelung ist zu präzisieren, zumal nicht klar ist, welche Überprüfungsbefugnisse der Beauftragte ausserhalb einer Untersuchung haben wird.

DSG	41	5		Wir regen an, in Art. 41 Abs. 5 VE-DSG auch den Interessen der angezeigten Person Rechnung zu tragen. Insbesondere soll die angezeigte Person vom Beauftragten über das weitere Vorgehen und das Ergebnis einer allfälligen Untersuchung informiert werden. Anpassungsvorschlag (Ergänzungen unterstrichen): *Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung. Der Beauftragte hat dabei die Interessen der angezeigten Person zu berücksichtigen. Zudem hat der Beauftragte auch die angezeigte Person über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung zu informieren.*
DSG	42			Diese Bestimmung ist **ersatzlos zu streichen**. Die geltende Regelung, wonach der EDÖB beim Bundesverwaltungsgericht eine entsprechende Massnahme beantragen muss, hat sich bewährt und sollte nicht ohne Not geändert werden. Auch hier besteht kein Erfordernis über die allgemeinen Regeln des VwVG hinauszugehen. Zudem bleibt hier auch zu erwähnen, dass die betroffenen Personen auch auf zivilprozessualem Weg die Möglichkeit haben, entsprechende Massnahmen einzuleiten (vgl. Art. 28 ff. ZGB).
DSG	43			Der Beauftragte sollte diese Massnahmen nur ergreifen können, wenn er zuvor den Verantwortlichen beraten hat, es aber dennoch zu einer Verletzung kommt (im Sinne einer vorgängigen Abmahnung); i.V.m. Art. 44 VE-DSG haben die betroffenen Parteien Anspruch auf rechtliches Gehör (Art. 29 ff. VwVG), welcher hier zu gewähren ist. Wie bereits oben im Zusammenhang mit Art. 4 Abs. 4 und 5 VE-DSG (Grundsätze) und Art. 25 Abs. 3 VE-DSG (Rechtsansprüche) erwähnt, können zudem zwingende gesetzliche Vorschriften (z.B. Art. 958 f. OR oder Art. 7 GwG) oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter der Vernichtung oder Löschung von Personendaten entgegenstehen (vgl. obenstehende Ausführungen zu Art. 4 und Art. 25 VE-DSG). Anpassungsvorschlag (Ergänzungen unterstrichen): *Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden, sofern zwingende gesetzliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder*

				aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter der Vernichtung nicht entgegenstehen.
DSG	46 f.			**Zusammenarbeit mit ausländischen Aufsichtsbehörden nach EU-DSGVO**: Gemäss EU-DSGVO sind Datenverantwortliche von Drittstaaten, die jedoch trotzdem der EU-Datenschutzgrundverordnung unterstehen, grundsätzlich zur Zusammenarbeit mit den Europäischen Aufsichtsbehörden verpflichtet. Ob eine Zusammenarbeit allerdings aus strafrechtlicher Sicht überhaupt zulässig ist, ist unklar (Art. 271 StGB – Verbotene Handlungen für einen ausländischen Staat). Hier wäre es wünschenswert, die Möglichkeiten der Amtshilfe (via den EDÖB bzw. die von uns unter Art. 50 ff. VE-DSG geforderte neue Verwaltungsbehörde) in das Gesetz zu übernehmen. Dann könnten Informationen über den Amtshilfeweg an die ausländischen Behörden übermittelt werden. Ausserdem besteht bereits durch das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates eine Rechtsgrundlage, die den Weg der Amtshilfe und den Datenschutz entsprechend regelt (Art. 13 des Übereinkommens).
DSG	50 ff.			Art. 50 ff. VE-DSG enthalten eigentliche Strafbestimmungen, im Gegensatz zu den entsprechenden europäischen Regelungen, die Verwaltungssanktionen vorsehen. Bereits damit ist die mit dieser Gesetzesrevision bezweckte Äquivalenz gefährdet, da Verwaltungsverfahren eine effizientere Sanktionierung ermöglichen. Ein Wechsel vom Strafrecht hin zum Bundesverwaltungsrecht schafft eine rasche und kohärente Anwendung des Datenschutzgesetzes in der Praxis. Damit wird, wie bereits dargelegt, auf ein einheitliches und vor allem effizientes Verwaltungsverfahren hingewirkt. Verbleiben die Strafbestimmungen im Gesetz, so wird die Strafverfolgung automatisch an die Kantone delegiert. Damit ist kein einheitlicher Vollzug des Datenschutzgesetzes mehr möglich. Der Vollzug des Datenschutzrechtes in der Schweiz und damit auch die Sanktionierung von Verstössen ist aber klarerweise eine Bundesaufgabe. Bereits die bestehenden Strafbestimmungen im heutigen DSG haben nicht dazu beigetragen, die Vollstreckungspraxis des Datenschutzes zu vereinheitlichen. Es ist zudem ein Irrglaube, mit dem Abstützen auf das Strafrecht die Europäischen Vorgaben an den Datenschutz besser erfüllt zu haben. Dies führt zudem dazu, dass unter Strafrecht als Primat nicht die Unternehmen, sondern die einzelnen Individuen bestraft werden. Nach Art. 29 StGB setzt die strafrechtliche Haftung voraus, dass die betreffende natürliche Person (i) eine ihr obliegende Pflicht (ii) in einer der folgenden Eigenschaften verletzt hat:

				- als Organ oder Mitglied eines formellen (Bst. a) oder faktischen (Bst. d) Organs; - als Gesellschafter einer Personengesellschaft (Bst. b); - als Mitarbeiter mit selbständigen Entscheidungsbefugnissen im betreffenden Bereich (Bst. c). Der Kreis der von Strafe bedrohten Personen ist daher relativ weit gezogen. Ein Risiko strafrechtlicher Haftung hätten deshalb insbesondere - VR- und GL-Mitglieder der Gesellschaft; - VR- und GL-Mitglieder der Muttergesellschaft, falls sie bei der Tochter faktische Entscheidungskompetenzen in Anspruch nehmen; - Mitglieder einer Kollektivgesellschaft; - ggf. die für den Datenschutz eigenverantwortlichen Mitarbeiter im Rechtsdienst; - ggf. ein Compliance-Officer; - ggf. interne und externe Datenschutzbeauftragte. Gestützt auf die sehr offene Formulierung im VE-DSG wären aber letztlich sämtliche Mitarbeitenden von Strafsanktionen bedroht. Diese Tatsache, zusammen mit der extremen Unbestimmtheit der Straftatbestände (dazu unten), **führt zu einer durch nichts zu rechtfertigenden Bedrohung derjenigen Personen, die mit Personendaten umzugehen haben** – und zwar gerade derjenigen Personen, die unternehmensintern die Einhaltung des Datenschutzes sicherstellen müssen und die durch das Datenschutzrecht deshalb zu schützen sind. Dies insbesondere auch wegen der Tatsache, dass geschäftliche Datenbearbeitungen notwendigerweise täglich stattfinden müssen. In scharfem Gegensatz zu den allermeisten anderweitig implementierten Strafnormen betreffen diejenigen gemäss VE-DSG demzufolge alltägliche Situationen, denen die natürlichen Personen gar nicht ausweichen können. Zudem fällt ins Gewicht, dass das Datenschutzgesetz ausschliesslich geschäftliche Datenbearbeitungen erfasst (vgl. oben Vorbemerkung II), die natürlichen Personen als Mitarbeitende des Unternehmens somit gestützt auf die geschlossenen Arbeitsverträge für das Unternehmen handeln. Auch deshalb erscheint das Primat der Belangung der natürlichen Personen als nicht sachgerecht. Folgerichtig liegt der vom VE-DSG

				gewählte Ansatz auch nicht auf der Linie zahlreicher anderer Gesetze mit spezialgesetzlichen Strafnormen, welche konsequenterweise zu Recht das Primat des Unternehmens statuieren (vgl. z.B. KG, UWG, FMG u. BEHG). Eine solch flächendeckende Pönalisierung eines Grossteils der schweizerischen Arbeitnehmer wäre **verfassungswidrig und weltweit einmalig**. Das europäische Recht sieht Sanktionen lediglich auf Ebene der Unternehmen vor. Solche Sanktionen wären auch ein klar überschiessender und mit Blick auf die zu erreichende Äquivalenz unnötiger und kontraproduktiver Swiss Finish. **Viele Pflichten des VE-DSG und damit auch die daraus abgeleiteten strafrechtlichen Tatbestände gemäss Art. 50 ff. VE-DSG sind überdies zu wenig konkret.** Art. 50 ff. VE-DSG erfüllen damit die strafrechtsdogmatische, im Verfassungsrecht begründete Regel von «nulla poena sine lege (stricta, certa)» offensichtlich nicht. Nur wenn aufgrund der Regel klar ist, welches konkrete Verhalten gefordert ist bzw. welche Unterlassung eine Verletzung darstellt, ist eine Sanktionierung zulässig. Strafrechtlich sanktionierbar dürfen mit Blick auf die weitreichenden Folgen und auf den Verhältnismässigkeitsgrundsatz jedenfalls zum Vornherein nur solche Pflichten sein, die (i) eine wesentliche Verbesserung des Datenschutzes bei den betroffenen Personen sicherstellen wollen und – kumulativ – (ii) genügend präzis formuliert sind, damit der Verantwortliche bzw. dessen Mitarbeitende durch geeignete Handlungsweisen, Implementierung geeigneter Massnahmen, etc. tatsächlich verhindern können, je mit strafrechtlichen Vorwürfen konfrontiert zu werden. Offene Sachverhalte wie z.B. «Informationspflichten», «Dokumentationspflichten» oder «Auskunftspflichten» können die skizzierten Anforderungen per definitionem nicht erfüllen, weil sie mit einem zu grossen Ermessensspielraum versehen sind. Vollends problematisch ist es nach dem Gesagten, trotz offenen Sachverhalten sogar fahrlässige Handlungsweisen strafrechtlichen Sanktionen unterstellen zu wollen. Mit dem vorgeschlagenen Strafrechtspaket wären die gesamte Wirtschaft und insbesondere die einzelnen natürlichen Personen, die als Angestellte von Unternehmen täglich mit Personendaten umzugehen haben, zu Unrecht mit unabsehbaren strafrechtlichen Risiken belastet. Dies hätte wohl massivste, heute noch gar nicht überblickbare Auswirkungen auf den Wirtschaftsstandort Schweiz. Die Abwanderung zahlreicher Unternehmen ins Ausland wäre eine mögliche Folge. Mit alldem würde das krasse Gegenteil von Äquivalenz erreicht. Solche Szenarien stünden auch in krassem Gegensatz zu aktuellen Anstrengungen in Bundesbern, ausländische Anbieter z.B. unter dem Thema FinTech anzuziehen, um damit die Wettbewerbsfähigkeit des Wirtschaftsstandorts Schweiz zu sichern und zu verbessern.

				Wir fordern deshalb, auf Strafrechtsartikel grundsätzlich zu verzichten und stattdessen den Verwaltungsbehörden eine angemessene Sanktionskompetenz einzuräumen. Dies entspräche den europäischen Parallelbestimmungen. Es wäre insbesondere deshalb sachgerecht, weil das Strafrecht primär natürliche Personen erfasst und das Unternehmensstrafrecht systembedingt nur als zusätzliches «Auffangbecken» zum Tragen kommen soll (vgl. Art. 53 VE-DSG). Wegen der Komplexität vieler datenschutzrechtlicher Setups (z.B. grenzüberschreitende Sachverhalte, zunehmender Trend zu Arbeitsteilung, etc.) ist es aber nicht angemessen, für die Implementierung eines suboptimalen datenschutzrechtlichen Setups einzelne natürliche Personen verantwortlich zu machen, dies sogar in strafrechtlich relevanter Form mit für eine Privatperson völlig unverhältnismässigen Bussen-Ansätzen. Vielmehr ist es sachgerecht und fairer, wenn stattdessen das zuständige Unternehmen wegen Organisationsmängeln – um die es bei der Datenschutz-Compliance ja gerade geht – die Verantwortung übernimmt. Mit dem Wechsel zu verwaltungsrechtlichen, durch die Verwaltungsbehörden verhängten Sanktionen wäre Art. 43 VE-DSG analog zum Kartellgesetz (KG) auszugestalten, allerdings im Gegensatz zum KG wegen den unterschiedlichen in Frage stehenden Rechtsgütern mit einem wesentlich tieferen Höchstbetrag (z.B. CHF 1 Mio.; vgl. oben zu Art. 17 VE-DSG). Da solche Sanktionen – anders als im Strafrecht – primär auf das Unternehmen zielen, kann damit das vorstehend skizzierte zentrale Thema, die primäre Haftung natürlicher Personen zu verhindern, angemessen geregelt werden. Dieses **Verwaltungsverfahren** ist wie folgt auszugestalten: a) Bei Verstössen gegen Datenschutzbestimmungen richten sich die Sanktionen grundsätzlich mit dem **Anknüpfungspunkt von Organisationsmängeln** direkt gegen die **Unternehmen**. b) Der **EDÖB** bleibt im Wesentlichen auf seine bisherigen Kompetenzen gemäss geltendem DSG beschränkt; stellt der EDÖB bei seinen eigenen Untersuchungen im Sinne einer Vorselektion grobe Datenschutzverletzungen fest, hat er die Untersuchung an eine (neu zu schaffende) **Spruchbehörde (DSG-«Kommission»)** in einem anderen Departement wie z.B. im EDI zu übertragen, welcher Untersuchungs- und Spruchkompetenz und falls nötig Verordnungskompetenz zukommt. Damit wird ein **rechtsstaatliches System** geschaffen, welches sich an der funktionalen Aufteilung zwischen Strafuntersuchungsbehörden und Strafgerichten anlehnt. Der finanzielle Zusatzaufwand für die Schaffung dieser Kommission wird durch die Einsparung von Aufwand beim EDÖB selbst und bei kantonalen Strafbehörden mehr als wettgemacht.

				c) Zur Sicherstellung der verfassungsmässigen Verfahrensgarantien darf es bei solchen Verwaltungsverfahren **keine Mitwirkungspflicht des Unternehmens** geben. d) Gegen Entscheide der Spruchbehörde steht der **Weg ans Bundesverwaltungsgericht** als Rechtsmittelinstanz offen. e) **Maximale Sanktion** gegen ein Unternehmen ist – wie im VE-DSG vorgesehen – eine **Busse von CHF 500'000.** Dieses Sanktionsmass ist auch im Lichte internationaler Vorgaben ausreichend. Da bei DSG-Verletzungen alltägliche Datenbearbeitungen im Fokus stehen, welche typischerweise auch nur eine einzelne natürliche Person betreffen, verbieten sich insbesondere massiv höhere, i.d.R. umsatzbezogene Sanktionsansätze wie z.B. unter dem KG. Dort haben sanktionierte Unternehmen typischerweise jahrelang von kartellistischen Machenschaften finanziell massiv profitiert, was im Einzelfall höhere Bussen zu rechtfertigen vermag (zumal selbst diese höheren Bussen i.d.R. nur einen Teil des unrechtmässig erzielten Gewinns zurückholen). Unter dem DSG gibt es demgegenüber kaum Gewinn zu erzielen, weil die Datenbearbeitungen ohnehin stattfinden müssen. f) Lediglich **subsidiär** ist parallel zu oder anstatt einem gegen das Unternehmen gerichteten Verwaltungsverfahren eine strafrechtliche Verfolgung von **klar kriminellen Mitarbeitenden** möglich. Dies jedoch mit folgenden Beschränkungen: (i) Beschränkung der Delikte auf solche Handlungen, welche eine direkte Schädigung bei betroffenen Personen bewirken können; (ii) Strafbarkeit auf direkten Vorsatz beschränkt (sonst besteht das Risiko, dass auf Basis der Organisationspflichten des Unternehmens allzu schnell Eventualvorsatz «konstruiert» wird); und (iii) Recht zum Strafantrag nur für ein betroffenes Unternehmen. g) Generell sind die **Straftatbestände zu konkretisieren** und auf ein vernünftiges und mit den strafrechtlichen Prinzipien konformes Mass einzugrenzen, insb. durch (i) Streichung der Strafandrohung bei verweigerter Mitwirkung / Kooperation ab der zweiten Stufe des Verfahrens; (ii) Konkretisierung / Streichung der zu offen formulierten Tatbestände; (iii) Einführung einer Erheblichkeitsschwelle, welche sich z.B. an der Schwere der Persönlichkeitsverletzung (in quantitativer oder qualitativer Hinsicht) oder an der Höhe des entstandenen Schadens orientiert; zu einem schweren Verstoss gegen das Datenschutzgesetz gehört auch, dass die unbefugte Datenbearbeitung direkt vorsätzlich vorgenommen wurde; (iv) Verzicht auf die Pönalisierung von reinen Fahrlässigkeitsdelikten; und (v) Beschränkung des allgemeinen Berufsgeheimnisses auf Fälle, in

				denen der Geheimnisherr eine berechtigte Erwartung der Geheimhaltung hat (z.B. aufgrund eines Vertrages). Art. 35 DSG ist beizubehalten, eventualiter ist der Tatbestand mindestens auf das Niveau von Art. 321 StGB zu relativieren. h) Das Zusammenspiel der Pflicht, Datenschutzverstösse zu melden, mit der damit einhergehenden anschliessenden Bestrafung im Rahmen eines Strafverfahrens verstösst gegen das Selbstbelastungsverbot (nemo tenetur) und ist unfair, weil sie die korrekt handelnden Personen, welche ihren Meldepflichten nachkommen, dafür bestraft. Umgekehrt werden falsche Anreize gesetzt, denn andere Personen, welche bewusst die Meldepflicht nicht befolgen, können nach dem natürlichen Lauf der Dinge ernsthaft damit rechnen, dass der Fall nicht publik wird und sie demzufolge straffrei bleiben. Deshalb sollte ein kooperatives Verhalten im Sinne einer Schadensminderung gefördert werden. Dies muss durch einen gesetzlich anerkannten Katalog angemessener **Rechtfertigungsgründe** geschehen. Solche Fallgruppen fairer Rechtfertigungsgründe sind insb. (i) Einhaltung der Corporate Governance: Einhalten sämtlicher unternehmensinternen Regulative, Ausschöpfen der betriebsinternen Eskalationsleiter und Interventionsmöglichkeiten, Meldung eines möglichen Verstosses sowie kooperatives Verhalten gegenüber den Behörden; (ii) Handeln nach Treu und Glauben durch vernünftigen Umgang mit komplexen Regeln: Angemessene Umsetzung komplexer Verhältnisse (u.a. viele Beteiligte und grenzüberschreitende Verhältnisse) unter Berücksichtigung des «state of the art» und bei bestehender Rechtsunsicherheit; (iii) Wahrung berechtigter Interessen: Rechtfertigende Pflichtenkollision mit anderen zwingenden Rechtsregeln, welche in einer Güterabwägung im konkreten Fall überwogen haben. Beispielsweise unter Zeitdruck angewendete etablierte Notfallszenarien (BCM) im öffentlichen Interesse der Abwendung eines Unternehmenskonkurses (vgl. Notstand, Art. 17 StGB); (iv) Strafrechtliche Verfolgung eines Mitarbeiters: Eine Anzeige gegen einen direkt vorsätzlich handelnden Mitarbeiter durch das Unternehmen muss im Rahmen der Bestrafung des Unternehmens, insbesondere im Hinblick auf das Schuldprinzip, berücksichtigt werden; und (v) Aktive Schadensverminderung und damit die aktive Zusammenarbeit mit den Behörden im Falle einer Verletzung. Auch die von uns als Ersatz für Strafrechtstatbestände geforderten verwaltungsrechtlichen Sanktionen sind genügend präzis im weiter vorne skizzierten Sinn zu formulieren.

DSG	51	2		Absatz 2 sollte **ersatzlos gestrichen** werden, ansonsten könnte jeder Verantwortliche bei jedem Entscheid, der sich als nicht richtig herausstellt, bereits gebüsst werden. Dies würde zu einer Kriminalisierung sämtlicher Verantwortlichen führen.
DSG	51bis (neu)			In Anlehnung an Art. 83 Abs. 3 EU-DSGVO regen wir für den Eventualfall an, mit Art. 51bis VE-DSG einen neuen Artikel mit dem Titel «Konkurrenz» einzufügen. Formulierungsvorschlag: *Konkurrenz* *Hat eine private Person bei der gleichen oder bei miteinander verbundenen Datenbearbeitungsvorgängen vorsätzlich oder fahrlässig mehrere Bestimmungen dieses Gesetzes verletzt, so übersteigt der Gesamtbetrag der Busse nicht den Betrag der für die schwerwiegendste Verletzung vorgesehen ist.*
DSG	52			Die **Abgrenzung zu anderen gesetzlich geregelten Geheimhaltungspflichten** ist unklar. Unterschiedliche Regelungen in verschiedenen Gesetzen im Bereich strafrechtlich relevanter Handlungen schaffen Rechts*un*sicherheit und unnötige Abgrenzungs- und Auslegungsprobleme und widersprechen damit auch strafrechtlichen Grundprinzipien. Die Regelung strafrechtlicher Tatbestände auf solche, bereits grundsätzlich unklarer Regelungen ist verfassungsrechtlich unzulässig (Verletzung des Grundsatzes nulla poena sine lege stricta). Umso mehr ist Art. 52 VE-DSG zu streichen (vgl. oben zu Art. 50 ff. VE-DSG).
DSG	53			Es ist wichtig, dass diese Bestimmung, wenn schon, nicht als Kann-Vorschrift ausgestaltet ist, ansonsten es sehr schwierig sein wird, qualifizierte Personen zu finden, die sich für eine Anstellung unter solchen Bedingungen zur Verfügung stellen. Anpassungsvorschlag: *Übertretungen und Vergehen in Geschäftsbetrieben* *Von der Ermittlung der strafbaren Personen wird ~~kann~~ Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt.~~werden Busse 100 000 Franken nicht überschreitet und~~

				~~*die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären*~~
DSG	54			Da dies bereits in der Strafprozessordnung geregelt ist, ist diese Bestimmung jedenfalls obsolet und ersatzlos zu streichen.
DSG	55			Da dies bereits in Art. 109 des Strafgesetzbuches geregelt ist, ist diese Bestimmung jedenfalls obsolet und ersatzlos zu streichen.
DSG	59			Die Übergangsbestimmungen von Art. 59 VE-DSG beschränken sich auf die Regelungen von Art. 16, 18 u. 19 VE-DSG. In Tat und Wahrheit lässt sich der gegenüber dem bestehenden DSG wesentlich veränderte und mit zahlreichen veränderten bzw. neuen Pflichten ausgestattete VE-DSG nur im Zuge einer **umfassenden IT-gestützten Umstellung der gesamten internen Datenbearbeitungsprozesse** bewerkstelligen. Dies geht weit über Art. 16, 18 u. 19 VE-DSG hinaus und umfasst sämtliche geänderten oder neuen Pflichten und anderen, zur Strukturierung der rechtskonformen Datenbearbeitung notwendigen Regeln. Nur schon für einfache Umsetzungsprojekte sind auf der Zeitachse **zwischen Analyse, Entscheidfindung und IT-gestützter massengeschäftstauglicher Umsetzung erfahrungsgemäss rund zwei Jahre Übergangsfrist** notwendig. Mit Blick auf die **Komplexität des neuen VE-DSG** mit Bezug auf die zahlreichen zur rechtskonformen Umsetzung notwendigen Anpassungen an sämtlichen Datenbearbeitungsprozessen sind dafür **im Minimum drei Jahre** absolut zwingend.
DSG	59	b		Es ist kein Grund ersichtlich, weshalb vom gesetzgeberischen **Grundsatz der Nichtrückwirkung** abgewichen werden soll. Die Datenbearbeitungen bis zum Inkrafttreten des VE-DSG erfolgten rechtskonform auf Basis des aktuellen DSG und sämtlicher anderen anwendbaren Gesetze und wurden überdies auch von den zuständigen Prüfgesellschaften periodisch geprüft. Auch das aktuelle DSG statuiert bereits zahlreiche Informationspflichten. Auch die in Art. 18 u. 19 Bst. b VE-DSG neu formulierten Pflichten finden sich in anderer Systematik bereits im geltenden DSG. Deshalb erscheint eine Rückwirkung als Ausnahme von der Regel nicht angemessen. Die Rückwirkung würde in der praktischen Umsetzung zudem einen enormen Aufwand und überdies zahlreiche kaum lösbare Herausforderungen generieren. Bei langjährigen Kunden würde schlussendlich eine Information erheblichen Ausmasses generiert, welche die meisten Kunden überdies kaum mehr

				interessieren würde, weil z.B. die Datenbearbeitung viele Jahre zurückliegt, heute gar nicht mehr zur Anwendung kommt, u.ä. Sämtliche Kunden müssten – als Erben früherer Kunden – auch über längst zurückliegende Datenbearbeitungen informieren, welche nur schon wegen dem inzwischen verstorbenen Erblasser nach Jahr und Tag kaum mehr von Interesse sein dürften. Zahlreiche Informationen zur Wahrnehmung solcher nachträglichen Informationspflichten wären ohnehin nicht mehr vorhanden, weil sie inzwischen nach Ablauf der Archivierungs- und anderweitigen Aufbewahrungspflichten gar nicht mehr vorhanden sind. Die allermeisten betroffenen Personen würden solche nachträglichen Informationen mit einigem Erstaunen zur Kenntnis nehmen und könnten damit kaum etwas Vernünftiges anfangen, sondern wären eher verwirrt. Im dümmsten Fall würden sich zahlreiche Kunden und andere betroffene Personen auf der Basis der erhaltenen Informationen beim verantwortlichen Unternehmen melden und zusätzliche Fragen stellen. Der Aufwand für die Unternehmen wäre massiv, ohne dass damit ein wesentlicher datenschutzrechtlicher Mehrwert geschaffen würde. Nach dem Gesagten ist Art. 59 Bst. b VE-DSG **ersatzlos zu streichen** und die Systematik des verbleibenden Art. 59 VE-DSG anzupassen und als vollständiger Satz zu formulieren (da eine einzelne Bst. a keinen Sinn mehr macht).
GwG	34	2		Vgl. Anmerkungen zum unten vorgeschlagenen Art. 34bis. Anpassungsvorschlag (Ergänzungen unterstrichen): *Sie dürfen Daten aus diesen Datensammlungen nur an die FINMA, die Eidgenössische Spielbankenkommission, Selbstregulierungsorganisationen, die Meldestelle und Strafverfolgungsbehörden weitergeben. <u>Vorbehalten bleibt die Weitergabe an Zweigniederlassungen und innerhalb einer Finanzgruppe gemäss Artikel 34bis.</u>*
GwG	34bis (neu)			Die FINMA konkretisiert das per 2016 in Kraft getretene revidierte Geldwäschereigesetz sowie die entsprechende GwV-FINMA dahingehend, dass ein Finanzintermediär, der Zweigniederlassungen im Ausland besitzt oder der eine Finanzgruppe mit ausländischen Gesellschaften leitet, seine mit Geldwäscherei und Terrorismusfinanzierung verbundenen Rechts- und Reputationsrisiken global erfassen, begrenzen und überwachen muss (Art. 6 Abs. 1 GwV-FINMA). Art. 6 Abs. 2 Bst. a und b GwV-FINMA setzt bei der Pflicht zur gruppenweiten Erfassung, Begrenzung und Überwachung von Risiken

				im Bedarfsfall den Zugang der zuständigen Überwachungsorgane der Gruppe zu Informationen über einzelne Geschäftsbeziehungen voraus. Die Bestimmungen des Geldwäschereigesetzes sind daher dahingehend zu ergänzen, dass der Informationsaustausch innerhalb der Finanzgruppe im In- und Ausland zulässig ist, falls und soweit dieser zur Erfüllung der Pflichten aus dem GwG erforderlich ist. Dies entspricht auch der in Präambel (19) der EU-DSGVO festgehaltenen Bestimmung, wonach die Mitgliedstaaten Erlasse beschliessen können, welche die in der EU-DSGVO festgehaltenen Pflichten und Rechte beschränken, soweit dies zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung erforderlich und verhältnismässig ist. Formulierungsvorschlag: *Weitergabe an Zweigniederlassungen und innerhalb einer Finanzgruppe* *Sofern zur Erfüllung der in diesem Gesetz festgelegten Pflichten erforderlich, darf der Finanzintermediär, der Zweigniederlassungen besitzt oder Teil einer Finanzgruppe ist, Informationen an Zweigniederlassungen und andere Rechtseinheiten innerhalb der Finanzgruppe im In- und Ausland weitergeben. Davon eingeschlossen sind sämtliche für die globale Überwachung der Rechts- und Reputationsrisiken wesentlichen Informationen, inklusive Informationen über einzelne Geschäftsbeziehungen und Informationen aus Datensammlungen gemäss Art. 34.*
ZPO	20 99 113 114 243	d 3 2 2	d d g f d	Wir verlangen die ersatzlose Streichung der Änderungen in der ZPO. Betroffen davon sind die Gerichtsstandbestimmungen, Sicherheiten und Gerichtskosten. Als speziell stossend betrachten wir den Umstand, dass ein neuer Gerichtsstand für Datenschutzstreitigkeiten eingeführt wird. Weshalb im Rahmen der Datenschutzgesetzgebung die Streitwertgrenzen in der Zivilprozessordnung aufgehoben werden sollen ist uns ebenfalls nicht ersichtlich. Generell besteht kein sachlicher Grund, für Datenschutzbelange von den bewährten Regeln der ZPO abzuweichen. Letztere müssen aus Gründen von Klarheit und Übersichtlichkeit Grundregel bleiben. **Ausnahmen** davon sind nur für **zwingend notwendige Spezialsituationen** zuzugestehen. Solche liegen im Bereich Datenschutz nicht vor und werden dementsprechend im Erläuterungsbericht auch nicht angeführt.

Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Wir bedanken uns für die wohlwollende Prüfung unserer Bemerkungen und Anliegen. Für allfällige Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer Kantonalbanken

Hanspeter Hess
Direktor

Dr. Adrian Steiner
Leiter Public Affairs

SCHWEIZER MEDIEN
MÉDIAS SUISSES | STAMPA SVIZZERA | SWISS MEDIA

EINSCHREIBEN
Bundesamt für Justiz
Herr Jonas Amstutz
Bundesrain 20
CH-3003 Bern

Zürich, 3. April 2017
Vernehmlassung – Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Sehr geehrte Frau Bundesrätin Sommaruga,
sehr geehrte Damen und Herren

Der Verband SCHWEIZER MEDIEN (VSM) ist die Branchenorganisation der privaten schweizerischen Medienunternehmen. Zusammen mit den beiden Schwesterverbänden MÉDIAS SUISSES und STAMPA SVIZZERA setzt sich der VSM für die Wahrung der Interessen der privaten Medienunternehmen in der Schweiz ein.

Mit grossem Interesse haben wir vom Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz Kenntnis genommen. Gerne nehmen wir wie folgt Stellung:

I. Executive Summary

1 Das revidierte Datenschutzgesetz muss den Schweizer Unternehmen weiterhin Raum und Flexibilität bieten, um die Rechte der betroffenen Datensubjekte zu wahren und gleichzeitig ohne bürokratische Last wirtschaftlich sinnvoll agieren zu können.

2 Der Vorentwurf erreicht dieses Ziel nicht. Anstatt weiterhin auf das etablierte System der Selbstregulierung und eine risikobasierte Umsetzung der Vorgaben zu vertrauen, zeichnet sich der Vorentwurf durch eine, für ein Schweizer Gesetz äusserst untypische Starrheit und Überregulierung aus. Obschon hauptsächlich mit der gesetzgeberischen Entwicklung in Europa begründet, wiederspiegelt der Wortlaut des Vorentwurfs mit seinen strafbewehrten Dokumentations-, Melde- und Informationspflichten, eine ganz grundsätzliche Skepsis am Willen und an der Fähigkeit der Wirtschaft, die für einen angemessenen Datenschutz nötigen Massnahmen zu treffen.

3 Tatsächlich obliegt der Schweiz nicht die Pflicht, die europäischen Regulierungsvorgaben tel quel zu übernehmen. Noch viel weniger besteht ein vernünftiger Anlass für eine Verschärfung ebendieser Regulierungen. Das Hauptanliegen des Verbandes SCHWEIZER MEDIEN ist es daher, dass der im Vorentwurf mehrfach vorhandene "Swiss Finish" unter keinen Umständen

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

Eingang in den Entwurf und die Botschaft finden darf, die im Vorentwurf unvernünftigen Sanktionen gestrichen und die Regelungen wesentlich praktikabler ausgestaltet werden.

4 Die Medienbranche kämpft zusehends mit sinkenden Leserzahlen und Werbeeinnahmen. Die zusätzlichen Pflichten, welche den Unternehmen mit dem Vorentwurf auferlegt werden, erhöhen den administrativen Aufwand massiv oder verunmöglichen die Ausübung gewisser Tätigkeiten gänzlich, bringen dem Datenschutz aber im Ergebnis nichts, ja führen teilweise gerade im Medienbereich zu absurden Ergebnissen. Der Vorentwurf wurde in manchen Punkten nicht durchgedacht. Vor diesem Hintergrund schlägt der Verband SCHWEIZER MEDIEN in seiner Stellungnahme eine Reihe von Anpassungen vor. Nur so kann sichergestellt werden, dass Medienschaffende und Verlage weiterhin ungehindert ihre sowohl demokratie- als auch sozialrelevante Tätigkeit ausüben können.

II. Allgemeine Bemerkungen

5 Die Kernanliegen der Totalrevision des Schweizer Datenschutzgesetzes sind die Stärkung des Datenschutzes durch Schaffung von mehr Transparenz und Kontrollmöglichkeiten sowie die gleichzeitige Verbesserung der Wettbewerbsfähigkeit der Schweiz und damit der Schweizer Unternehmen.

6 Diese Kernanliegen wiederspiegeln sich im Vorentwurf des Bundesgesetzes über den Datenschutz (**VE-DSG**) jedoch nicht. Dieser zeigt nur in eine Richtung; nämlich in die einer umfassenden Regulierung sämtlicher innerbetrieblichen Vorgänge, die mit der Bearbeitung von Personendaten zusammenhängen, komplementiert mit der weitreichenden Informations- und Notifikationspflicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (**EDÖB**) sowie einem umfangreichen Sanktionskatalog von Strafbestimmungen, falls einer der beiden ersten Punkte auf irgendeine Art und Weise nicht oder nicht richtig umgesetzt worden ist.

7 Der Verband SCHWEIZER MEDIEN sieht für viele neue Regeln im VE-DSG sowie für den Versuch einen Paradigmenwechsel im DSG einzuführen keinerlei Anlass. Das bisherige Schweizer Datenschutzmodell hat sich in den letzten Jahren mehr als bewährt. Beim hiesig geltenden Prinzip der "Erlaubnis mit Verbotsvorbehalt" handelt es sich um ein reiflich durchdachtes und fein austariertes Konzept, bei dem sämtliche involvierten Interessen zum Tragen kommen. Dieses soll nicht ohne Not angetastet werden.

8 Eine solche Not liegt nicht vor. Zwar ist unbestritten, dass die europäischen Entwicklungen im Datenschutzrecht und insbesondere die Haager Konvention zum Schutz des Menschen bei der

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

automatisierten Verarbeitung personenbezogener Daten (**Konvention 108**) gewisse Anpassungen erfordern. Doch in vielen Punkten geht der VE-DSG darüber hinaus, was in der Konvention 108, ja sogar der Europäischen Datenschutzgrundverordnung (**DSGVO**) vorgesehen ist. Für ein solches "Swiss-Finish" gibt es keinerlei Anlass und Grund. Auch die Furcht, dass die Schweiz ihren EU-Status als Land mit einem angemessenen Datenschutz verlieren könnte, ist sachlich und real-politisch unbegründet, auch wenn die Europäische Kommission betont, die Angemessenheit sei nicht garantiert. Dieses Klappern gehört zum Handwerk, und die Schweiz sollte sich nicht einschüchtern lassen, sondern nur solche Regeln verabschieden, die auch Sinn machen. Ohnehin würde ein Verlust der EU-Angemessenheit die Schweizer Wirtschaft bei Lichte betrachtet nicht mehr wirklich treffen.

9 Ungeachtet dessen bringen viele der vorgeschlagenen Neuerungen, wie nachfolgend detailliert aufgezeigt wird, auch keinerlei Mehrwert im Hinblick auf den Persönlichkeitsschutz der betroffenen Personen. Die neuen Regulierungen werden aber mit Sicherheit für hohe Budgetposten für Compliance- und Rechtsabteilungen und blendende Geschäfte für Berater sorgen sowie den EDÖB in einer Flut von Notifikationen, Informationen und Anfragen ersticken lassen. Der Verbesserung der Wettbewerbsfähigkeit der Schweiz dient dies indes nicht.

10 Für die Mitglieder des Verbandes SCHWEIZER MEDIEN bergen viele der neuen, starren Normen im VE-DSG die spezielle Gefahr, dass sie ihrer journalistischen Arbeit – und damit ihrer Kerntätigkeit – nur noch unter sehr erschwerten Bedingungen nachgehen können, falls sie sich an das Gesetz halten sollen. In vielen Bestimmungen im VE-DSG wird dem Umstand, dass Schweizer Medienschaffende eine besondere und wichtige Aufgabe haben, denn auch keinerlei Rechnung getragen. Zweifellos war es nicht die Absicht, ihnen Steine in den Weg zu legen, aber manche der Bestimmungen sind in ihren Konsequenzen nicht wirklich durchdacht und werden genau diesen Effekt haben. Damit droht der Datenschutz nach Vorgabe des VE-DSG die Funktion der Medien für eine freie Demokratie nachhaltig zu untergraben, was wohl niemand will.

11 Die Arbeit mit der die Aufgabe der Medienschaffenden erfüllt wird, besteht hauptsächlich darin, Informationen und eben auch Personendaten zu erheben, zu bearbeiten und zu veröffentlichen. Die neue Starrheit, welche das VE-DSG vorgibt, erschwert jeden vernünftigen Umgang mit datenschutzrechtlichen Grundsätzen. Dies kann für den Journalismus letztlich auch bedeuten, dass dieser nicht mehr ausgeübt werden kann. Erschwert wird hauptsächlich die journalistische Arbeit an sich (welcher Journalist wird bei jeder Recherche von jeder involvierten Person deren Einwilligung einholen können). Aber auch die Finanzierung dieser Arbeit über Werbung sowie über den Nutzermarkt wird bei fehlenden Marketinglösungen zunehmend schwierig. Dies ist ein zweiter wichtiger Aspekt: Es ist zwar *en vogue*, die Analyse- und Marketing-Möglichkeiten

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

moderner Online-Medien zu kritisieren, aber dabei wird vergessen, dass marketing- und werbefinanzierte Inhalte inzwischen ein zentrales Standbein der Medienwelt geworden sind. Wer diese Möglichkeiten einschränkt, beschneidet damit die Medien in ihrer Tätigkeit genauso, wie wenn er ihnen inhaltliche Beschränkungen auferlegt. Dem Persönlichkeitsschutz der Konsumenten hilft auch dies nicht wirklich: Sie nutzen Online-Medien freiwillig und fühlen sich damit ausgesprochen wohl, wie auch die Erfahrungen des Verbandes zeigen. Die im VE-DSG zum Ausdruck kommenden paternalistischen Tendenzen, die Konsumenten zu ihrem datenschutzrechtlichen Glück zu zwingen, sind fehl am Platz.

III. Bemerkungen zu den einzelnen Artikeln

A. Art. 1 – Zweck

12 Der Zweckartikel soll die Kernanliegen des Schweizer Datenschutzrechts wiederspiegeln und gilt damit auch als eine wichtige Auslegungshilfe bei der Anwendung datenschutzrechtlicher Grundsätze und der Abwägung sich entgegenstehender Interessen. Weil der Schutz der Wettbewerbsfähigkeit eines der Ziele der vorliegenden Totalrevision ist, muss dies auch im Zweckartikel ausdrücklich erwähnt werden.

B. Art. 2 Abs. 2 lit. c – Ausnahme vom Geltungsbereich

13 Gemäss Art. 2 Abs. 2 lit. c VE-DSG sollen neu Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden, vom Anwendungsbereich des Datenschutzgesetzes ausgenommen sein. Im Gegensatz zum heutigen Wortlaut, wonach an die Hängigkeit eines Verfahrens angeknüpft wird, hätte der jetzige Formulierungsvorschlag zur Folge, dass nur noch die Datenbearbeitung durch die Justizbehörden vom Datenschutzrecht ausgenommen ist. Auf die Parteien dieser Verfahren sollen die Regeln des DSG neu anwendbar sein. Dies birgt mitunter die Gefahr, dass die Parteien in Verbindung mit Art. 20 f. VE-DSG auch noch während einem Verfahren bei der Gegenpartei um Auskunft ersuchen können, obschon die Edition von Urkunden und die der Edition zu Grunde liegende Interessenabwägung Gegenstand des geltenden Prozessrechts sind und darin auch abschliessend geregelt sind. Diese Erweiterung des Anwendungsbereichs ist daher unnötig, unverhältnismässig und ebnet den Weg für den Missbrauch des Auskunftsrechts (vgl. auch Ausführungen zu Art. 20 VE-DSG in Abschnitt III.Q). Davon sind

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

auch Medienunternehmen immer stärker betroffen; Auskunftsgesuche zu datenschutzfremden Zwecken verursachen immer höhere Kosten.

C. Art. 3 lit. c Ziff. 4 – biometrische Daten

14 Nach dem jetzigen Wortlaut von Art. 3 lit. c Ziff. 4 VE-DSG gelten sämtliche biometrischen Daten, die eine natürliche Person eindeutig identifizieren, als besonders schützenswerte Personendaten.

15 Damit gilt jedes Foto sowie Bewegtbild eines Gesichts, welches in den Medien erscheint, als ein besonders schützenswertes Personendatum, was viel zu breit ist. Dies war gemäss dem Erläuternden Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (**Erläuterungsbericht**) auch nie das Ziel dieser Bestimmung. Dort steht, dass nur solche Bilder unter den Begriff biometrische Daten fallen sollen, "die mit spezifischen technischen Mitteln so [also *zu diesem Zweck*] bearbeitet werden, dass eine eindeutige Identifizierung oder Authentisierung eines Individuums möglich ist" (Erläuterungsbericht, S. 43).

16 Diese Einschränkung gibt die heutige Formulierung des VE-DSG aber nicht wieder. Entsprechend muss der Wortlaut so präzisiert werden, dass er mit dem eigentlichen Sinn und Zweck der Norm übereinstimmt, d.h. dass biometrische (wie im Übrigen auch genetische) Daten nur dann besonders schützenswert sind, wenn ihr primärer Zweck die eindeutige Identifikation einer Person ist. Fotos von Menschen in den Medien sollten (von Ausnahmen wie Fahndungsfotos abgesehen) allein aufgrund der Tatsache, dass darauf ein bestimmter Mensch eindeutig zu erkennen ist, nie als besonders schützenswerte Personendaten gelten, wie das auch bisher nicht der Fall ist. Darauf ist auch in der Botschaft hinzuweisen.

D. Art. 3 lit. f – Profiling

17 In Art. 3 lit. f VE-DSG wird neu der Begriff des Profilings eingeführt. Im Gegensatz zum Begriff des Profilings in der DSGVO ist die Definition in der VE-DSG extrem breit. Ein Profiling nach VE-DSG liegt nicht nur bei einer automatisierten, sondern bei jeder Auswertung von Daten vor. Sie liegt selbst dann vor, wenn Daten ausgewertet werden, die keine Personendaten sind, sofern damit der Zweck verfolgt wird persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Dies bedeutet, dass fast jede journalistische Recherche als Profiling zu qualifizieren ist.

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

18 Dies ist deshalb höchst problematisch, weil gemäss Art. 23 Abs. 2 lit. d VE-DSG ohne Begründung jedes Profiling per Generalverdacht eine Persönlichkeitsverletzung darstellen soll, obwohl der Begriff des Profiling derart breit definiert ist, dass er auch unzählige alltägliche und völlig harmlose Handlungen erfasst. Die Regel von Art. 23 Abs. 2 lit. d VE-DSG hat wiederum zur Folge, dass es damit nur mit einem Rechtfertigungsgrund erfolgen darf, also beispielsweise einer vorgängig eingeholten ausdrücklichen Einwilligung oder einem überwiegenden Interesse. Mit anderen Worten muss ein Journalist vor jeder Recherche, selbst wenn es sich hierbei um eine manuelle Recherche für einen Artikel handelt, zuerst bezüglich der diversen davon betroffenen Personen Einwilligungen einholen oder entsprechende überwiegende Interessen dokumentieren. Da *per se* eine Persönlichkeitsverletzung vorliegt, wird nach Art. 16 VE-DSG zudem zwingend eine Datenschutz-Folgenabschätzung durchgeführt werden müssen, mit den nötigen Meldungen an den EDÖB (vgl. Ausführungen dazu in Abschnitt III.N). Dies ist völlig unverhältnismässig und verunmöglicht jegliche journalistische Arbeit (vgl. Ausführungen zu diesem Paradigmenwechsel in Abschnitt III.R). Sofern am Begriff des Profilings festgehalten wird, sollte er auf automatisierte Datenbearbeitungen beschränkt werden.

19 Weiter umfasst der Begriff des Profilings gemäss VE-DSG auch die Bearbeitung von Daten, also nicht nur Personendaten. Weil aufgrund von Art. 2 VE-DSG nach wie vor klar sein muss, dass das VE-DSG nur auf die Bearbeitung von Personendaten anwendbar ist, steht die Formulierung in Art. 3 lit. f VE-DSG im Widerspruch mit dem Rest des Schweizer Datenschutzrechts. Dieser unnötige Zusatz "Daten oder" sollte aus dem Gesetz gestrichen werden.

20 Schliesslich gilt es anzumerken, dass die Analyse von Personendaten für sich alleine keine Auswirkungen auf die Rechte der betroffenen Personen haben kann. Richtigerweise kann es erst in Rahmen einer Bewertung eben dieser Analyse zu einem Eingriff in die Persönlichkeit der betroffenen Personen kommen, weshalb auch eine entsprechende sprachliche Präzisierung notwendig ist.

21 In Anbetracht all dieser Gründe sollte der Begriff des Profilings komplett gestrichen werden; es braucht ihn nicht. Eine Regel über automatisierte Einzelentscheide reicht aus, um die problematischen Fälle zu erfassen und der Konvention 108 zu genügen. Darüber hinaus sorgt der dem DSG ohnehin inhärente risikobasierte Ansatz dafür, dass die Anforderungen an eine heikle Datenbearbeitung höher sind als an andere, ganz gleich, aus welchem Grund eine Datenbearbeitung als heikel erscheint.

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

E. Art. 4 Abs. 3 – Zweckbindung

22 Personendaten sollen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft und bearbeitet werden dürfen. Im Rahmen des Wortlauts von Art. 4 Abs. 3 wird der neue Grundsatz eingeführt, dass Personendaten auch für Zwecke verwendet werden dürfen, die mit dem ursprünglichen Zweck kompatibel sind. Diese Erweiterung ist zu begrüssen. Es sollte in der Botschaft betont werden, dass dies auch die Nutzung und Weitergabe von Daten innerhalb von Gruppengesellschaften ermöglicht, selbst wenn ein "Controller-Controller"-Transfer vorliegt.

23 Der Erläuterungsbericht suggeriert jedoch, es entspreche der allgemeinen Wahrnehmung, dass beispielsweise die Weiterverwendung von erhobenen Adressen für Werbezwecke nicht zulässig sei, weil dieser Zweck für die betroffenen Personen im Erhebungszeitpunkt nicht erkennbar gewesen sei. Diese Ansicht ist überholt. In der heutigen Zeit ist unbestritten, dass ein Konsument, der zum Beispiel bei einem Verlag ein Abonnement löst oder an einem Wettbewerb teilnimmt, wissen muss bzw. davon ausgeht, dass seine Daten eben auch für Marketingzwecke verwendet werden. Dafür braucht es keine zusätzlichen Erklärungen und auch keine gesonderte Einwilligung. Dies sollte in der Botschaft klargestellt werden, oder jedenfalls auf Aussagen wie im Erläuterungsbericht verzichtet werden, da sie ein falsches Bild vermitteln.

24 Aus dem Gesetzestext erschliesst sich nicht, was ein "klar" erkennbarer Zweck sein soll. Die im konkreten Fall notwendige Deutlichkeit einer Darstellung bestimmt sich immer anhand des mit der konkreten Datenbearbeitung verbundenen Risikos. Daher ist dieser Zusatz "klar" zu streichen. Andere Rechtsordnungen mögen solche Attribute verwenden, aber im Schweizer Rechtssystem führt es zu mehr Fragen als Antworten.

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

F. Art. 4 Abs. 6 – Einwilligung

25 Gemäss dem Wortlaut des VE-DSG muss eine Einwilligung "eindeutig" erfolgen. Was das bedeutet, geht weder aus dem Gesetzeswortlaut noch aus dem Erläuterungsbericht hervor. Auch in Bezug auf die Ausdrücklichkeit der Einwilligung, die es im Zusammenhang mit besonders schützenswerten Personendaten und Profiling braucht, schafft der Erläuterungsbericht mehr Verwirrung als Klarheit.

26 Der scheinbar in der Lehre ausgetragenen Kontroverse im Zusammenhang mit Einwilligung in Datenschutzangelegenheiten soll keine Beachtung geschenkt werden und schon gar keinen Eingang in Gesetzesmaterialen finden. Damit entsteht die Gefahr, dass die Einwilligung im Datenschutzrecht auf ein besonderes Podest gehoben wird. Hierfür gibt es keinen vernünftigen Grund. Die Einwilligung ist eine Willenserklärung wie jede andere auch. Nichts Anderes geht aus dem Gesetzestext hervor. Dies muss zumindest in der Botschaft klargestellt werden. In diesem Sinne begrüsst es der Verband SCHWEIZER MEDIEN, dass im VE-DSG von den in der DSGVO vorgesehenen Einschränkungen im Zusammenhang mit Einwilligungen im Datenschutz klar Abstand genommen wird und demnach weder ein Koppelungsverbot eingeführt wird noch, dass eine Einwilligung erst dann unmissverständlich sein soll, wenn diese durch eine eindeutige bestätigende Handlung vorgenommen wird. Dafür bleibt im Schweizer Recht kein Platz.

27 Demnach gelten die Bestimmungen des allgemeinen Obligationenrechts, was insbesondere bedeutet, dass eine ausdrückliche Einwilligung vorliegt, wenn der Sinngehalt der Willenserklärung ausdrücklich aus dieser selbst hervorgeht, ohne dass notwendigerweise zur Deutung weitere Umstände herangezogen werden müssen. Diese Willensäusserung kann einerseits durch Sprache und andererseits – und das ist in der herrschenden Lehre unbestritten – auch durch vorab vereinbartes Schweigen im Sinne von Art. 6 OR erfolgen (ausdrücklich anstatt vieler: HUGUENIN CLAIRE, Obligationenrecht Allgemeiner und Besonderer Teil, 2. Aufl., Zürich 2015, Rn. 173; GAUCH PETER / SCHLUEP WALTER R. / SCHMID JÖRG, Schweizerisches Obligationenrecht Allgemeiner Teil ohne ausservertragliches Haftpflichtrecht, Bd. I, 9. Aufl., Zürich 2008, Rn. 180; KOLLER ALFRED, Schweizer Obligationenrecht Allgemeiner Teil. Handbuch des allgemeinen Schuldrechts ohne Deliktsrecht, 3. Aufl., Bern 2009, § 3 Rn. 117; SCHWENZER INGEBORG, Schweizerisches Obligationenrecht. Allgemeiner Teil, 7. Aufl., Bern 2016, Rz. 27.11).

28 Angesichts der wichtigen praktischen Bedeutung der Möglichkeit einer stillschweigenden Übernahme von Allgemeinen Geschäftsbedingungen (AGB) und aufgrund der bestehenden Unsicherheit im Zusammenhang mit Datenbearbeitungen soll dies zumindest in der Botschaft klar zum Ausdruck kommen. Es sollte klargestellt werden, dass datenschutzrechtliche

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

Einwilligungen ebenso im Rahmen von AGBs möglich sind, wie Einwilligungen in anderen Bereichen des Rechts auch (z.B. Verzicht auf das Bankgeheimnis).

29 Schliesslich ist der Verband SCHWEIZER MEDIEN der Meinung, dass sich für das Profiling keine ausdrückliche Einwilligung rechtfertigt, da es sich hierbei in Wirklichkeit um alltägliche Datenbearbeitungen (z.B. Spam- oder Virenfilter) handelt und nicht, wie mit dieser Bestimmung suggeriert wird, um besonders bedrohliche oder für die Persönlichkeit der betroffenen Personen heikle Projekte. Solche kann es vereinzelt geben, aber das rechtfertigt nicht die Sonderbehandlung.

G. Art. 5 und 6 – Grenzüberschreitende Datenbekanntgabe

30 Für Medienschaffende ist die grenzüberschreitende Datenbekanntgabe insbesondere dann ein Thema, wenn Medienerzeugnisse, die regelmässig Personendaten enthalten, im Ausland vertrieben (als Print-Produkte) oder zugänglich gemacht werden (als Online-Medien). In der Praxis stellen solche Fälle grenzüberschreitend zugänglich gemachter Publikationen kein Problem dar, doch wird dieser von Art. 5 und 6 VE-DSG nicht erfasst. Bisher existierte lediglich für automatisierte Informations- und Kommunikationsdienste eine Ausnahmeregelung in Art. 5 VDSG.

31 Im Zuge der Revision des DSG sollte diese Lücke geschlossen und festgehalten werden, dass die Publikation von Inhalten (und nachgelagerte Übermittlungen publizierter Informationen) keinen Fall der grenzüberschreitenden Bekanntgabe im Sinne von Art. 5 VE-DSG darstellt. Die Regel des heutigen Art. 5 VDSG muss korrekterweise ins DSG aufgenommen und auf alle öffentlich zugänglichen Inhalte erweitert werden. Es gibt keinen Grund, Online-Medien gegenüber Print-Publikationen zu privilegieren.

32 Ferner sind die Meldepflichten gemäss Art. 6 VE-DSG zu streichen. Sie sind überflüssig und praxisfremd. Der Rechtfertigungsgrund der Vertragserfüllung ist auf Personen zu erweitern, für welche ein Vertrag abgeschlossen wurde (z.B. Empfänger eines geschenkten Abonnements).

H. Art. 7 – Auftragsdatenbearbeitung

33 Im heutigen Recht kann jeder, der an einer Persönlichkeitsverletzung "mitwirkt", für diese nach Art. 28 ZGB ins Recht gefasst werden. Das geht nach dem "Tribune de Geneve"-Entscheid des Bundesgerichts (5A_792/2011) allerdings so weit, dass auch derjenige, der lediglich eine technische Plattform zur Verfügung stellt, für die darauf publizierten persönlichkeitsverletzenden Inhalte verantwortlich gemacht werden kann, auch wenn er keine redaktionelle Kontrolle hat.

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

34 Datenschutzrechtlich gesprochen wurde der Auftragsbearbeiter dafür verantwortlich gemacht, dass sein Auftraggeber sich nicht rechtskonform verhielt. Das ergibt sich zwar aus den allgemeinen Grundsätzen von Art. 28 ZGB missachtet aber das Subordinationsverhältnis des Auftragsbearbeiters im Bereich des Datenschutzes. Ein solcher sollte daher entsprechend vor datenschutzrechtlicher Verantwortlichkeit geschützt werden, solange er den Weisungen des Auftraggebers folgt und seinen sonstigen Pflichten diesem gegenüber nachkommt.

35 Es sollte daher in Art. 7 VE-DSG festgehalten werden, dass der Auftragsbearbeiter für das rechtskonforme Verhalten seines Auftraggebers zivilrechtlich nicht verantwortlich ist, sondern solche Ansprüche gegen den Auftraggeber zu richten sind. Ansonsten wird der Auftragsbearbeiter gezwungen, eine redaktionelle Kontrolle über Inhalte auszuüben, die ihm an sich nicht zusteht. Selbstverständlich kann ein Gericht stellvertretend für den Auftraggeber dem Auftragsbearbeiter entsprechende Weisungen erteilen.

I. Art. 12 Daten einer verstorbenen Person

36 Diese Bestimmung ist ein Fremdkörper im Schweizer Datenschutzgesetz. Die Persönlichkeit einer Person endet mit dem Tod. Folglich auch ihr Recht auf Datenschutz. Ein Angehöriger kann höchstens ein eigenes Datenschutz- oder Persönlichkeitsinteresse haben.

37 Es muss verhindert werden, dass ein pauschaler postmortaler Schutz von Angehörigen geschaffen wird und unter dem Deckmantel dieser Bestimmungen Medienschaffende gezwungen werden können, Daten aus ihren Medienarchiven zu löschen. Es besteht keine Notwendigkeit für diese Bestimmung. Sie muss ersatzlos gestrichen werden. Entsprechende Fragestellungen sind, wo ein Bedarf besteht, in Spezialgesetzen bzw. im ZGB zu adressieren.

38 Eventualiter gilt es zu verhindern, dass über diese Bestimmung die Medienschaffenden von Angehörigen verstorbener Personen gezwungen werden können, Information zu löschen. Aus diesem Grund soll die Vermutung eines überwiegenden öffentlichen Interesses an der Aufbewahrung und Archivierung von journalistischen Inhalten in diese Bestimmung ausdrücklich aufgenommen werden, sowie in Abs. 2 von Art. 12 ein schutzwürdiges Interesse gewisser Personen vermutet wird. Sub-Eventualiter sollte in der Botschaft festgehalten werden, dass Medienarchive sich in der Regel auf ein überwiegendes öffentliches Interesse berufen können, um Löschungen unter Berufung auf Art. 12 VE-DSG zu verhindern. Vorbehalten bleiben selbstverständlich Löschungen der Angehörigen aus eigenem Recht.

39 Es sei an dieser Stelle darauf hingewiesen, dass der Umgang mit Daten von Verstorbenen in Sozialen Medien, um welche es in Art. 12 VE-DSG an sich geht, von diesen ohnehin autonom

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

im Rahmen ihrer Vertragsbedingungen geregelt werden und die hier vorgeschlagene Regelung darauf keinen Einfluss nehmen wird, da sich die Betreiber der relevanten Sozialen Medien nicht an die Bestimmung von Art. 12 VE-DSG gebunden fühlen werden. Da es sich nicht um "echte" Ansprüche aus Persönlichkeitsschutz handelt, greift wohl auch die Anknüpfung von Art. 139 IPRG nicht. Damit kann Art. 12 VE-DSG seinen Zweck nicht mehr erfüllen und ist auch aus diesem Grunde überflüssig.

J. Art. 13 – Informationspflicht bei der Beschaffung von Personendaten

40 Die Ausweitung der öffentlich-rechtlichen, sanktionsbewehrten Informationspflichten nach Art. 13 VE-DSG auf alle Personendaten wird zu einem enormen Mehraufwand für Schweizer Unternehmen jeder Grösse führen, falls die denn im vorgesehenen Umfang überhaupt umgesetzt werden können. Einen sachlichen Grund für diese Ausweitung gibt es nicht.

41 Bereits nach geltendem Recht gilt, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angezeigt wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Diese Lösung berücksichtigt im Rahmen eines Bearbeitungsgrundsatzes das Risiko der jeweiligen Datenerhebung und mögliche Rechtfertigungsgründe. Dies ist ausreichend, um gegenüber der betroffenen Person Transparenz in Bezug auf die Datenerhebung und den mit der Bearbeitung verbundenen Zweck zu wahren, und genügt auch den Vorgaben der Konvention 108. Eine darüberhinausgehende Regulierung und die damit einhergehende Formalisierung von Informationen wird in einer Flut von Schildern, Nutzungsbedingungen, Privacy Notices, Policies u.ä. resultieren, welche letztlich bekanntermassen von niemandem gelesen werden. Damit wird das exakte Gegenteil von Transparenz bewirkt.

42 Demgegenüber ist das heute geltende und in Bezug auf die konkrete Datenbearbeitung individuelle Transparenzgebot einfach, klar und in der Sache ausreichend. Auf eine separate Informationspflicht ist zu verzichten, oder aber sie ist wie heute in Art. 14 DSG auf die Beschaffung von schützenswerten Personendaten zu beschränken. Allerdings wird auch diese Bestimmung in der Praxis erfahrungsgemäss regelmässig nicht befolgt, weil sie sich nicht sinnvoll umsetzen lässt. Mit dem nunmehr vorgeschlagenen Art. 13 VE-DSG wird die Situation schlimmer. Es macht jedoch keinen Sinn eine Bestimmung ins Gesetz aufzunehmen, bei welcher von vornherein klar ist, dass sie so nicht vernünftig eingehalten werden kann. Art. 13 VE-DSG verlangt zum Beispiel von jedem Journalisten, der über eine Person (Politiker, Schauspieler, Fussballer etc.) Informationen zusammenträgt (Zeitungsberichte, Interviews, Medienmitteilung etc.), diese entsprechend darüber zu informieren. Die Ausnahmeregelungen

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

werden regelmässig nicht greifen, oder es wird nicht klar sein, ob sie es tun. Eine solche Pauschalregelung dient dem Datenschutz in keiner Weise, führt aber zu unbilligen Ergebnissen, wie das Beispiel zeigt.

43 Während Art. 13 VE-DSG sich immerhin noch teilweise an die DSGVO anlehnt, handelt es sich bei Art. 13 Abs. 4 VE-DSG um einen unverhältnismässigen Swiss-Finish. Betroffene Personen wissen heute, dass nicht jede Dienstleistung und die damit einhergehende Datenbearbeitung von ihrem jeweiligen Vertragspartner selber erbracht werden wird. Das Auslagern von Datenbearbeitungen ist in unserer arbeitsteiligen Wirtschaft normal. Entsprechend gilt in diesem Rahmen das sog. Bekanntgabeprivileg, wonach nicht über jede Auslagerung einer Datenbearbeitung an einen dritten Dienstleister informiert werden muss. Aus persönlichkeitsrechtlichen Überlegungen ist in Art. 7 VE-DSG abschliessend festgehalten, dass diese Auslagerungen nur unter Einhaltung ganz bestimmter Vorgaben erfolgen darf. Eine darüberhinausgehende Regulierung dient nicht dem Persönlichkeitsschutz der betroffenen Person und ist daher unverhältnismässig und weltfremd. Schliesslich müsste somit jede Neugestaltung von Prozessen mit Dritten den betroffenen Personen sogleich mitgeteilt werden, was nicht immer praktikabel ist und für den Betroffenen überdies oft auch nicht relevant. Art. 13 Abs. 4 VE-DSG ist daher ersatzlos zu streichen. Sollte die betroffene Person im Einzelfall ein Interesse an den Angaben zu den Auftragsdatenbearbeitern haben, so kann man ihr diese im Rahmen ihres Auskunftsrechts geben. So ist zumindest sichergestellt, dass nur dort Aufwand generiert wird, wo tatsächlich auch eine Nachfrage dafür besteht.

44 Aus dem Wortlaut von Art. 13 VE-DSG geht insgesamt nicht genau hervor, über was nun genau informiert werden muss. Sind es im Zusammenhang mit Abs. 3 nun die Dritten, die Empfänger oder die Kategorien von Empfängern? Handelt es sich bei Dritten und Empfängern um die gleiche Person? Wann muss individuell und wann nur kategorisch informiert werden? Gerade auch im Hinblick darauf, dass es sich hierbei um eine potenziell strafbedrohte Norm handelt, sind derart ungenaue Formulierungen untauglich. Auch Abs. 3 ist daher ersatzlos zu streichen.

45 Weiter geht aus dem jetzigen Wortlaut von Art. 13 VE-DSG nicht klar hervor, in welchem Zeitpunkt die Information zu erfolgen hätte. Wäre dies bereits im Zeitpunkt der Recherchearbeit, bei der Speicherung oder bei der Veröffentlichung des daraus resultierenden Artikels in einem Medium? Und was gilt, wenn ein Journalist im eigenen Medienarchiv recherchiert? Stellt dies eine neue Datenerhebung dar? Dies hätte wohl zur Folge, dass Journalisten auf ihren Dossiers nicht mehr laufend recherchieren könnten. All diese Punkte sind zu durchdenken und zu präzisieren.

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

K. Art. 14 – Ausnahmen von der Informationspflicht und Einschränkungen

46 Art. 14 VE-DSG zählt diejenigen Fälle auf, bei denen eine Informationspflicht entfällt. Hierbei verwendet der Artikel verschiedene Begriffe, die möglicherweise dasselbe bedeuten. Es erschliesst sich uns nicht gänzlich, weshalb in Abs. 3 von der Übermittlung von Informationen die Rede ist, sollte es sich hierbei um die Informationspflicht gegenüber der betroffenen Person handeln. Zudem ist nicht klar worauf sich das "dies" in Abs. 3 lit. a und b bezieht. Dies gilt es klarzustellen.

47 Bearbeiten Medienschaffende Personendaten, beispielsweise im Rahmen eines Interviews, für einen Artikel, der in einem Medium erscheinen soll, so können sie sich gemäss dem aktuellen Wortlaut von Art. 14 Abs. 4 lit. a VE-DSG unter keinen Umständen auf ein überwiegendes eigenes Interesse abstützen, weil die Personendaten mit der Veröffentlichung in den Medien Dritten bekannt gegeben werden. Warum im Falle einer Weitergabe von Personendaten an Dritte die Berufung auf überwiegende eigene Interessen nicht mehr möglich sein soll, ist nicht ersichtlich. Sollten im Einzelfall nämlich tatsächlich die Interessen der betroffenen Personen durch die Bekanntgabe an Dritte beeinträchtigt sein, so ist diesem Umstand bereits mit der in Art. 24 VE-DSG vorgesehenen Interessenabwägung Rechnung getragen worden. Diese Einschränkung ist deshalb zu streichen, so dass überwiegende private Interessen uneingeschränkt geltend gemacht werden können.

48 Nach der gegenwärtigen Regelung können sich Medienschaffende jedenfalls nur auf überwiegende Interessen Dritter im Sinne von Art. 14 Abs. 3 lit. b VE-DSG berufen. Selbst die Berufung auf überwiegende öffentliche Interessen ist ihnen im Gegensatz zu Bundesorganen verwehrt. Um die Unsicherheit zu vermeiden, ob nun tatsächlich bei jedem Interview und jeder Recherche die betroffenen Personen über die Datenbearbeitungen informiert werden müssen, sollte ferner in der Botschaft festgehalten werden, dass Medien eine zentrale Rolle in einer funktionierenden Demokratie einnehmen und aus diesem Grund ein öffentliches Interesse daran besteht, dass Medienschaffende im Rahmen ihrer redaktionellen Arbeit von der Informationspflicht ausgenommen sind.

49 Zudem ist Art. 14 Abs. 5 VE-DSG ersatzlos zu streichen. Demnach müsste jedes Unternehmen konstant seine Interessenabwägung überprüfen. Dies bedingt die Einführung eines äusserst kostenintensiven Prozesses, mit dem konstant die involvierten Interessen gegeneinander abgewogen werden, um dann im Fall der Fälle nachträglich noch informieren zu können. Dies ist insbesondere deshalb hinfällig, als dass über das Auskunftsrecht, welches die betroffenen Personen jederzeit geltend machen können, bereits sichergestellt ist, dass diese Informationen

auch später noch erlangt werden können. Abs. 5 bringt daher für die betroffenen Personen keine zusätzlichen Rechte, sondern generiert nur Kosten für die betroffenen Unternehmen.

50 Schliesslich ist in diesem Artikel sicherzustellen, dass die in Art. 22 vorgesehenen Einschränkungen des Auskunftsrechts für Medienschaffende auch auf die Informationspflichten der Medienschaffenden anzuwenden ist. Es ist nicht einzusehen, warum Medienschaffende bei spezifischer Rückfrage zwar die Auskunft verweigern können, aber gleichzeitig gezwungen werden, von sich aus aktiv zu informieren.

L. Art. 15 – Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung

51 Im Gegensatz zur entsprechenden Bestimmung in der DSGVO, der an "erhebliche Auswirkungen" anknüpft, deutet der jetzige Wortlaut von Art. 15 Abs. 1 VE-DSG darauf hin, dass die Informations- und Anhörungspflichten immer greifen, wenn die automatisierte Einzelentscheidung rechtliche Auswirkungen auf die betroffenen Personen haben. Damit bleibt gänzlich ungeklärt, welchen Schweregrad diese rechtlichen Wirkungen haben müssen.

52 Bei der Konkretisierung dieser Eingriffsschwelle ist zu berücksichtigen, dass eine automatisierte Datenbearbeitung per se noch kein schwerer Eingriff in das Persönlichkeitsrecht der betroffenen Personen darstellt. Es lässt sich sogar argumentieren, dass gerade weil ein auf einem Algorithmus basierter Entscheid letztlich ohne den Risikofaktor Mensch funktioniert, im Grundsatz datenschutzfreundlicher ist. Dabei ist zu bedenken, dass die jetzt vorgeschlagene Lösung in ganz viele Bereiche des Alltags eingreift, die in keiner Weise die Persönlichkeit einer betroffenen Person tangieren. Für diese Fälle verlangt auch die Konvention 108 keine entsprechende Regelung. Da Art. 15 Abs. 1 VE-DSG jede rechtliche Wirkung bereits als genügend erscheinen lässt, erfasst die Bestimmung bereits jeden Webshop. Auf das Online-Angebot eines Verlags übertragen bedeutet dies, dass dieser bei jedem Artikel, den er einem Leser online verkauft (was vollautomatisch abläuft), diesbezüglich einer umfassenden Informations- und Anhörungspflicht unterliegt. Das verursacht massive Kosten, ist völlig übertrieben und bringt dem Datenschutz rein gar nichts.

53 In der Botschaft sollte ferner klargestellt werden, dass personalisierte Werbung und ähnliche Aktivitäten oder auch personalisierte Inhalte (z.B. ein Online-Medium, welches einem Leser eine auf ihn zugeschnittene Auswahl an Beiträgen präsentiert) nicht der Bestimmung von Art. 15 Abs. 1 VE-DSG unterliegen. Auf fast jedem modernen Online-Angebot finden solche Vorgänge statt; die Regelung von Art. 15 Abs. 1 VE-DSG sollte auf jene Fälle beschränkt werden, in denen ein Einzelentscheid wirklich massive Auswirkungen hat.

M. Art. 16 Abs. 1 – Schwelle für Datenschutz-Folgeabschätzung

54 Der Entwurf setzt die Schwelle für die Durchführung einer Datenschutz-Folgeabschätzung bei einem "voraussichtlich erhöhten Risiko" an. Dies ist zum einen ein unklarer und damit für die betroffenen Unternehmen unbrauchbarer Begriff, weil daraus nicht hervorgeht, gegenüber was eine Erhöhung des Risikos vorliegen muss. Zum anderen stellt jede einzelne Datenbearbeitung – gerade in Unternehmen – immer ein erhöhtes Risiko dar, weshalb diese Voraussetzung *per se* untauglich ist. Das gilt erst recht, wenn eine Datenbearbeitung zwar gerechtfertigt ist, aber aufgrund der Fiktion von Art. 23 VE-DSG als Persönlichkeitsverletzung gilt, z.B. ein Profiling oder Bearbeitung gegen den Willen einer Person.

55 Auch der Erläuterungsbericht hilft hier nicht weiter. Demgemäss ist ein erhöhtes Risiko immer dann gegeben, "wenn die spezifischen Eigenschaften der geplanten Datenbearbeitung darauf schliessen lassen, dass die Verfügungsfreiheit der betroffenen Personen über ihre Daten erheblich eingeschränkt wird oder werden kann". Würde dies gelten, so würde jedes Verfassen eines kritischen Medienberichts einer vorgängigen Datenschutz-Folgeabschätzung bedürfen, was für sich betrachtet schon unmöglich ist und in Verbindung mit den damit einhergehenden Meldepflichten zu absurden Situationen führt.

56 Die Notwendigkeit einer formalisierten Datenschutz-Folgeabschätzung mit Meldung muss zumindest dann wegfallen, wenn für die Datenbearbeitung ein Rechtfertigungsgrund vorliegt; also beispielsweise ein Fall von Art. 24 Abs. 2 lit. d VE-DSG, die interviewte Person ihre Einwilligung abgegeben hat oder weil die Öffentlichkeit ein überwiegendes öffentliches Interesse an der Veröffentlichung eines Artikels hat. Insbesondere beim Vorliegen einer Einwilligung, welche ja nur gültig ist, wenn diese auf informierter Basis erfolgt, fehlt es an der Notwendigkeit einer formalisierten Datenschutz-Folgeabschätzung. Es wäre in diesen Fällen lediglich nachzuweisen, dass der Verantwortliche davon ausgegangen ist, dass seine Bearbeitung mindestens gerechtfertigt ist. Müsste er für jede Bearbeitung (im Falle von Medien: Dem Verfassen jedes einzelnen Beitrags über eine natürliche Person) ein formalisiertes Beurteilungsverfahren durchführen, wäre dies uferlos.

57 In keinem Fall darf die Schwelle nach Schweizer DSG unter diejenige in Art. 36 Abs. 1 DSGVO fallen; darin wird immerhin von einem "hohen" Risiko gesprochen.

58 Zudem kann und darf es nicht die Aufgabe eines Auftragsdatenbearbeiters sein, eine Datenschutz-Folgeabschätzung durchzuführen. Diesem ist es im Sinne von Art. 7 Abs. 1 lit. a VE-DSG ja bereits vertraglich nur erlaubt, die Daten so zu bearbeiten, wie der Verantwortliche selbst es tun dürfte. Aus diesem Grund entsteht durch die Datenschutzfolgeabschätzung weder

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

ein Mehrwert noch wird ein Auftragsdatenbearbeiter überhaupt erst die hierfür notwendigen Informationen haben. Der Auftragsdatenbearbeiter ist ersatzlos aus Art. 16 Abs. 1 VE-DSG zu streichen.

N. Art. 16 Abs. 3 und 4 – Meldepflicht und Einwendungsmöglichkeiten

59 Die pauschale Meldepflicht gemäss Art. 16 Abs. 3 VE-DSG muss gestrichen werden oder zumindest – wie in der DSGVO – auf solche Datenbearbeitung beschränkt werden, die zu wesentlichen Risiken für die betroffenen Personen führen und denen auch mit den vorgesehenen Massnahmen nicht ausreichend begegnet werden kann. Die heutige Formulierung ist nicht praktikabel, unverhältnismässig und ohne jeden Mehrwert für die betroffenen Personen. Nach dem Vorbild der DSGVO wären diese Meldungen zumindest auf systematische umfangreiche Überwachungen im öffentlichen Bereich und auf umfangreiche Bearbeitungen von besonders schützenswerten Personendaten zu beschränken. Alternativ könnte eine entsprechende abschliessende Liste auch in der Verordnung geführt werden.

60 Der EDÖB wäre mit einer Flut von Meldungen konfrontiert, die er nicht im Stande ist zu bearbeiten, was wiederum zu einer Verzögerung der geplanten Projekte auf der Seite der Unternehmen führt. Es liegt auf der Hand, dass mit dieser Regulierung das Tagesgeschäft von Medienschaffenden komplett verunmöglicht wird. Dieses Instrument darf nicht eine kritische Medienberichterstattung verhindern; es kann nicht sein, dass Medien kritische Medienberichte über eine natürliche Person dem EDÖB zuerst zur Prüfung vorlegen müssen. Genau so kann Art. 16 VE-DSG im Ergebnis jedoch verstanden werden.

61 Dieser Swiss-Finish birgt neben den damit einhergehenden hohen Kosten gerade wegen der in Abs. 4 vorgesehenen Wartefrist von drei Monaten – die vom EDÖB notabene noch um drei Monate verlängert werden können, indem er weitere Informationen anfordert – noch weitere einschneidende Konsequenzen für Schweizer Unternehmen. Für Unternehmen bedeutet dies erhebliche Wettbewerbsnachteile im Vergleich zu ihren Europäischen Konkurrenten, was dem Revisionsziel des Datenschutzrechts widerspricht. Aus diesen Gründen sind Abs. 3 und 4 von Art. 16 VE-DSG zu streichen oder alternativ auf oben beschriebene Fälle zu beschränken sowie durch eine angemessene kürzere Frist zu ersetzen.

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

O. Art. 17 – Meldung von Verletzungen des Datenschutzes

62 Die Umsetzung des jetzigen Wortlauts von Art. 17 Abs. 1 VE-DSG hätte zur Folge, dass jede unbefugte Datenbearbeitung, namentlich jede Datenbearbeitung die einem Grundsatz gemäss Art. 4 ff. VE-DSG widerspricht (also auch eine unverhältnismässige Datenverarbeitung), dem EDÖB gemeldet werden muss. Der Versuch, eine Ausnahme für solche Verletzungen des Datenschutzgesetzes zu schaffen, die voraussichtlich nicht zu einem Risiko für die Persönlichkeit der betroffenen Person führen, schlägt fehl, weil diese Ausnahme sachlogisch gar nie aufgerufen werden kann. Denn jede unbefugte Datenbearbeitung stellt gemäss geltendem Recht immer eine Verletzung von Persönlichkeitsrechten dar (vgl. Art. 23 Abs. 2 lit. a VE-DSG).

63 Zudem geht dies inhaltlich massiv über das hinaus, was unter dem Regime der DSGVO gilt. Dort ist nämlich nur im Falle eines Sicherheitsverstosses, der zu einem Verlust des Gewahrsams an den Daten führt, eine Meldung zu erstatten.

64 Ausserdem muss die parallele Strafbewehrung des Verstosses an sich und der Meldepflicht ebendieses Verstosses rechtsstaatlich als höchst bedenklich eingestuft werden (*nemo tenetur*) und wird wohl letztlich zu einer Unternehmensstruktur mit vollständiger Überwachung der Mitarbeiter und Pflicht zum gegenseitigen Verrat führen. Die Konvention 108 verlangt jedenfalls nicht solch weitgehende Massnahmen; sie sind auch kontraproduktiv und richten mehr Schaden an, als sie dem Datenschutz dienen. Es würde völlig genügen, wenn lediglich jene *Data Breaches* gemeldet werden müssten, bei denen so viele Personen so massiv betroffen sind, dass es sinnvoll ist, dass eine Behörde überprüft, ob die nötigen Schutzvorkehrungen getroffen worden sind (die sich schon aus dem geltenden DSG ergeben). So wie sich die Regelung heute präsentiert, müsste jede Zeitungsmeldung, die einen Fehler mit Bezug auf eine natürliche Person enthält, dem EDÖB unverzüglich gemeldet werden.

65 Es erscheint weiter unklar, was genau unter einer "unverzüglichen" Meldung im Sinne von Art. 17 Abs. 1 VE-DSG zu verstehen ist. Stattdessen wäre eine Formulierung "ohne unnötigen Verzug" einerseits in sich griffiger und andererseits könnte auf diesem Weg sichergestellt werden, dass die betroffenen Unternehmen erst dann Meldung erstatten, wenn sie den notwendigen Sachverhalt untersucht, geklärt, analysiert und – was im Sinne der betroffenen Personen wohl nach wie vor am wichtigsten ist – den Fehler behoben haben.

66 Als eine weitere Ergänzung rein sprachlicher Natur ist anzuregen, dass Art. 17 Abs. 5 VE-DSG für Auftragsdatenbearbeiter inhaltlich mit Abs. 1 übereinstimmen muss.

P. Art. 19 lit. b – Information von Empfänger von Personendaten

67 Diese Bestimmung wirkt auf den ersten Blick sinnvoll und nachvollziehbar, auf den zweiten Blick ist festzustellen, dass dies viel zu breit formuliert ist und auch unbedeutende Vorgänge pauschal mitumfasst, bei denen eine Information an die Empfänger erstens, überhaupt keinen Sinn macht und zweitens, auch für die betroffene Person keinerlei datenschutzrelevante Interessen befriedigt.

68 Werden im Rahmen einer Berichterstattung in einem Zeitungsartikel Daten über eine Person in einer den Datenschutz verletzenden Art und Weise bearbeitet, so müssten alle Leser in jedem einzelnen Fall darüber informiert werden. Dies gilt selbst dann, wenn es sich nicht um eine meldepflichtige Datenschutzverletzung handelt, sondern lediglich um eine Löschung, weil die Daten beispielsweise nicht mehr benötigt werden.

69 Weil dies rein technisch sehr einfach zu bewältigen wäre und zudem der "unverhältnismässige Aufwand" gemäss Erläuterungsbericht nur sehr eng ausgelegt werden soll, könnte sich ein Medienschaffender kaum darauf berufen.

70 Mitunter würde eine solche Informationspflicht das in Art. 28g ff. ZGB abschliessend geregelte Gegendarstellungsrecht unterlaufen. Gemäss den dort normierten Anspruchsvoraussetzungen ist erforderlich, dass die betroffene Person zumindest in ihrer Persönlichkeit unmittelbar betroffen sein muss, die falsche Tatsachenbehauptung also eine gewisse Schwere aufweisen muss. Sodann muss die betroffene Person zwingend immer ein schützenswertes Interesse an der Gegendarstellung haben. Im Gegensatz dazu wird in Art. 19 lit. b VE-DSG vermutet, dass bei jeder Berichtigung von Personendaten ein Anspruch auf Information der Empfänger – also auch der Leser von periodisch und nicht periodisch erscheinenden Medien – besteht und nur im Falle eines unverhältnismässigen Aufwandes seitens des Datenbearbeiters davon abgesehen werden kann. Eine derart weitgehende Informationspflicht würde für Medienunternehmen einen substantiellen Mehraufwand bedeuten, der vor dem Hintergrund des bewährten Anspruchs auf Gegendarstellung jeglicher Verhältnismässigkeit entbehrt.

71 Aus diesen Gründen ist der ganze Buchstabe ersatzlos zu streichen. Eventualiter muss die Informationspflicht auf solche Fälle beschränkt werden, in welchen die betroffene Person dies ausdrücklich verlangt und sie an dieser Information schützenswerte Interessen hat, die über das hinausgehen, was in Art. 28g ff. ZGB bereits festgehalten ist.

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

Q. Art. 20 f. – Auskunftsrecht und Einschränkung

72 Obwohl das Auskunftsrecht in der Praxis inzwischen regelmässig als prozessvorbereitendes Beweisbeschaffungsmittel genutzt wird, wurde im VE-DSG auf einen effektiven Mechanismus gegen solche Missbräuche verzichtet. Im Gegenteil wird der Anwendungsbereich des Auskunftsrechts im Vorentwurf sogar noch weiter ausgebaut, indem neu sämtliche Datenbearbeitungen (und nicht mehr nur die in einer Datensammlung vorhandenen Daten) sowie auch hängige Verfahren (siehe Ausführungen in Abschnitt III.B) darunterfallen sollen. In Verbindung mit der in der Schweiz geltenden Rechtsprechung, wonach kein Auskunftsgesuch je als rechtsmissbräuchlich eingestuft werden kann, ist diese Bestimmung unverhältnismässig und muss angepasst werden. Es ist unverständlich, dass nicht versucht wird, diesen Missbräuchen, welche die Wirtschaft erheblich belasten, keinen Riegel zu schieben. Ferner könnte ein unverhältnismässiges Auskunftsrecht auch Journalisten im Vorfeld von Publikationen bei ihrer gesellschafts- und demokratierelevanten Arbeit behindern. Es wäre also in der Botschaft mindestens auf die partikulären Interessen der Medien und allfällige Rechtfertigungsgründe um die Auskunftspflicht zu beschränken hinzuweisen.

73 Möglichkeiten hierzu gibt es diverse. So könnte zum Beispiel vorgesehen werden, dass der Auskunftspflichtige bei Vorliegen von datenschutzfremden Interessen die Möglichkeit hat, den Inhalt der Auskunft nicht der betroffenen Person direkt aushändigen zu müssen, sondern sie bei einer neutralen Stelle zur Einsicht zu deponieren, welche diese nur im Falle eines Prozesses herausgibt. Es sollte ferner – analog der Rechtsprechung des EuGH – festgehalten werden, dass das Auskunftsrecht keinen Anspruch auf Dokumente gibt, sondern lediglich auf Personendaten; in der Praxis wurde das Auskunftsrecht durch sachunkundige Gerichte inzwischen zu einer Bestimmung zur kostenlosen Dokumentenedition degradiert, die mit dem Datenschutz nichts mehr zu tun hat.

74 Sodann muss es weiterhin möglich bleiben, für querulatorische Auskunftsersuchen, Ausnahmen von der Kostenlosigkeit vorzusehen, wobei die pauschale Kostenlosigkeit aus dem Gesetzestext zu streichen und stattdessen zumindest die Ermächtigung einer solchen Ausnahmeregelung auf Verordnungsstufe festzuhalten ist. Dies stünde denn auch im Einklang mit der geltenden Regelung in der DSGVO. Alles andere ist ein unnötiger Swiss-Finish und muss korrigiert werden.

75 Ebenfalls weiter als die DSGVO geht Art. 20 Abs. 3 VE-DSG, wonach über das Ergebnis, das Zustandekommen und die Auswertung einer Entscheidung Auskunft erteilt werden muss. Dies greift in drastischer Weise in die Entscheidungsfreiheit und das Geschäftsgeheimnis der Unternehmen ein, welche sich hierbei unter Umständen (siehe Ausführungen in Abschnitt III.K)

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

nicht einmal auf ein eigenes überwiegendes Interesse berufen können; beispielsweise wenn diese Informationen im Rahmen eines Verfahrens an Behörden bekannt gegeben werden mussten. Eine solche Auskunft hat rein gar nichts mit Datenschutz zu tun und ist ebenfalls ersatzlos zu streichen. Wenn jemand über Entscheide Auskunft verlangen können soll, dann einzig derjenige, der von einer automatisierten Einzelentscheidung selbst in erheblicher Weise betroffen ist, und auch dann nur in diesem Einzelfall. Für eine Pflicht zur faktischen Rechtfertigung der in einem Unternehmen getroffenen Entscheide hat es im Datenschutz keinen Raum. Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende

76 Im Zusammenhang mit Art. 22 VE-DSG ist in der Botschaft festzuhalten, dass nur redaktionelle Änderungen vorgenommen worden sind.

R. Art. 23 Abs. 2 lit. d – Persönlichkeitsverletzung bei Profiling

77 Die Vermutung, dass Profiling ohne ausdrückliche Einwilligung per se eine Persönlichkeitsverletzung darstellt, ist im Schweizer Datenschutzrecht fehl am Platz. Es gibt keinen Grund diese zusätzliche Anforderung an das Profiling zu stellen und hierfür einen Paradigmenwechsel im sehr gut funktionierenden Schweizer Datenschutz- und Persönlichkeitsrecht vorzunehmen. Selbst wenn man das Profiling auf rein automatisierte Vorgänge beschränkt (vgl. Ausführungen in Abschnitt III.D), muss beachtet werden, dass das Profiling auch harmlose Datenbearbeitungen umfassen kann (Bsp. massgeschneiderte Informationsangebote oder Werbung an bestehende Kunden, welche diese interessant finden könnten).

78 Diese Regelung gründet hauptsächlich im latenten Misstrauen gegenüber Datenbearbeitungen, die sich mit Schlagworten wie *Big Data, Data Mining* oder *Programmatic Advertising* umschreiben lassen und die gemeinhin im Zusammenhang mit Profiling verwendet werden, wobei das Unbehagen primär im Unwissen darin besteht, was dabei überhaupt geschieht. Diesbezüglich wird jedoch bereits in der Anwendung der allgemeinen datenschutzrechtlichen Grundsätze dem konkret mit der Bearbeitung verbundene Risiko Rechnung getragen. Dieser Buchstabe ist als reine Symbolbestimmung ersatzlos zu streichen.

S. Art. 24 – Rechtfertigungsgründe

79 Dass gemäss Art. 24 Abs. 2 VE-DSG ein überwiegendes Interesse der bearbeitenden Person nur "möglicherweise" gegeben sein soll, stellt eine grundlose Abkehr vom bisherigen Wortlaut dar und führt bei den Unternehmen zu Rechtsunsicherheit. In den in Abs. 2 aufgezählten

Anwendungsfällen ist ebengerade ein überwiegendes Interesse der Datenbearbeiterin üblicherweise gegeben und die Gerichte sollten davon ihrerseits nur in begründeten Fällen abweichen können. Der Einleitungssatz von Art. 24 Abs. 2 VE-DSG sollte daher den bisherigen Wortlaut von Art. 13 Abs. 2 DSG weiterführen.

80 Im Zusammenhang mit Art. 24 Abs. 2 lit. d VE-DSG ist in der Botschaft festzuhalten, dass keine inhaltlichen Änderungen vorgenommen worden sind. Weiter ist in der Botschaft festzuhalten, dass jede Datenbearbeitung unter diesen Rechtfertigungsgrund fällt; also auch die Bekanntgabe an Dritte sowie die Datenbearbeitung vor und nach der Veröffentlichung (insbesondere die Aufbewahrung der im Rahmen der Recherche gesammelten Dokumente).

T. Art. 50 bis 55 – Strafbestimmungen

81 Die VE-DSG sieht einen zweiseitigen individualstrafrechtlichen Sanktionskatalog vor. Obschon der EDÖB neu auch eine Verfügungskompetenz hat, obliegt die Untersuchungsbefugnis im Zusammenhang mit diesen Sanktionen den kantonalen Untersuchungsbehörden und die Befugnis Sanktionen zu erlassen den kantonalen Gerichten bzw. Strafbehörden. Demgegenüber fehlen im VE-DSG Verwaltungssanktionen für Unternehmen nach dem Vorbild der DSGVO.

82 Diese nicht sachgerechte Kriminalisierung jedes einzelnen Mitarbeiters eines Unternehmens ist abzulehnen. Sie gefährdet den allgemeinen und sich als gewinnbringend erweisenden risikobasierten Ansatz dahingehend, als dass der gesetzlich vorgegebene und wirtschaftlich betrachtet äusserst sinnvolle Anwendungsspielraum aus Angst vor Sanktionen nicht mehr ausgeschöpft wird. Stattdessen werden die Unternehmen und ihre Mitarbeiter stets den bürokratisch aufwändigen aber rechtlich absolut sicheren Weg wählen. Dies birgt die Gefahr, dass der Fokus der Unternehmen auf diejenigen Prozesse gelegt wird, die mit Strafe bedroht sind, während die Einhaltung der allgemeinen Datenschutzgrundsätze, deren Verletzung nicht strafbewehrt ist, zweitrangig wird. Der Ausbau der Bürokratie zwecks Selbstschutz kann nicht Sinn der Sache sein, doch wird der VE-DSG genau dies bewirken.

83 Es ist zudem anzunehmen, dass kaum ein Mitarbeiter mehr gewillt sein wird, sich dem Risiko einer strafrechtlichen Sanktion auszusetzen. Es wird daher schwierig werden, Fachleute für die zentralen Stellen, beispielsweise in der Informatik-, Marketing oder Rechtsabteilung eines Unternehmens, zu finden. Dies trifft gleichermassen auch auf Journalisten und Mitarbeiter auf dem Werbemarkt zu, weil diese ebenfalls jeden Tag Personendaten bearbeiten und damit auch, im Falle einer Verletzung der einschlägigen Normen, als beteiligt gelten.

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

84 Neben der bereits angesprochenen Verletzung des strafrechtlichen Grundprinzips *nemo tenetur* (vgl. Ausführungen in Abschnitt III.O), ist aufgrund der vielen allgemeinen Begriffe im Datenschutzgesetz jede Sanktionierung immer ein Ermessenentscheid, was auch dem Grundsatz *nulla poena sine lege* widerspricht.

85 Der Verband SCHWEIZER MEDIEN vertritt die Auffassung, dass der Katalog der Strafbestimmungen auf den heute geltenden Katalog der Strafbestimmungen reduziert werden kann. Falls dieser Katalog dennoch ausgebaut werden soll, so darf eine Verletzung von Datenschutzbestimmungen nur in der Sanktionierung des datenbearbeitenden Unternehmens resultieren. Die persönliche Strafbarkeit von Mitarbeitern und die fahrlässige Tatvariante ist ersatzlos zu streichen. Die Konvention 108 erfordert eine solche jedenfalls nicht.

86 Die Spruchkompetenz dieser Sanktionen ist mangels ausreichenden Fachkenntnissen weder den kantonalen Gerichten und Strafbehörden noch, aufgrund einer wegen der Verfügungskompetenz entstehenden Machtkonzentration, dem EDÖB aufzuerlegen. Einzige sinnvolle Lösung wäre demnach die Schaffung einer neuen, beispielsweise dem EJPD angegliederten Kommission, der diese Funktion zukäme.

87 Schliesslich ist die in Art. 52 VE-DSG vorgesehene Einführung einer beruflichen Schweigepflicht in Bezug auf alle Personendaten zu streichen. Es ist absurd zum Beispiel einem Medienschaffenden die gleiche strafbewehrte Geheimhaltungspflicht aufzuerlegen, wie einem Arzt oder einem Anwalt. Es besteht keinerlei Anlass den heute geltenden Art. 35 DSG zu ändern.

88 Eine Geheimhaltungspflicht soll nur greifen bei beruflichen Schweigepflichten, die unabhängig von Art. 52 VE-DSG bestehen. In den spezialgesetzlich erfassten Berufszweigen (z.B. Arzt, Anwalt) ist für alle Beteiligten klar, dass eine besondere Vertraulichkeit notwendig ist, z.B. für Patientendaten. Für viele andere Geschäftsfelder, die standardmässig Personendaten erfassen und bearbeiten (z.B. Online-Händler, Werbe-Dienstleister etc.), ist dies nicht der Fall. Früher oder später können praktisch alle Berufszweige mit geheimen Personendaten in Berührung kommen. Die vorgeschlagene Regel schliesst Anbieter damit weitgehend von jeglicher Nutzung der beschafften Daten aus. Die Bussendrohung für derart weit gefasste Pflichten ist unverhältnismässig. Sie ist zu beschränken auf berufliche Schweigepflichten, die ein anderes Gesetz vorschreibt. Wie bei anderen beruflichen Geheimnispflichten, muss eine Befreiung durch die Aufsichtsbehörde möglich sein.

89 Die Ausweitung des Geheimnisschutzes auf alle Personen, welche geheime Daten kommerziell bearbeiten, ist überschiessend. Nicht einmal die EU sieht eine derart strenge Regelung vor. Dienstleister im Bereich personalisierter Online-Werbung, wie etwa Betreiber von

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

Werbenetzwerken, könnten solche Dienstleistungen kaum mehr in der Schweiz anbieten. Die Sanktionsdrohung wäre ein weiterer massiver Standortnachteil für die Schweiz.

90 Nur diejenigen geheimen Daten sind zu schützen, für die der Geheimnisherr auch eine berechtigte Erwartung an die Geheimhaltung hat. Sofern zwischen dem Geheimnisherrn (d.h. der betroffenen Person) und dem Bearbeiter als Geheimnisträger z.B. eine vertragliche Grundlage für die Bearbeitung besteht, soll auch die Bearbeitung und entsprechende Offenlegung möglich sein.

Besten Dank für die Kenntnisnahme unserer Vernehmlassungsantwort.

Mit freundlichen Grüssen

Pietro Supino
Präsident

Andreas Häuptli
Geschäftsführer

Verband SCHWEIZER MEDIEN
Konradstrasse 14, Postfach, CH-8021 Zürich
Telefon 044 318 64 64, Telefax 044 318 64 62
www.schweizermedien.ch, contact@schweizermedien.ch

SCHWEIZER MARKTFORSCHUNG
Verband Schweizer Markt- und Sozialforschung

Verband Schweizer Markt- und Sozialforschung Gruebengasse 10 6055 Alpnach

Eidgenössisches Justiz- und Polizeidepartement
EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Per E-Mail an: jonas.amstutz@bj.admin.ch

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes 04.04.2017

Sehr geehrte Frau Bundesrätin

Der Verband Schweizer Markt- und Sozialforschung (vsms) wendet sich hiermit im Vernehmlassungsverfahren über die Totalrevision des Datenschutzgesetzes (VE-DSG) an Sie. Wir erbitten höflich um Gelegenheit, Stellung zur geplanten Gesetzesrevision zu nehmen und lassen Ihnen untenstehend im Namen unserer Mitglieder folgende Meinungsäusserung zukommen.

1. Vorstellung des vsms und seiner Mitglieder

Das Tätigkeitsgebiet der Mitglieder des vsms ist die Durchführung von Umfragen bei der Schweizer Bevölkerung. Auftraggeber sind unter anderem der Bund (Bundesamt für Statistik), die Kantone, Gemeinden, Universitäten, Institutionen und private Unternehmen. Wir stellen für die Verwaltung auf Ebene Bund, Kantone, Gemeinden wichtige Planungsgrundlagen zur Verfügung. Unternehmen brauchen die Informationen aus Umfragen als Entscheidungsgrundlagen, um Investitionen und Marketing effizient umzusetzen und erfolgreich neue Produkte zu entwickeln, die den Bedürfnissen der Kunden entsprechen. Beispiele für Studien, die zurzeit von vsms-Instituten durchgeführt werden, sind die Schweizerische Arbeitskräfteerhebung (SAKE), die Einkommens- und Verbrauchserhebung (HABE) oder Nachbefragungen zu den eidgenössischen Abstimmungen.

Die Umfragen werden mittels verschiedener wissenschaftlich fundierter Methoden, namentlich durch schriftliche und persönliche Befragungen, online-Befragungen oder per Telefon durchgeführt. Unsere Dienstleistung und damit der Zweck der Datenbearbeitung unterscheiden sich in folgenden Punkten markant von jenen anderer Unternehmen, welche im Zuge des Verkaufs von Waren- und Dienstleistungen Daten ihrer Kunden „abschöpfen“:

Im Gegensatz zu teilweise praktizierten Methoden im Direkt-Marketing und Verkauf werten wir bei Befragungen Antworten nach wissenschaftlichen Methoden anonym-statistisch aus und verkaufen die Daten nicht an Dritte weiter.

Die Teilnahme an unseren Umfragen ist absolut freiwillig und wir bieten keine oder kaum Gegenleistungen an. Wir sind damit auf den Goodwill der Befragten angewiesen. Eine hohe Teilnahmebereitschaft ist Voraussetzung dafür, dass wir unsere Aufgabe erfüllen können, weil die Ergebnisse sonst nicht repräsentativ sind.

Unsere Tätigkeit ist am ehesten mit Befragungen in der medizinischen Forschung vergleichbar, die ebenfalls auf den Goodwill und die Teilnahmebereitschaft von Patienten angewiesen ist. Aus diesem Grund erscheint eine analoge Betrachtungsweise unserer Tätigkeit mit der Datenbearbeitung im Zusammenhang mit Forschung, Planung und Statistik angebracht.

2. Änderungsanträge zur Revision des Datenschutzgesetzes

Im Zuge der laufenden Gesetzesrevision beantragt der vsms zusammenfassend folgende Änderungen:

- Zu Art. 3 lit. e VE-DSG: Die Legaldefinition des Profiling soll in Anlehnung an die Bestimmung des EU-DSGVO restriktiver gefasst werden, alternativ sei die gesamte lit. e zu streichen;
- Zu Art. 4 Abs. 6 VE-DSG: Die Einwilligung zur Bearbeitung von Daten soll einheitlich geregelt werden; die Kategorien der „eindeutigen“ und der „ausdrücklichen“ Einwilligung seien abzuschaffen;
- Zu Art. 8 VE-DSG: Der vsms lehnt Art. 8 in dieser Form ab. Soll dennoch an der Konzeption festgehalten werden, wird dringend ein Kontrollmechanismus empfohlen, der die faktische Gesetzgebungskompetenz des EDÖB austariert.
- Zu Art. 13 Abs. 2 lit. a und b VE-DSG: Die pauschale Informationspflicht ist nicht sachgerecht und geht zu weit. Der vsms befürwortet eine differenzierte Abstufung der Informationspflichten. Des Weiteren besteht in Art. 13 eine terminologische Unschärfe.
- Zu Art. 24 Abs. 2 lit. e VE-DSG: Die einschränkende Formulierung bei den Rechtfertigungsgründen sei zu streichen und es sei der bisherige Gesetzeswortlaut beizubehalten.

3. Begründung

3.1 Art. 3 lit. f VE-DSG – Begriff – Profiling

Die Revision des Datenschutzgesetzes möchte den Entwicklungen auf der Ebene des Europarates und der Europäischen Union Rechnung tragen. Mit der neuen Begriffsdefinition des Profiling schiesst die schweizerische Revision aber an diesem Ziel vorbei und verleiht dem Begriff einen deutlich umfassenderen Anwendungsbereich als die Begriffsdefinition in Art. 4 Ziff. 3 der EU-

Datenschutzverordnung (EU-DSGVO). Ausserdem wird die Legaldefinition durch die Verwendung des Begriffs „persönliche Merkmale“ selbst auslegebedürftig, was die Aufnahme einer Definition ins Gesetz obsolet werden lässt.

Art. 3 lit. f VE-DSG	Art. 4 Ziff. 3 der EU-Datenschutzverordnung (EU-DSGVO)
„Profiling: jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;“	„Profiling: jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;“

Durch die neue Legaldefinition in Art. 3 lit. f VE-DSG wird das automatisierte und nicht-automatisierte Profiling gleichermassen erfasst, was eine unzulässige Ausweitung des Geltungsbereichs darstellt und damit im Widerspruch zu Art. 2 Abs. 1 VE-DSG steht. Der Vorentwurf unterscheidet zudem genauso wenig nach dem Zweck des Profilings. Dabei ist eine unterschiedliche Behandlung von zentraler Bedeutung: Der vsms ist für die Erstellung von statistischen Zukunftsprognosen (z.B. bei demografischen Studien) auf die prädikative Analytik und damit auf eine automatisierte Datenenbearbeitung angewiesen. Der Wortlaut des Vorentwurfs erlaubt es jedoch nicht, das Profiling zu statistischen (Forschungs-)Zwecken von seinem Geltungsbereich auszunehmen und zwar selbst dann nicht, wenn man bei der prädikativen Analytik ausschliesslich anonymisierte Daten verwendet. Der Rechtsfertigungsgrund in Art. 24 Abs. 2 lit. e VE-DSG bietet für die Mitglieder des vsms keinen genügenden Schutz, da es sich um keinen absoluten Rechtfertigungsgrund handelt (vgl. Ziff. 3.5). Diesem Umstand muss im Zuge der Gesetzgebung Rechnung getragen werden, da ansonsten sowohl eine massive Behinderung der Wirtschaft und der Forschung in der Schweiz droht, als auch eine signifikante Benachteiligung gegenüber Unternehmen auf ausländischen Märkten, welche weniger strengeren Regelungen unterliegen.

Die Begriffsdefinition sollte in Anlehnung an die Bestimmung des EU-DSGVO zwischen dem automatisierten und nicht-automatisierten Profiling unterscheiden. Bei Ersterem ist sodann das

Profiling zu Forschungszwecken – sofern zur Bearbeitung lediglich anonymisierte Daten verwendet werden – von seinem Anwendungsbereich auszunehmen.

Alternativ sei die gesamte lit. f zu streichen.

3.2 Art. 4 Abs. 6 VE-DSG – Grundsätze

Indem der Vorentwurf neu die „eindeutige Einwilligung" vorsieht, schafft der Gesetzgeber ohne Not Rechtsunsicherheit. Bereits unter dem geltenden Recht kommt nämlich der risikobasierte Ansatz zur Anwendung. Dieser Zusatz ist daher wegzulassen und es ist der geltende Wortlaut des Gesetzes weiterzuführen.

Die Einwilligung fürs Profiling soll künftig wie auch zur Bearbeitung von besonders schützenswerten Personendaten gesondert geregelt werden. Es soll dafür eine „ausdrückliche Einwilligung" notwendig sein.

Wann eine „ausdrückliche" Einwilligung vorliegt, ist nicht klar. Dem erläuternden Bericht[1] zufolge kann eine ausdrückliche Einwilligung nicht mehr konkludent erfolgen und muss durch „schriftliche Erklärung (einschliesslich auf elektronischem Weg), eine mündliche Äusserung oder Zeichen gegeben werden. Dies ist insbesondere möglich durch das Ankreuzen eines Kästchens oder das Anklicken einer Schaltfläche (z.B.: «weiter») auf einer Website, die Auswahl bestimmter technischer Parameter für die Dienste eines Informationsverarbeitungsunternehmens oder anderweitige Erklärungen." (Erläuternder Bericht, S. 48). Diese Aufzählung ist beispielhaft und stark auslegungsbedürftig, was wiederum zu kontroversen Diskussionen führen wird. Im Bereich der wissenschaftlichen Umfrageforschung, welche auch besonders schützenswerte Daten zum Gegenstand haben kann (z.B. Religion und Gesundheit), könnte eine solche ausdrückliche Einwilligung nur mit unverhältnismässig hohem Aufwand eingeholt werden. Man denke dabei an die praktische Umsetzung bei Telefonumfragen: Die mündlich erfolgte Einwilligung müsste technisch aufbereitet und zu Beweiszwecken aufbewahrt werden, den Befragten müsste vorgängig zunächst ein Formular zur Einverständniserklärung zugestellt werden etc. Die wissenschaftliche Umfrageforschung würde dadurch praktisch verunmöglicht. Der vsms ist der Auffassung, dass diese gesonderte Regelung zur „ausdrücklichen Einwilligung" ersatzlos zu streichen ist.

Alternativ sei zumindest das Profiling von dieser erhöhten Einwilligungsschwelle auszunehmen, da ansonsten auch die Durchführung unproblematischer Verfahren auf der Basis von prädikativer Analytik (vgl. Ziff. 3.1) dadurch behindert, wenn nicht sogar verunmöglicht wird.

---

[1] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016.

3.3 Art. 8 VE-DSG – Empfehlungen der guten Praxis

Art. 8 VE-DSG äussert sich zu Empfehlungen der guten Praxis und gewährt dem EDÖB diesbezüglich weitreichende Kompetenzen. Den Gedanken der praxisorientierten Selbstregulierung erachtet der vsms im Grundsatz als sinnvoll, weil er ein bewährtes Regulierungsmodell darstellt, das einen hohen Grad an Umsetzbarkeit gewährleistet und erfahrungsgemäss gut geeignet ist, komplexe Sachverhalte vernünftig und sachgerecht zu normieren. Dies wird vor allem dadurch möglich, dass verschiedene Branchen und Interessengruppen wie der vsms ihre jeweiligen Anliegen einbringen können. Der Impuls für Empfehlungen der guten Praxis soll jedoch stets von den interessierten Kreisen aus der Praxis ausgehen. Der VE-DSG hätte jedoch eine derartige Kompetenzerweiterung des EDÖB zur Folge, die dem Gedanken der Selbstregulierung zuwiderliefe. Gemäss Art. 8 Abs. 1 VE-DSG ist es primär der EDÖB, der durch seine Empfehlungen die Datenschutzvorschriften konkretisieren soll.

Sodan ist die Geltungskraft der durch den EDÖB erlassenen Empfehlungen der guten Praxis nicht zu unterschätzen. Art. 9 Abs. 1 VE-DSG setzt die Befolgung der Empfehlungen der guten Praxis mit dem Einhalten der Datenschutzvorschriften gleich, welche durch die Empfehlungen konkretisiert werden sollen. Dem EDÖB wird damit faktisch Gesetzgebungskompetenz eingeräumt.

Der Entstehungsprozess, der zur Formulierung von Empfehlungen der guten Praxis führt, ist allerdings nicht hinreichend definiert. Dieser Umstand wird dadurch verstärkt, dass sogar Empfehlungen der interessierten Kreise einem Genehmigungsvorbehalt des EDÖB unterliegen. Es mangelt damit den quasi-gesetzlichen Empfehlungen der guten Praxis an demokratischer Legitimation. Zudem besteht die Gefahr, dass der EDÖB die Anliegen einzelner Interessengruppen einseitig berücksichtigt. Checks and Balances oder anderweitige Kontrollmechanismen, welche die Machtkonzentration beim EDÖB entschärfen, sind nicht zu identifizieren. Die in dieser Form im VE-DSG vorgesehene Institution der Empfehlungen der guten Praxis mutet willkürlich an und widerspricht dem Grundgedanken der Selbstregulierung.

Der vsms ist der Meinung, dass der EDÖB in der gegenwärtigen Form gut funktioniert und lehnt daher Art. 8 des VE-DSG ab. Soll dennoch an der Konzeption von Art. 8 VE-DSG festgehalten werden, plädiert der vsms für eine Institutionalisierung eines Kontrollmechanismus, welcher die faktische Gesetzgebungskompetenz des EDÖB austariert.

3.4 Art. 13 Abs. 2 lit. a und b VE-DSG – Informationspflicht bei der Beschaffung von Personendaten

Während im gegenwärtig geltenden DSG in Art. 14 die Informationspflichten einzig beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen auferlegt werden, verschärft der VE-DSG diese Pflichten massiv.

Die Informationspflichten des Verantwortlichen gemäss Art. 13 VE-DSG, insbesondere Abs. 2, werden branchenunabhängig und ungeachtet des Geschäftsmodells pauschal auferlegt. Dies erscheint nicht sachgerecht und widerspricht dem zentralen Grundsatz der Verhältnismässigkeit. Im Sinne der Vermeidung überschiessender Regulierung erachtet der vsms eine Abstufung der Informationspflichten als sachgerechteren Lösungsansatz. Eine differenzierte Abstufung könnte etwa nach Art der Datenerhebung (z.B. Telefonumfrage), Sensitivität der zu erhebenden Daten oder Zweck der Beschaffung erfolgen. So erscheint es beispielsweise unverhältnismässig, bei einer kurzen telefonischen Befragung zu rein statistischen Zwecken über nicht sensitive oder zuordenbare Daten die gleich strengen Informationspflichten anzulegen wie bei einer detaillierten Befragung zu sensitiven Themen wie der Gesundheit.

Zudem erscheint es fraglich, inwiefern eine pauschale Informationspflicht dem Zweck des VE-DSG gemäss Art. 1 (Schutz der Persönlichkeit und der Grundrechte natürlicher Personen) dient. Gerade bei Telefonumfragen wäre die verlangte Informationspflicht in ihrem Umfang und Detaillierungsgrad [insbesondere nach lit. a (Kontaktdaten) und lit. b (Kategorien der bearbeiteten Daten)] nicht nur impraktikabel, sondern gar kontraproduktiv.

Müssten die verlangten Informationen nach Abs. 2 zu Beginn eins Anrufes mündlich verlesen werden, erscheint es mehr als fraglich, ob der Befragte die grosse Menge an Informationen derart schnell verarbeiten kann, dass sich seine Informationslage deutlich verbessert. Eine Flut an Information führt nicht automatisch dazu, dass man besser informiert ist. Vielmehr kann eine abschreckende Wirkung nicht ausgeschlossen werden, weshalb die benötigte Dauer für die Kenntnisnahme wohl eine unüberwindbare Hürde für die Teilnahme eines Befragten darstellen würden.

Die wissenschaftlich fundierte Umfrageforschung ist jedoch auf den Goodwill der Befragten angewiesen. Dieser ist gerade bei Umfragen, welche Anspruch auf Repräsentativität erheben (z.B. für das Bundesamt für Statistik), besonders wichtig. Daher ist eine praktikable Regelung der Informationspflicht mit Augenmass nicht nur für die Branche wichtig, zumal repräsentative Umfragen für statistische Erhebungen vor allem im öffentlichen Bereich von generellem Nutzen sind. Eine Abstufung der Informationspflichten ist daher dringend zu empfehlen.

Terminologisch schafft die Verwendung der Begriffe „Beschaffung/Bearbeitung“ Raum für Unklarheiten. Art. 13 VE-DSG verwendet die Begriffe „Beschaffung/beschaffen“ sowie „Bearbeitung/bearbeiten“ in nicht konsequenter Weise. Art. 3 lit. d VE-DSG definiert den Begriff „Bearbeiten“ und legt fest, dass damit unter anderem das Beschaffen gemeint sei. Somit ist der

Begriff des „Bearbeitens“ weiter gefasst als jener des „Beschaffens“. Es erstaunt daher, dass in Art. 13 VE-DSG Abs. 1 lediglich von „Beschaffung“ die Rede ist, während in Abs. 2 die Informationspflicht auf den weiteren Begriff des „Bearbeitens“ abzielt. Dies erscheint für die Informationspflicht bezüglich des Zwecks sinnvoll (Abs. 2 lit. c), weniger jedoch für die Informationspflicht bezüglich der Personendaten oder die Kategorie der bearbeiteten Personendaten (Abs. 2 lit. b). Hier wäre „Beschaffen“ wohl angebrachter. Der vsms ist daher der Auffassung, dass eine terminologische Überarbeitung sinnvoll ist.

3.5 Art. 24 VE-DSG – Rechtfertigungsgründe

Der vsms begrüsst, dass der Vorentwurf bei der Erhebung von Personendaten zu nicht personenbezogenen Zwecken, insbesondere in der Forschung, Planung und Statistik weiterhin ein überwiegendes Interesse statuiert (Art. 24 Abs. 2 lit. e VE-DSG).

Diesem Rechtfertigungsgrund droht künftig jedoch eine schwächere Bedeutung zugemessen zu werden, wenn der Passus „fällt insbesondere in Betracht“ durch „ist möglicherweise gegeben“ ersetzt wird.

Datenschutzgesetz (aktuell) Art. 13 Ab. 2	Datenschutzgesetz (neu, VE) Art. 24 Abs. 2
„Ein überwiegendes Interesse der bearbeitenden Person fällt insbesondere in Betracht, wenn diese:“	„Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser“

Dem erläuternden Bericht lässt sich dafür keine Begründung entnehmen. Klar ist jedoch, dass mit dieser Aufzählung keine absoluten Rechtfertigungsgründe geschaffen werden sollen (Erläuternder Bericht, S. 69); die Rechtslage bleibt demnach unverändert. Aus Gründen der Rechtsicherheit ist deshalb am bisherigen Wortlaut festzuhalten.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Hochachtungsvoll

Dr. Stefan Oglesby
Mitglied des vsms Präsidiums

Nicole Siegrist
Geschäftsführerin vsms

VEREINIGUNG SCHWEIZERISCHER NACHRICHTENOFFIZIERE
ASSOCIATION SUISSE DES OFFICIERS DE RENSEIGNEMENTS
ASSOCIAZIONE SVIZZERA DEGLI UFFICIALI INFORMATORI

VSN ▪ c/o Brunau-Stiftung ▪ Edenstrasse 20 ▪ 8027 Zürich

via E-Mail: jonas.amstutz@bj.admin.ch
Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
CH – 3003 Bern

Bern, 4. April 2017

Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Vernehmlassung der Vereinigung Schweizerischer Nachrichtenoffiziere

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Ich bedanke mich im Namen der Vereinigung Schweizerischer Nachrichtenoffiziere bestens für die Gelegenheit zur Teilnahme am titelerwähnten Vernehmlassungsverfahren und unterbreite Ihnen nachfolgend gerne unsere Stellungnahme, enthaltend folgende

Anträge:

1. Die Tätigkeit nachrichtendienstlicher Organe sei vom Geltungsbereich des Datenschutzgesetzes vollumfänglich **auszunehmen** (zu Art. 2).

2. Es sei eine **Ausnahme zur Bekanntgabe von Daten ins Ausland** für nachrichtendienstliche Organe im Gesetz aufzunehmen (zu Art. 6).

3. Es sei eine weitere **generelle Ausnahme von der Informationspflicht** für nachrichtendienstliche Organe vorzusehen (zu Art. 14).

4. Nachrichtendienstliche Organe seien insb. von den **Pflichten gemäss Art. 17 und Art. 18 DSG** zu entbinden (zu Art. 17 und 18).

5. Nachrichtendienstliche Organe seien (unter Vorbehalt der nachrichtendienstlichen Aufsicht) von der **Pflicht zur Dokumentation** ihrer Datenbearbeitung zu entbinden (zu Art. 19).

6. Es sei im Rahmen der weiteren gesetzgeberischen Arbeiten gutachterlich zu prüfen, ob die im Nachrichtendienstgesetz enthaltenen Grundlagen als formell-gesetzliche Grundlage im Sinne von Art. 27 DSG genügend ist. Verneinendenfalls seien diese Grundlagen vor Erlass

des DSG entsprechend anzupassen, oder aber in Art. 27 DSG sei ein entsprechender **Vorbehalt für nachrichtendienstliche Tätigkeiten** anzubringen (zu Art. 27).

7. Es sei zu prüfen, inwiefern die **verschärften Straf- und Offenlegungsbestimmungen** für Private dazu führen, dass diese von einer proaktiven Zusammenarbeit mit Polizei- und Staatsschutzorganen abgehalten werden (zu Art. 50ff).

8. Der Nachrichtendienst des Bundes sei durch eine entsprechende Änderung des Nachrichtendienstgesetzes zum **Profiling** zu berechtigen (zu Änderungen bisherigen Rechts).

* * * * *

Begründung:

Der vorliegende Erlassentwurf hat weitereichende Änderungen im schweizerischen Datenschutzrecht zur Folge. Ob diese Änderungen und insbesondere die deutlich schärfere Gangart im Sanktionswesen gesellschaftspolitisch gewünscht sind, wird hier nicht kommentiert.

Ziel der vorliegenden Eingabe ist einzig, die Auswirkungen des neuen Datenschutzrechts auf die Tätigkeit der Nachrichtendienste zu thematisieren. Es ist in dieser Hinsicht insbesondere darauf zu achten, dass die Dienste bei ihrer nachrichtendienstlichen Tätigkeit nicht durch das Datenschutzrecht eingeschränkt werden.

Allgemein fällt auf, dass die Thematik von Nachrichtendienst und Staatsschutz im Erlassentwurf wie auch in der Botschaft kaum thematisiert werden. Dieses Versäumnis ist wo notwendig nachzuholen.

Soll die nachrichtendienstliche Tätigkeit im Einzelfall eingeschränkt werden, so ist dies durch entsprechende Kontrolle und Aufsicht, sowie durch die Vorgabe von entsprechenden Grundsätzen im Nachrichtendienstgesetz selbst vorzunehmen. Zusätzliche Einschränkungen nachrichtendienstlicher Tätigkeiten im Datenschutzgesetz führen zu Doppelspurigkeiten und sind letztlich auch gesetzessystematisch verfehlt. Am Saubersten wäre es daher, wenn nachrichtendienstliche Tätigkeiten (die berechtigten Organe sind im Nachrichtendienstgesetz abschliessend aufgezählt) **vollständig vom Geltungsbereich des Datenschutzgesetzes ausgenommen** wären.

Kommt eine solche Regelung aus politischen Erwägungen nicht in Betracht, so sind immerhin an verschiedener Stelle **Vorbehalte zu Gunsten nachrichtendienstlicher Tätigkeiten** im Datenschutzgesetz vorzusehen. Diese Vorbehalte betreffen insbesondere die weitgehenden Informations- und Offenlegungspflichten, die das neue Gesetz zum Schutz der Privatsphäre einführt, die aber im nachrichtendienstlichen Bereich eben gerade hinderlich sind und nicht selten nachrichtendienstliche Tätigkeit geradezu vereiteln.

Es kann überdies nicht sein, dass das vom Stimmvolk mit komfortabler Mehrheit angenommene und damit bestens demokratisch legitimierte Nachrichtendienstgesetz nun wiederum durch

datenschutzrechtliche Bestimmungen aufgeweicht und verwässert wird. Eine solche Verwässerung wäre weder politisch noch gesetzgeberisch sinnvoll.

Schliesslich erlaube ich mir den Hinweis auf die **administrativen Folgen** des Datenschutzgesetzes für den Nachrichtendienst. Der Dienst sieht sich heute bereits einer umfassenden und strikten Kontrolle durch eine mehrstufige Aufsicht unterstellt. Wiederum kann nicht angehen, dass der Nachrichtendienst nun durch Doppelspurigkeiten, welche das Datenschutzgesetz auch in administrativer Hinsicht schafft, zusätzlich belastet wird (z.B. weitestgehende Dokumentationspflichten). Der Erlassentwurf ist auch diesbezüglich daher erneut kritisch zu prüfen.

* * * * *

Wir danken Ihnen bestens für die Gelegenheit, an Ihrer Vernehmlassung mitzuwirken und hoffe, Ihnen mit diesen Ausführungen gedient zu haben. Genehmigen Sie, sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren, den Ausdruck meiner

vorzüglichen Hochachtung.

VEREINIGUNG SCHWEIZERISCHER NACHRICHTENOFFIZIERE (VSN)

Michael Suter
Präsident

Amstutz Jonas BJ

Von: Andrea Hordynski <Andrea.Hordynski@vsud.ch>
Gesendet: Dienstag, 4. April 2017 14:45
An: Amstutz Jonas BJ
Betreff: Totalrevision des Dantschutzgesetzes
Anlagen: VSUD Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de.doc

Sehr geehrter Herr Amstutz

Vielen Dank für die Gelegenheit zum erläuternden Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG) sowie zu den Änderungen weiterer Erlasse zum Datenschutz Stellung zu nehmen.

Anbei erhalten Sie unserer Stellungnahme im dafür vorgesehenen Formular.

Für die Berücksichtigung unserer Anliegen danken wir Ihnen im Voraus und stehen Ihnen für weitere Fragen gerne zur Verfügung.

Freundliche Grüsse
Andrea Hordynski

Andrea Hordynski
Rechtskonsulentin
Vereinigung Schweizerischer Unternehmen
in Deutschland (VSUD)
Hirzbodenweg 95
CH - 4052 Basel
Tel.: 0041 61 375 95 00
Fax: 0041 61 375 95 01
e-mail: andrea.hordynski@vsud.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Vereinigung Schweizerischer Unternehmen in Deutschland

Abkürzung der Firma / Organisation : VSUD

Adresse : Hirzbodenweg 95, CH- 4052 Basel

Kontaktperson : Stefanie Luckert, Andrea Hordynski

Telefon : 061 375 95 00

E-Mail : info@vsud.ch

Datum : 04. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
VSUD	Sehr geehrte Damen und Herren Vielen Dank für die Gelegenheit zum erläuternden Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG) sowie zu den Änderungen weiterer Erlasse zum Datenschutz Stellung zu nehmen. Die Vereinigung Schweizerischer Unternehmen in Deutschland (VSUD) ist der branchenübergreifende Zusammenschluss der in Deutschland investierenden schweizerischen Unternehmen aller Branchen und Grössenordnungen. Die Mitgliedsunternehmen der VSUD sind sowohl in der Schweiz als auch in Deutschland aktiv.
VSUD	Da die Mitgliedsunternehmen der VSUD grenzüberschreitendtätig sind, zählt auch der Transfer von Kunden- und Mitarbeiterdaten aus der EU in die Schweiz bzw. innerhalb eines Konzerns und die Beachtung des damit verbunden Datenschutzrechts zu deren Tätigkeiten. Das bisherige schweizerische Datenschutzniveau hat sich hierfür bewährt.
VSUD	Grundsätzlich begrüsst die VSUD jede Massnahme, durch die das schweizerische Bundesdatenschutzgesetz an das Datenschutzniveau der Europäischen Union sowie an die revidierte Konvention 108 des Europarates angepasst wird. Eine Anpassung des geltenden Bundesgesetzes über den Datenschutz sollte allerdings nicht auf Kosten der von kleinen und mittelständischen Unternehmen, sog. KMU, erfolgen. Die KMU sollten nicht mit zusätzlichem Bürokratieaufwand wie zusätzliche Informations- und Begründungspflichten, der Implementierung eines Folgeabschätzungsverfahrens und eines Datenschutzverantwortlichen belastet werden. Auch die Durchsetzung der Datenschutzvorschriften sollte wie bisher effizient und kostengünstig bleiben. In den Bereichen, in denen eine Anpassung an die EU-Datenschutzgrundverordnung (DSGVO) und die revidierte Konvention 108 des Europarates nicht erforderlich ist, sollte auf die Einführung von Regelungen verzichtet werden. Daher sollte nach Ansicht der VSUD von Schweizer Seite her darauf verzichtet werden, über die Vorgaben der DSGVO und der revidierten Konvention 108 des Europarates hinaus strengere Regelungen zu erlassen. Regelungen, die strenger und ineffizienter sind als die Vorschriften der DSGVO, sind nicht erforderlich, damit die Schweiz weiterhin als Land mit einem angemessenen Datenschutzniveau von der Europäischen Union anerkannt wird. Zudem könnten strengere Regelungen im Datenschutz zu einem Wettbewerbs- oder Standortnachteil für Schweizer Unternehmen führen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
VSUD	DSG	Art. 3		Lit. c, Ziff. 4	Die Ziffer 4 des Entwurfs geht über die Vorgaben der Konvention 108 hinaus und sollte daher entsprechend angepasst werden. Es sollte sich hier nur um biometrische Daten handeln, die zum Zweck bearbeitet werden, eine natürliche Person zu identifizieren.
VSUD	DSG	Art. 3		Lit. f	Die Definition des Begriffs „Profiling“ geht hier weiter als der in der DSGVO. Bei der Formulierung „Daten oder Personendaten“ ist der Hinweis auf Daten zu streichen. Das DSG gilt nur für die Bearbeitung von Daten natürlicher Personen. Denn auch bei der Auswertung von Daten muss es sich um solche von natürlichen Personen handeln.
VSUD	DSG	Art. 4	3		Hier stellt sich die Frage, unter welchen Voraussetzungen die Beschaffung von Personendaten für die betroffene Person für einen Zweck „klar“ erkennbar ist. Um hier Rechtsunsicherheit zu vermeiden, sollte das Wort „klar“ gestrichen werden.
VSUD	DSG	Art.4	4		Diese Vorschrift sollte gestrichen werden. Die Dauer der Aufbewahrung von Personendaten ist bereits vom Grundsatz der Verhältnismässigkeit gedeckt, welcher in Art. 4 Abs. 2 geregelt ist.
VSUD	DSG	Art. 4	5		Aus den Erläuterungen zum Vernehmlassungsentwurf des DSG ist nicht nachvollziehbar, warum der Wortlaut der Vorschrift geändert wurde. Ferner müsste der Verantwortliche ständig überprüfen, ob die Daten richtig sind und wenn nötig, ob sie nachgeführt worden sind. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Diese dauerhafte Überprüfungspflicht ist kaum erfüllbar. Zudem entsteht beim Verantwortlichen ein zusätzlicher Aufwand und die betroffene Person wird mit Informationen überflutet.

					Hier sollte die alte Formulierung des Art. 4 Abs. 5 weiter verwendet werden.
VSUD	DSG	Art. 5	2		Positiv und zu begrüssen ist die Einführung des Entscheids des Bundesrats zum angemessenen Schutz der Daten im Ausland. Somit muss nicht mehr der Datenexporteur beurteilen, ob die Daten im Ausland angemessen geschützt sind, sondern er kann sich neu auf den Entscheid des Bundesrates verlassen.
	DSG	Art. 5	5		Fraglich ist, ob ein Verantwortlicher oder Auftragsbearbeiter im schlimmsten Fall sechs Monate warten will um einen Datentransfer ins Ausland vorzunehmen. Die sechs Monatsfrist ist zu lange und sollte daher auf eine Frist von höchstens 30 Tagen angepasst werden oder ganz gestrichen werden.
VSUD	DSG	Art. 5	6		Die DSGVO sieht keine Informationspflicht des Beauftragten in dem Fall vor, in dem der Verantwortliche oder Auftragsbearbeiter von den Standardklauseln Gebrauch macht. Daher sollte auf eine solche Informationspflicht im DSG verzichtet werden.
VSUD	DSG	Art. 6	2		Eine derartige Mitteilungspflicht gegenüber dem Beauftragten sieht die DSGVO nicht vor. Die Schweizer Regelung geht damit weiter als die entsprechende Regelung in der DSGVO. Art. 6 Abs. 2 sollte daher ersatzlos gestrichen werden. Ferner werden Unternehmen dazu verpflichtet, dem Beauftragten Geschäftsinternas mitzuteilen. Diese wären aufgrund des Öffentlichkeitsgrundsatzes auch für Dritten einsehbar. Auch deswegen ist die Vorschrift zu streichen.
VSUD	DSG	Art. 8			Fraglich ist hier, inwieweit Verantwortliche oder Auftragsbearbeiter verpflichtet sein werden, die Empfehlungen der guten Praxis zu übernehmen.
VSUD	DSG	Art. 9			Die Übernahme der Empfehlungen der guten Praxis sollte freiwillig sein. Der Verantwortliche sollte keinem Nachteil ausgesetzt werden, wenn er die Empfehlungen der guten Praxis nicht übernimmt.
VSUD	DSG	Art. 12			Diese Regelung sollte gestrichen werden. Weder die DSGVO noch die Konvention 108 enthalten eine Regelung zur Bearbeitung von Daten verstorbener Personen. Art. 12 des Vernehmlassungsentwurfs zum DSG beruht auf einer öffentlichen Diskussion. Ferner sollte beachtet werden, dass die Regelung in dieser Form nicht nur soziale Medien betrifft, sondern auch Unternehmen, die Daten von natürlichen Personen

					bearbeiten. Zu beachten ist, dass die Persönlichkeit einer Person mit dem Tod endet, § 31 ZGB. Vorschriften, welche sich mit der Nachwirkung des Endes einer Persönlichkeit befassen, fehlen im ZGB. Zudem ist unklar, welche Interessen eine verstorbene Person hat. Unklar ist auch, wie der Verantwortliche überprüfen soll, ob die einsichtverlangende Person mit der verstorbenen Person eine faktische Lebensgemeinschaft führte. Ferner haben Erben die Möglichkeit sich auf das allgemeine Löschungs- und Berichtigungsrecht zu berufen, sofern sie einen Anspruch auf Löschung ihrer eigenen Daten haben.
VSUD	DSG	Art. 13	2		Unklar ist hier, welche Informationen der Verantwortliche der betroffenen Person mitteilen muss, damit diese ihre Rechte nach dem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist. Da eine Verletzung der Informationspflicht nach dem Entwurf strafbar sein soll, werden Verantwortliche gezwungen, der betroffenen Person mehr Informationen mitzuteilen, als sie tatsächlich müssen. Dies verursacht bei den Verantwortlichen einen grösseren Aufwand.
VSUD	DSG	Art. 13	4		Die Informationspflicht in Abs. 4 geht über die DSGVO hinaus. Die DSGVO sieht nicht vor, dass der Verantwortliche auch über die Identität und die Kontaktdaten des Auftragsbearbeiters informieren muss. Beides sollte gestrichen werden. Die Bekanntgabe der Identität und der Kontaktdaten sollte allenfalls im Rahmen des Auskunftsrechts möglich sein.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	Art. 15	2		Dieser Absatz sollte gestrichen werden. Die betroffene Person hat bereits nach Art. 4 Abs. 5 des Vernehmlassungsentwurfs zum DSG die Möglichkeit sich zu den über sie bearbeitenden Personendaten zu äussern. Zudem sieht die DSGVO ein Recht zur Äusserung zu den bearbeitenden Daten zu automatisierten Einzelfallentscheidungen nicht vor.
VSUD	DSG	Art. 15			Insgesamt ist die Regelung zu automatisierten Einzelfallentscheidung im Art. 15 des Vernehmlassungsentwurfs zum DSG strenger als in der DSGVO oder in der revidierten Konvention 108 vorgesehen. So sieht Art. 15 Vernehmlassungsentwurf zum DSG keine Ausnahmen vor, wie es die DSGVO vorsieht. Die Vorschrift sollte überarbeitet werden und ebenfalls Ausnahmen vorsehen.

VSUD	DSG	Art. 16	1		Gemäss der Vorschrift muss der Auftragsbearbeiter eine Datenschutz-Folgeabschätzung durchführen. Es ist zu bezweifeln, ob er fähig sein wird, dieser Pflicht nachzukommen. Die DSGVO sieht eine Übertragung der Pflicht zur Datenschutz-Folgeabschätzung nicht vor. Die schweizerische Vorschrift im Entwurf geht damit weiter als die Vorschrift in der DSGVO. Zur Datenschutz-Folgeabschätzung sollte allein der Verantwortliche verpflichtet werden. Ein voraussichtliches „erhöhtes Risiko“ als Voraussetzung zur Durchführung einer Datenschutz-Folgeabschätzung ist eine zu niedrige Hürde. Jede Form der Bearbeitung von Daten stellt ein voraussichtliches „erhöhtes Risiko“ dar. Um eine Sanktion zu vermeiden, würden Unternehmen bei jeder Datenbearbeitung vorab eine Datenschutz-Folgeabschätzung vornehmen. Dies stellt einen enormen Verwaltungs- und Kostenaufwand für die Wirtschaft dar. Ein Verstoss gegen das Datenschutzgesetz wird dadurch nicht verhindert. Ferner sollte Art. 16 eine abschliessende Aufzählung von Fällen enthalten, in denen Unternehmen eine Datenschutz-Folgeabschätzung vornehmen müssen. Der Verweis auf die Grundrechte der betroffenen Personen sollte gestrichen werden. Private Unternehmen sind nicht verpflichtet, die Grundrechte von natürlichen Personen zu wahren.
VSUD	DSG	Art. 16	4 und 3		Beide Absätze sind zu streichen. Die DSGVO sieht weder eine Pflicht des Verantwortlichen oder Auftragsbearbeiters den Beauftragten über die Ergebnisse der Datenschutz-Folgeabschätzung zu informieren noch hat der Beauftragte ein Vetorecht.
VUSD	DSG	Art. 17	1		Diese Regelung gilt über die Bestimmung der DSGVO hinaus, da diese Meldepflicht jede Datenbearbeitung erfassen soll, die gegen das Bundesgesetz zum Datenschutz verstösst. Diese Meldepflicht würde damit viel mehr Fälle erfassen als die Meldepflicht nach der DSGVO und würde den Beauftragten mit Meldungen überfluten. Ferner kann es innerhalb eines Unternehmens zu Konflikten kommen, wenn der betriebliche Datenschutzbeauftragte Kenntnisse von Datenschutzverstössen im Betrieb erlangen würde. So müsste er jeden Mitarbeiter anzeigen, der eine Datenschutzverletzung im Betrieb begangen hat. Zudem müsste jeder Mitarbeiter, der eine Datenschutzverletzung begangen hat, dies melden und sich damit selbst belasten. Diese Pflicht zur Selbstanzeige steht im Widerspruch zu dem Grundsatz, sich im

					Strafverfahren nicht selbst belasten zu müssen. Auch die Pflicht „unverzüglich“ einen Datenschutzverstoss zu melden, ist oft nicht möglich. So muss dem betrieblichen Datenschutzbeauftragten die Zeit bleiben, sich ein Bild von der möglichen Datenschutzverletzung zu machen, um zu entscheiden, ob diese tatsächlich vorliegt. Art. 17. Abs. 1 ist aus diesen Gründen entweder zu streichen oder allenfalls auf den Inhalt der Bestimmung der DSGVO zu reduzieren.
VSUD	DSG	Art. 18	1		Die Übertragung der Pflicht zum Datenschutz durch Technik und zur Implementierung von datenschutzfreundlichen Voreinstellungen auf den Auftragsbearbeiter ist nicht in der DSGVO vorgesehen. Diese Pflichten sollten nur auf den Verantwortlichen beschränkt werden. Es ist auch nicht nachvollziehbar, warum diese Pflichten auch auf den Auftragsbearbeiter übertragen werden sollte, da dieser in der Regel nicht in der Lage sein wird, diese Pflichten zu erfüllen.
VSUD	DSG	Art.19		Lit. b	Auch die Übertragung der Pflichten zur Berichtigung und Löschung von Daten auf den Auftragsbearbeiter geht weiter als in der DSGVO vorgesehen. Die Pflichten zur Berichtigung und Löschung von Daten sollten auf den Verantwortlichen begrenzt werden. Die Informationspflicht sollte auf Fälle beschränkt werden, in denen die betroffene Person ein schützenwertes Interesse hat oder sie die Nachinformationen aufgrund berechtigter Gründe verlangen kann. Ansonsten würde die Informationspflicht ausufern und jedes Unternehmen müsse seine Datenbanken ständig dahingehend prüfen, wem es die Daten der betroffenen Personen mitgeteilt hat und die betroffenen Personen darüber informieren. Auch die Regelung geht hinsichtlich der mitzuteilenden Daten über die DSGVO hinaus. So müssen auch Verletzungen des Datenschutzes vom Datenempfänger mitgeteilt werden, selbst dann, wenn die betroffenen Personen nicht informiert werden müssen. Der Wortlaut unterscheidet auch nicht zwischen den meldepflichtigen Datenschutzverletzungen und denen, die nicht meldepflichtig sind.
VSUD	DSG	Art. 23	2	Lit. d	Die Norm sollte gestrichen. Resultieren aus einem Profiling Personendaten, so werden diese Personendaten vom DSG geschützt. Eine gesonderte Aufführung des Profilings ohne ausdrückliche Einwilligung als Persönlichkeitsverletzung ist aus diesem Grund nicht erforderlich. Müsste ein

					Unternehmen, welches bei der Durchführung eines Profilings Personendaten erhält, jede betroffene Person informieren und eine ausdrückliche Einwilligung der betroffenen Person einholen, um eine Persönlichkeitsverletzung zu vermeiden, würde dies einen erheblichen Aufwand für das Unternehmen bedeuten.
VSUD	DSG	Art. 24	2		Das Wort „möglicherweise“ sollte gestrichen werden. Es sorgt bei den Beteiligten für Rechtsunsicherheit.
VSUD	DSG	Art. 41	4		Unklar ist, warum der Beauftragte gegenüber privaten Personen und Bundesorganen tätig werden darf, ohne dass eine konkrete Datenschutzverletzung vorliegt. Dieser Absatz ist zu streichen.
	DSG	Art.44	3		Beschwerden gegen vorsorgliche Massnahmen sollte eine aufschiebende Wirkung haben. Vor allem im Bereich der automatisierten Datenbearbeitung ist z. B. eine Löschung von Daten oder ein Bearbeitungsstopp als vorsorgliche Massnahmen oft nicht möglich bzw. oft mit hohen Kosten für die Unternehmen verbunden. Das betroffene Unternehmen sollte die Chance haben, eine vorsorgliche Massnahmen des Beauftragten durch ein Gericht überprüfen zu lassen. Die Vorschrift ist dementsprechend zu streichen oder anzupassen.
VSUD	DSG	Art. 50ff			Die Art. 50 ff des Vernehmlassungsentwurfs zum Bundesgesetz über den Datenschutz gehen weiter als die DSGVO. Ein strafrechtliches Sanktionssystem ist in der DSGVO nicht vorgesehen und geht entschieden zu weit. Auch sieht die DSGVO keine primäre strafrechtliche Verantwortung von Privatpersonen vor. Eine Strafbarkeit von Privatpersonen führt dazu, dass die Unternehmen entsprechende Compliance-Systeme einführen werden, um diese Personen zu finden, damit diese zur Rechenschaft gezogen werden können. Die Einführung dieser Compliance-Systeme würde zur Zunahme des Complianceaufwands und der –kosten in den Unternehmen führen. Aufgrund der Compliance werden die Unternehmen gezwungen, die Arbeitsverhältnisse mit den betroffenen Mitarbeitern zu beenden. Diese Mitarbeiter werden es in Zukunft schwerer haben bei anderen Unternehmen wieder eingestellt zu werden. Ferner ist zu befürchten, dass die Mitarbeiter dazu neigen könnten, sich gegenseitig anzuzeigen. Besser wäre es ein verwaltungsrechtliches Sanktionssystem einzuführen. Primär verantwortlich sollten nicht Privatpersonen sein, sondern die Unternehmen, da die Bearbeitung von Daten im Verantwortungsbereich der Unternehmen erfolgt. Das datenschutzwidrige Verhalten einer Privatperson z.

					B. eines Mitarbeiters könnte die Sanktion gegen das Unternehmen reduzieren. Im Gegensatz zur DSGVO, welche von den Mitgliedstaaten nur die Einführung von Rechtsbehelfen, die im Fall einer Geldbusse abschreckend und verhältnismässig sein müssen, sieht das DSG einen Sanktionskatalog vor. Der in den Art. 50 und 51 vorgesehen Sanktionskatalog ist nicht erforderlich, um ein mit der EU vergleichbares Datenschutzniveau in der Schweiz sicherzustellen. Zudem ist die Höhe der Sanktion unverhältnismässig. Ferner sollte auf Freiheitsstrafen verzichtet werden. Unklar ist, bei den Art. 50 – 52 des Vernehmalssungsentwurfs zum DSG antragsberechtigt sein soll. Daher sollte das Sanktionssystem in den Art. 50 ff des Vernehmlassungsentwurfs zum DSG bearbeitet werden.
VSUD	DSG	Art. 50	4		Für fahrlässiges Handeln sollte keine Sanktion vorgesehen werden. Ansonsten würde derjenige bestraft werden, der lediglich eine Pflicht im Sinne des DSG zu verletzt, und nicht nur derjenige der Personendaten bewusst zweckwidrig und unverhältnismässig verwendet. Der Absatz ist daher zu streichen.
VSUD	DSG	Art. 51	2		Der Absatz ist aus den gleichen Gründen wir zu Art. 50 Abs. 4 des Vernehmlassungsentwurfs zum DSG zu streichen.
VSUD	DSG	Art.52			Auf Freiheitsstrafen sollte verzichtet werden. Die Vorschrift ist ersatzlos zu streichen.
VSUD	DSG	Art. 54			Nicht nachvollziehbar ist, warum das Untersuchungsverfahren nach Art. 44 des Vernehmlassungsentwurfs des DSG sich nach dem Verwaltungsverfahrensgesetz richtet und die Verfolgung und die Beurteilung der strafbaren Handlungen den Kantonen obliegen soll. Dies würde dazu führen, dass die Staatsanwaltschaften der einzelnen Kantone sich mangels Datenschutzerfahrung an der Einschätzung des Beauftragten orientieren müssten. Diese Regelung ist daher ineffizient. Auch hier sollte über das Verwaltungsverfahrensgesetz der Verwaltungsrechtsweg gelten.
VSUD	DSG	Art. 55			Die Verjährungsfrist sollte auf drei Jahre verkürzt werden.

VSUD	DSG	Art. 59			Es ist nicht nachvollziehbar, warum die Übergangsbestimmung von zwei Jahren nur für die Datenschutz-Folgeabschätzung und die Massnahmen nach den Art. 18 und 19 a) gelten soll. Damit die Unternehmen ausreichend Zeit haben, alle Datenschutzvorschriften des revidierten DSG in die Praxis umzusetzen, sollte das DSG eine generelle Umsetzungsfrist von mindestens zwei Jahren vorsehen. Der Art. 59 ist dementsprechend anzupassen.

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")		
Name/Firma	**Kapitel-Nr.**	**Bemerkung/Anregung**

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
VSUD	8.1.1.3	Art. 3 f DSG: Profiling Der Begriff Profiling im Vernehmlassungsentwurf zum DSG geht weiter als der Begriff in der DSGVO. Gemäss den Erläuterungen sieht der Begriff auch die manuelle Auswertung von Daten wie z. B. das Ausfüllen eines Bewertungsbogens für Mitarbeiter oder, die Prognose zur Entwicklung der wirtschaftlichen Lage eines Versicherten durch einen Versicherer vor. Damit würden diese Auswertungen nach den Vorschriften im Vernehmlassungsentwurf zum DSG eine Verletzung der Persönlichkeit darstellen (Art. 23 VE DSG), wofür wiederum ein Rechtfertigungsgrund oder die ausdrückliche Einwilligung des Betroffenen erforderlich wäre. Daher sollte die manuelle Auswertung von Daten nicht vom Profiling erfasst werden.
VSUD	8.1.2.1	Art. 4 Abs. 6 Einwilligung Hier ist darauf hinzuweisen, dass es ausreicht, wenn die Einwilligung grundsätzlich nur den Teil einer Bearbeitung abdeckt, für welchen sie eingeholt worden ist. Die Einwilligung muss nicht wie in den Erläuterungen formuliert den gesamten Zweck einer Bearbeitung abdecken. Die Erläuterungen sollten dementsprechend angepasst werden. Um Rechtsunsicherheit zu vermeiden, sollte in den Erläuterungen dargestellt werden, worin der Unterschied zwischen einer eindeutigen und einer ausdrücklichen Einwilligung besteht.
VSUD	8.1.2.1	Art. 4 Abs. 3 Grundsätze Aus den Erläuterungen lässt sich nicht entnehmen, in welchem Fall der Zweck zur Datenbeschaffung für die betroffene Person „klar“ erkennbar sein soll. Daher sollte entweder in den Erläuterungen aufgeführt werden, unter welchen Umständen der Zweck „klar“ erkennbar ist oder das Wort „klar“ sollte aus dem Abs. 3 gestrichen werden.
VSUD	8.1.3.1	Art. 13 Abs. 2 Informationspflicht Gemäss den Erläuterungen soll künftig der Verantwortliche entscheiden, welche Informationen die betroffene Person von ihm benötigt, um ihre Rechte nach dem DSG geltend zu machen. Dies führt allerdings zur Rechtsunsicherheiten und dazu, dass Unternehmen sich verpflichtet fühlen, mehr Informationen der betroffene Person mitzuteilen, als diese eigentlich benötig. Daher

		sollte die Erläuterung hier klarer gefasst werden. Sie sollte keine Mindestangaben sondern abschliessende Angaben enthalten.
VSUD	8.1.3.4	Art. 16 Datenschutz-Folgeabschätzung Hier ist fraglich, in welchen Fällen von einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen auszugehen ist. Gemäss den Erläuterungen ist von einem erhöhten Risiko auszugehen, wenn die Verfügungsfreiheit der betroffenen Person über ihre Daten erheblich eingeschränkt wird oder werden kann. Dies wird in sehr vielen Fällen der Fall sein. Was bedeutet, dass die Unternehmen in all diesen Fällen eine Datenschutz-Folgeabschätzung vorzunehmen haben. Dies wäre mit einem erheblichen Aufwand und mit Rechtsunsicherheit für die Unternehmen verbunden. Um dies zu vermeiden, sollte in den Erläuterungen oder in einer Verordnung abschliessende Fallgruppen aufgeführt werden, in welchen Fällen ein erhöhtes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen. Ferner lässt sich aus den Erläuterungen nicht entnehmen, in welchen Fällen bei einer Datenverarbeitung durch ein privates Unternehmen die Grundrechte der betroffenen Personen berührt werden. „die Grundrechte“ sind daher aus Art. 16 Abs. 1 des Vernehmlassungsentwurfs des DSG zu streichen.
VSUD	8.1.3.7	Art. 19 lit. a Weitere Pflichten Nach den Erläuterungen ist der Auftragsbearbeiter verpflichtet ebenfalls Datenschutzverstösse im Sinne von Art. 17 des Vernehmlassungsentwurfs zu dokumentieren. Diese zusätzliche Dokumentationspflicht bedeutet für den Auftragsbearbeiter einen zusätzlichen Aufwand. Dadurch lassen sich Datenschutzverstösse nicht vermeiden. Hier reicht es grundsätzlich aus, wenn die Pflicht auf die Dokumentation der Datenbearbeitung beschränkt bleibt. Um Rechtsunsicherheiten zu vermeiden, sollte definiert werden, wer mit „Empfängerinnen oder Empfänger von Personendaten“ im Sinne von Art. 19 lit. b des Vernehmlassungsentwurf zum DSG gemeint ist.
VSUD	8.1.5.1	Art. 23 Abs. 3 Persönlichkeitsverletzungen Gemäss den Erläuterungen zu Art. 23 Abs. 3 des Vernehmlassungsentwurfs zum DSG liegt keine Persönlichkeitsverletzung vor, wenn die Bearbeitung rechtmässig erfolgte, d. h. die Grundsätze von Art. 4 bis 6 und 11 eingehalten wurden. Dies ist so nicht richtig. Erfolgt die Veröffentlichung der Daten willentlich und wissentlich durch die betroffene Person, dann wäre die Bearbeitung dieser Daten nach dem Vernehmlassungsentwurf auch dann rechtmässig, wenn sie unter Verletzung der Bearbeitungsgrundsätze erfolgt.

Verband Schweizerischer Vermögensverwalter I VSV
Association Suisse des Gérants de Fortune I ASG
Associazione Svizzera di Gestori di Patrimoni I ASG
Swiss Association of Asset Managers I SAAM

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Herr Jonas Amstutz

Zürich, 4. April 2017

Nur per Email: jonas.amstutz@bj.admin.ch

Vernehmlassung: Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Wir nehmen Bezug auf Ihre Einladung vom 21. Dezember 2016, uns zu eingangs genanntem Gesetzgebungsprojekt vernehmen zu lassen. Wir möchten uns für diese Gelegenheit bedanken.

Zur Vernehmlassungsvorlage nimmt der VSV als führender nationaler Branchenverband der unabhängigen Vermögensverwalter in der Schweiz gerne in beiliegender, tabellarischer Form Stellung.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer
Vermögensverwalter | VSV

Alexander Rabian
Vorsitzender der Geschäftsleitung SRO

Ralph Frey
Mitglied der Geschäftsleitung SRO

Beilage erwähnt

Bahnhofstrasse 35
CH-8001 Zürich
Tel. 044 228 70 10
Fax 044 228 70 11
info@vsv-asg.ch
www.vsv-asg.ch

Chantepoulet 12
CH-1201 Genève
Tél. 022 347 62 40
Fax 022 347 62 39
info@vsv-asg.ch
www.vsv-asg.ch

Via Landriani 3
CH-6900 Lugano
Tel. 091 922 51 50
Fax 091 922 51 49
info@vsv-asg.ch
www.vsv-asg.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Verband Schweizerischer Vermögensverwalter (VSV)

Abkürzung der Firma / Organisation : VSV

Adresse : Bahnhofstrasse 35, 8001 Zürich

Kontaktperson : Alexander Rabian

Telefon : 044 208 25 25

E-Mail : alexander.rabian@streichenberg.ch

Datum : 04.04.2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
VSV	**Die Vorlage trägt der Situation der aufgrund finanzmarktregulatorischer Vorgaben zur Bearbeitung von besonders schützenswerten Personendaten und zum Profiling verpflichteten Finanz-KMU überhaupt keine Rechnung.**
	Der VSV vertritt als grösster und einziger nationaler Branchen- und Berufsverband die Interessen der unabhängigen Vermögensverwalter („uVV“) in der Schweiz. Die uVV sind über diverse finanzmarktaufsichtsrechtliche Erlasse in die gesetzliche und durch Behördenrundschreiben (insbesondere der FINMA) und Regulierungen behördlicher anerkannter Selbstregulierungsträgern (insbesondere Selbstregulierungsorganisation nach dem Geldwäschereigesetz (GwG) und Branchenorganisationen nach Kollektivanlagengesetz (KAG)) in die teilweise sehr komplexe Regulierung der Finanzmärkte und Finanzdienstleistungen eingebunden. Zudem sind auch uVV direkt oder indirekt (d.h. über die Depotbanken, bei denen Kundenvermögen deponiert sind) zu Steuerzwecken, insbesondere zur Durchführung des Automatischen Informationsaustauschs in Steuersachen (AIA) Personendaten zu bearbeiten. Diese zahlreichen Regulierungen unterschiedlichster Stufen verpflichten die uVV zur Bearbeitung von Personendaten. Von diesen Datenbearbeitungen betroffen sind primär die Kunden im In- und Ausland, über welche (insbesondere, aber nicht nur) nach den Vorgaben des GwG in erheblichem Umfang besonders schützenswerte Personendaten zu bearbeiten. Diese betreffend Daten über • religiöse Ansichten oder Tätigkeiten (namentlich im Hinblick auf die Prävention und Bekämpfung der Terrorismusfinanzierung) • politische, weltanschauliche oder gewerkschaftliche Tätigkeiten (namentlich im Hinblick auf die Identifikation politisch exponierter Personen und das Management der mit der Betreuung solcher Kunden verbundenen Risiken) • über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen (namentlich im Hinblick auf Erkennung und die Erfüllung gesetzlicher Meldepflichten im Zusammenhang mit Geldwäscherei- und Terrorismusfinanzierungsrisiken) Die bearbeiteten (auch besonders schützenswerten) Personendaten sind durch die uVV auszuwerten, mit dem Ziel, wesentliche persönliche Merkmale zu erkennen und zu analysieren und/oder zukünftige Entwicklungen hervorzusagen, namentlich in Bezug auf gegenwärtige und zukünftige Geldwäschereirisiken (namentlich die zukünftige Beibringung von Geldern durch Kunden zur Vermögensverwaltung) und Risiken der Terrorismusfinanzierung (namentlich Risiken beim Abzug von Geldern) und entsprechende Massnahmen im Rahmen des Risikomanagement, der Erfüllung von Meldepflichten und der Ausübung von Melderechten zu treffen. Die uVV sind also gehalten, Profiling im Sinne von Art. 3 VE-DSG zu betreiben, wenn sie ihre finanzmarktaufsichtlichen Pflichten erfüllen wollen. Als Arbeitgeber haben uVV zudem unter den Gesichtspunkten der Gewähr für eine einwandfreie Geschäftstätigkeit, Daten über verwaltungs- oder

	strafrechtliche Verfolgungen und Sanktionen ihrer Mitarbeitenden zu bearbeiten. Diese durch die Finanzmarktregulierung vorgegebenen Datenbearbeitungen sind mit wenigen Ausnahmen nicht auf der Stufe des Gesetzes im formellen Sinne vorgegeben. Sie ergeben sich in ihrer grossen Mehrheit aus der dem Gesetz nachgelagerten Regulierung, namentlich aus FINMA-Verordnungen und –Rundschreiben sowie der von der FINMA anerkannten Selbstregulierung. Besondere Beachtung aus datenschutzrechtlicher Sicht verdient dabei der sog. „risikobasierte Ansatz“, der für die Bearbeitung von Kundendaten (insbesondere zu GwG-Zwecken) im Ergebnis besagt, dass sich Umfang und Mass der zu bearbeitenden und zu profilierenden Kundendaten aus der Risikobeurteilung durch den Finanzintermediär bestimmt. Das Ausmass der Datenbearbeitung wird also nicht primär durch das Gesetz bestimmt, sondern durch die Risikobeurteilung der bei einem Finanzintermediär dafür zuständigen Person (im Regelfall eines entsprechend sachkundigen und geschulten Compliance-Officers). Diesen besonderen Umständen der Unternehmen, die aufgrund einer sehr allgemein gehaltenen gesetzlichen Grundlage, besonders schützenswerte Personendaten bearbeiten müssen und mit diesen auch Profiling betreiben müssen, trägt der VE-DSG keinerlei Rechnung. Die uVV müssen sich durch regulatorische Vorgaben im datenschutzrechtlichen Hochrisikobereich bewegen, wobei ihnen der VE-DSG keinerlei Rechtssicherheit (insbesondere durch Safe Harbour-Regeln) geben will. Der VE ist durch entsprechende Erleichterungen und Safe Harbour-Regeln zu ergänzen.
VSV	
	Die Vorlage überfordert Finanz-KMU, die aufgrund finanzmarktregulatorischer Vorgaben zur Bearbeitung von besonders schützenswerten Personendaten und zum Profiling verpflichtet sind
	Die Branche der uVV in der Schweiz setzt sich weit überwiegend aus Klein- und Kleinstunternehmen zusammen. Im „durchschnittlichen“, der SRO des VSV angeschlossenen Vermögensverwaltungsunternehmen sind rund 3.8 Personen beschäftigt. Die administrative Belastung für die KMU (Datenschutzverantwortlicher, Folgeabschätzungen, Informationspflichten unklaren Umfangs, Begründungspflichten für Entscheide, etc. etc.) wird durch den VE und die Regulierungsfolgenabschätzung völlig unterschätzt. Selbst dort, wo die Botschaft im Interesse der Wirtschaft auf die Praktikabilität eingeht, spiegelt sich dies im Wortlaut der Vorlage häufig nicht (so etwa bei den Informationspflichten). Die Vorlage ist nicht KMU-tauglich. Die wohlwollende Haltung der RFA durch PwC teilen wir nicht.
VSV	
	Verhältnis von neueren Bestimmungen eines revDSG zu älteren Verordnungsbestimmungen
	Es fehlt an Übergangsbestimmungen, die regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
VSV	VE-DSG	1			
VSV	VE-DSG	2	2	c	Beibehaltung des geltenden Wortlauts. Der VE will nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch kantonale Justizbehörden soll die bisherige Einschränkung also nicht mehr gelten. Das ist weder sinnvoll, noch schlüssig. Insbesondere sind Zivil- und Strafprozess auf Bundesebene einheitlich geregelt, entsprechend muss auch das Datenschutzrecht für die Verfahren nach diesen Gesetzen auf der Ebene der Eidgenossenschaft einheitlich geregelt sein. Das Verhältnis zu Art. 2 Abs. 3 VE-DSG ist unklar.
VSV	VS-DSG	2	3		Es ist nichts dagegen einzuwenden, dass das Datenschutzrecht für die Rechtsprechungstätigkeit der Gerichte keine Geltung haben soll. Für den Bereich der Justizverwaltung (d.h. die Selbstverwaltung der Justizbehörden) muss das Datenschutzrecht aus Gründen der Rechtsgleichheit der von Verwaltungsmass-nahmen betroffenen natürlichen Personen Geltung haben. Dies namentlich mit Bezug auf Arbeitnehmer-daten. Es ist nicht zielführend hier jedem eidgenössischen Gericht eine eigene Kompetenz einzuräumen, die dann weitgehend vom Legalitätsprinzip ausgenommen bleibt, und in welcher Verstösse nicht geahndet werden können.
VSV	VE-DSG	3		c	*Ziff. 4: Begriff der biometrischen Daten*: Auch elektronisch gespeicherte Fotografien sind biometrische Daten, die – jedenfalls bei ausreichender Qualität – eine eindeutige Personenidentifikation erlauben. Damit ist jede elektronisch gespeicherte Ausweiskopie mit Lichtbild bei einem Finanzintermediär eine Bearbeitung besonders schützenswerter Personendaten. Da Finanzintermediäre nach dem GwG ihre Kunden (und deren Vertreter) ausnahmslos über amtliche Ausweise mit Lichtbildern identifizieren und entsprechende Kopien anfertigen müssen, bearbeitet jeder Finanzintermediär von vornherein in grossem Umfang besonders schützenswerte Personendaten.

					Das geht zu weit. Entweder sind Lichtbilder *per se* von der Definition der besonders schützenswerten Personendaten auszunehmen, oder es sind im Sinne der anderen Ausführungen in dieser Vernehmlassung besondere Regeln für Finanzintermediäre im Sinne des GwG zu erlassen.
VSV	VE-DSG	3		c	*Ziff. 1: Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Tätigkeiten:* Die Qualifikation jeglicher Information über politische oder gewerkschaftliche Tätigkeiten als besonders schützenswerte Personendaten geht zu weit. Das reine Faktum, dass eine natürliche Person ein politisches Amt, eine leitende Stellung in einer Partei oder einer Gewerkschaft innehat, ist an sich noch nicht besonders schützenswert. Diese Daten sind in der Regel öffentlich bekannt. Die Bekanntmachung erfolgt mit der Zustimmung der Person, die das jeweils in Frage stehende bzw. die in Frage stehende Tätigkeit ausübt. Die natürliche Person kann hier keinen Anspruch und auch kein legitimes Interesse an besonderem Schutz mehr geltend machen. Auch Art. 10 der RL (EU) 2016/680 sieht in solchen Fällen kein besonderes Schutzbedürfnis. Art. 3 Bst. c. Ziff. 1 VE-DSG ist deshalb dahingehend anzupassen, dass die Ausübung politischer Ämter und leitender Ämter in der Verwaltung, in politischen Parteien und Gewerkschaften keine besonders schützenswerten Daten darstellen.
VSV	VE-DSG	3		f	Der VSV hat keine Einwände dagegen, dass der in hohem Masse unscharfe Begriff des „Persönlichkeitsprofil“ aufgegeben wird und durch einen Begriff ersetzt wird, der in der Verwendung heute üblich ist. Der Definition des neuen Begriffs, des Profiling wird im VE-DSG allerdings zu weit gefasst. Die reine Analyse von Kundendaten, welche seine Einkommens- und Vermögenslage im Zusammenhang mit Risiken der Prävention und Bekämpfung von Geldwäscherei und Terrorismusbekämpfung analysiert, würde unter den Begriff des Profiling fallen. Das geht zu weit. Die Erfüllung der Pflichten aus dem Geldwäschereigesetz kann nicht unter die höchstregulierte Kategorie der Datenbearbeitung fallen. Die Auswirkungen sind durch KMU im Finanzsektor nicht mit verkraftbarem Aufwand zu erfüllen. Entsprechend ist der Begriff des Profiling einzuschränken. Die Einschränkung hat zumindest darin zu bestehen, dass die Analyse von Einkommens- und Vermögenslage zur Erfüllung regulatorischer Vorgaben kein Profiling darstellt.
VSV	VE-DSG	3		h	Der Begriff des Verantwortlichen ist jedenfalls für den Privatsektor unverständlich definiert. Zum einen ist der Verantwortliche nicht zwingend identisch mit dem Inhaber einer Datensammlung. So weit so gut. Als

					Verantwortlicher gilt jedoch jede natürliche oder juristische Person, welche den Zweck, Umfang und die Mittel der Datenbearbeitung (mit-)bestimmt. Unklar bleibt demnach, ob jede natürliche Person, die einem geschäftsführenden Organ einer datenbearbeitenden juristischen Person damit zum „Verantwortlichen" wird und dies auch auf Dauer bleibt; und sei dies nur, weil sie in Wahrnehmung von Oberleitungsfunktionen über Reglemente und Weisungen sowie über das Budget mitentscheidet. Damit würde auch jedes nicht operativ tätige Verwaltungsratsmitglied automatisch zum Verantwortlichen, ohne dass das jeweilige Verwaltungsratsmitglied die entsprechenden Aufgaben in der Datenbearbeitung (und damit die Verantwortung) auch effektiv wahrnehmen kann. Implizite würde damit eine neue unentziehbare und unübertragbare Aufgabe für alle Verwaltungsratsmitglieder in Analogie zu Art. 716a OR geschaffen. Das kann nicht die Stossrichtung des VE-DSG sein. Die dem Verantwortlichen durch den VE zugewiesenen Aufgaben können nur durch operativ tätige Personen wahrgenommen werden. Entsprechend ist eine zusätzliche Bestimmung in den VE aufzunehmen, die es Kollektivorganen erlaubt, den oder die Verantwortlichen näher zu bestimmen.
VSV	VE-DSG	3		i	Der Begriff des Auftragsbearbeiters ist unklar definiert und erfasst. Er vermischt – jedenfalls, wenn man dem Erläuterungsbericht folgen will – datenschutzrechtliche Regelungen mit solchen des Vertrags-, Sozialversicherungs- und sogar des Personalverleihrechts. Im Ergebnis soll nur, wer zum Verantwortlichen in einem direkten Arbeitsverhältnis nach OR steht, kein Auftragsbearbeiter sein. Wer hingegen in anderer Weise in die Betriebsorganisation des Verantwortlichen eingebunden ist, aber aufgrund eines Auftrags (wie z.B. ein leitendes Organ) oder eines Entleihverhältnisses tätig ist, würde zum Auftragsbearbeiter. Dies entbehrt jeglicher Konsistenz. Entscheidend kann nur die Einbindung in die Betriebs- oder Unternehmensorganisation des Verantwortlichen sein. Die Formulierung ist wie folgt zu ergänzen: „..oder die im Auftrag des Verantwortlichen Personendaten bearbeitet, ohne in dessen betriebliche Organisation eingebunden zu sein."
VSV	E-DSG	4	3		Das Wort „klar" ist zu streichen. Der Erläuterungsbericht stellt dar, dass keine materielle Änderung beabsichtigt ist. Trifft dies zu, dann ist auch Wortlaut nicht zu ändern. Soll allerdings doch materiell abweichend legiferiert werden, so wäre das Wort „klar" ebenfalls zu streichen. Der Zweck der Datenbearbeitung durch Private, welche auf der Grundlage regulatorischer Vorgaben (hier namentlich durch das GwG und seine weitreichende Ausführungsgesetzgebung) erfolgt, verfolgt den zunächst den allgemeinen Zweck der Prävention und Bekämpfung von Geldwäscherei und

					Terrorismusfinanzierung. Andererseits dürfen und sollen dieselben Daten aber auch zu anderen Zwecken verwendet werden, wobei diese bei Datenerhebung in der Regel nicht oder wenigstens nicht abschliessend feststehen. So müssen, dürfen und werden namentlich zu GwG-Zwecken erhobene Daten zu Zwecken des Automatischen Informationsaustausches in Steuersachen verwendet. Dabei steht derzeit noch nicht feststeht, mit welchen Staaten, ab wann, welche Daten ausgetauscht werden. Bei der Datenerhebung sind also die regulatorischen Zwecke, zu welchen die Daten dereinst werden sollen oder gar müssen, noch gar nicht klar fest. Entsprechend dürften einmal zu Zwecken der der Prävention und Bekämpfung von Geldwäscherei und Terrorismusfinanzierung gar nie zu AIA-Zwecken erhoben werden, da dies für die betroffenen Personen gar nicht erkennbar war. Auf einer solchen Grundlage sind Datenschutz und Datenbearbeitung aufgrund der sich dynamisch entwickelnden Finanzmarktregulierung niemals vereinbar. Der Gesetzgeber würde so nur ein Durcheinander veranstalten. Entsprechend genügt es, wenn der Zweck der Datenbearbeitung für die betroffene Person in allgemeiner (und nicht in abschliessend klarer) Weise erkennbar ist.
VSV	VE-DSG	4	4		Die Bestimmung steht im Widerspruch zu regulatorischen Aufbewahrungspflichten, insbesondere, aber nicht nur nach dem GwG. Die GwG-relevanten Daten sind für 10 Jahre auch über die Beendigung einer Geschäftsbeziehung aufzubewahren und haben nach betroffenen Personen erschliessbar zu bleiben. Entsprechend ist die Bestimmung wie folgt zu ergänzen: „Vorbehalten bleiben gesetzliche und regulatorische Aufbewahrungspflichten.“
VSV	VE-DSG	4	5		Die Bestimmung steht im Widerspruch zu regulatorischen Datenbearbeitungspflichten, insbesondere, aber nicht nur nach dem GwG. Die GwG-relevanten Daten sind auch dann zu bearbeiten und nach betroffenen Personen erschliessbar, wenn sie falsch sind. Entsprechend ist die Bestimmung wie folgt zu ergänzen: „Vorbehalten bleiben gesetzliche und regulatorische Aufbewahrungspflichten.“
VSV	VE-DSG	4	6		Gegen eine angemessene Information der betroffenen Person in die Datenbearbeitung ist nichts einzuwenden. Jedoch dürfen keine übertriebenen Anforderungen an die Einwilligung in die Datenbearbeitung verlangt werden, wenn diese aufgrund gesetzlicher oder regulatorischer Vorschriften erfolgt. Dies muss auch für die Bearbeitung besonders schützenswerter Daten und das Profiling auf der Grundlage entsprechender Vorschriften gelten. Ist die Bearbeitung besonders schützenswerter Personendaten und Profiling regulatorisch vorgeschrieben, so muss es genügen, wenn die Information aus

					einem Hinweis auf den zugrundeliegenden Erlass (konkret das GwG) besteht und die Einwilligung implizite erfolgt. Missbräuche der Daten sind bei beaufsichtigten Finanzdienstleistern durch das Aufsichtsregime auszuschliessen. Entsprechend ist die Bestimmung wie folgt zu ergänzen: „Erfolgt die Datenbearbeitung (unter Einschluss der Bearbeitung besonders schützenswerter Personendaten und des Profiling) aufgrund gesetzlicher oder regulatorischer Vorschrift, so ist die betroffene Person über den Erlass, auf dessen Grundlage die Datenbearbeitung erfolgt, zu informieren. Nach entsprechender Bekanntgabe stimmt die betroffene Person durch Bekanntgabe der Daten der Bearbeitung zu. Eine durch die gesetzliche oder regulatorische Grundlage nicht vorgesehene Bekanntgabe bearbeiteter Daten an Dritte, ist – mit Ausnahme der Bekanntgabe an in zulässiger Weise beigezogene Auftragsbearbeiter - diesfalls ausgeschlossen." Zudem ist das Übergangsrecht unklar, wenn es um das Profiling auf kontinuierlicher Basis aufgrund von vorbestehenden Daten geht. Das muss geregelt werden.
VSV	VE-DSG	7	2		Der VE ist ausführlich genug. Es bedarf keiner weiteren, durch den Bundesrat eingeführten Pflichten der Auftragsbearbeiter. Der letzte Satz ist ersatzlos zu streichen.
VSV	VE-DSG	8			Die Bestimmung ist ersatzlos zu streichen. Es geht aus rechtsstaatlichen Überlegungen nicht an, durch die Kompetenz zur Festlegung von „Empfehlungen der guten Praxis" den Beauftragten faktisch zum Verordnungsgeber zu machen und ihm so – jenseits jeder demokratischen Kontrolle – gesetzgeberische Befugnisse zu übertragen, ohne dass klar geregelt wird, wie die rechtliche Überprüfung solcher Empfehlungen erfolgt.
VSV	VE-DSG	9			Vgl. Bemerkungen zu Art. 8. Die Bestimmung ist in diesem Kontext ebenfalls ersatzlos zu streichen.
VSV	VE-DSG	12	3		Das Berufsgeheimnis der Anwälte, Notare und Ärzte ist zu schützen. Angehörigen dieser Berufskategorien werden regelmässig Informationen anvertraut, die höchstpersönlicher Natur sind, und deren Vertraulichkeit über den Tod verlangt wird. Dies ist zu respektieren, auch wenn diese Daten über den Tod des Patienten oder Klienten hinaus, in nach der betroffenen Person erschliessbarer Weise aufbewahrt und damit bearbeitet werden bzw. infolge der Berufspflichten aufbewahrt werden müssen. Bei Einführung einer solchen Bestimmung werden Anwälte, Notare und Ärzte zukünftig gehalten sein, die Offenlegungspflicht gegenüber Angehörigen gegen die Verletzung der eigenen beruflichen

					Aufbewahrungspflichten abzuwägen, um höchstpersönliche Interessen Verstorbener sachgerecht zu wahren. Die Bestimmung ist neu wie folgt zu formulieren: „Das Berufsgeheimnis der Anwälte, Notare und Ärzte bleibt vorbehalten. Das Amts- und andere Berufsgeheimnisse können nicht geltend gemacht werden.“
VSV	VE-DSG	12	4		Die Bestimmung widerspricht den Aufbewahrungspflichten mehrerer finanzmarktaufsichtlicher Erlasse, namentlich dem GwG. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode, die Persönlichkeitsrechte gehen nicht auf die Erben oder gar auf Dritte (Nicht-Erben) über. Die Löschungspflicht steht zudem zu obligationenrechtlichen Buchführungspflichten, welche auch die Aufbewahrung von nach Personen erschliessbarer Geschäftskorrespondenz und weiteren Geschäftsakten verlangen, in diametralem Widerspruch. Die Bestimmung ist ersatzlos zu streichen oder aber um einen Bst. c wie folgt zu ergänzen: „c. die Personendaten des Erblassers sind aufgrund gesetzlicher oder regulatorischer Pflicht über den Tod hinaus zu bearbeiten.“ Die nachfolgende Bestimmung des Abs. 5 ist hier ungenügend, da sie nach „speziellen Bestimmungen“ und nicht nach implizite geltenden oder durch die Aufsichtspraxis entwickelten Grundsätzen verlangt.
VSV	VE-DSG	13	Alle		Die Bestimmung steht bezüglich der regulatorisch vorgeschriebenen Datenbearbeitung durch dem GwG unterstehende Finanzdienstleister in grossen Teilen „völlig quer in der Landschaft“. Die Ausführungs-gesetzgebung zum GwG und die anwendbare Selbstregulierung sehen die Beschaffung und die anderweitige Bearbeitung von Daten beim Vertragspartner, bei und durch Dritte vor. Dabei handelt es sich zumindest teilweise um besonders schützenswerte Daten sowie um Daten, die zu Profiling-Zwecken verwendet werden. Gegen eine Pflicht, in allgemeiner Form über die gesetzliche Grundlage der Datenbearbeitung und die Tatsache, dass die gesetzlich und regulatorisch verlangten Daten bearbeitet werden (vgl. dazu auch die Bemerkungen zu Art. 4 Abs. 6 VE-DSG) zu informieren, ist nichts einzuwenden. Eine umfassende Information über die bearbeiteten Personendaten oder deren (im Gesetz nicht näher definierten Kategorien) geht zu weit. Finanzintermediäre, die aufgrund gesetzlicher Vorgaben Daten bearbeiten, bedürfen damit für die Zwecke

					von Art. 13 einer Sonderordnung. Die ist zweckmässigerweise wie folgt in einen neuen Abs. 6 in Art. 13 VE-DSG aufzunehmen: „Erfolgt die Datenbearbeitung (unter Einschluss der Bearbeitung besonders schützenswerter Personendaten und des Profiling) aufgrund gesetzlicher oder regulatorischer Vorschrift, so ist die betroffene Person anstelle der in den Absätzen 1 bis 5 vorgesehenen Informationen nur über den Erlass, auf dessen Grundlage die Datenbearbeitung erfolgt, zu informieren.“
VSV	VE-DSG	13	1		Vgl. die allgemeinen Bemerkungen zu Art. 13 VE. Bezüglich der der Informationspflicht bei der Datenbeschaffung bei Dritten wird verlangt, dass auch hier ein allgemeiner Hinweis auf die gesetzliche Grundlage genügen muss.
VSV	VE-DSG	13	2		Vgl. die allgemeinen Bemerkungen zu Art. 13 VE. Bezüglich der der Informationspflicht bei der Datenbeschaffung bei Dritten wird verlangt, dass auch hier ein allgemeiner Hinweis auf die gesetzliche Grundlage genügen muss. Der Zweck der Datenbearbeitung ergibt sich aus dem Zweck, des im Rahmen der Information anzugebenden Erlasses.
VSV	VE-DSG	13	3		Vgl. die allgemeinen Bemerkungen zu Art. 13 VE. Im Übrigen widerspricht die Information der betroffenen Person über die Datenbekanntgabe an Dritte den Bestimmungen der Art. 9 ff. GwG über die Meldepflicht und dem Art. 305ter Abs. 2 StGB über das Melderecht.
VSV	VE-DSG	13	4		Vgl. die vorstehenden Ausführung zu Art. 4 Abs. 6 VE-DSG.
VSV	VE-DSG	13	5		Vgl. die allgemeinen Bemerkungen zu Art. 13 VE.
VSV	VE-DSG	14	2	a	Die Datenbearbeitung nach dem GwG folgt einem risikobasierten Ansatz. Dabei wird nicht ausdrücklich im Gesetz festgelegt, welche Daten gespeichert oder anderweitig zu bearbeiten sind. Art und Umfang der zu bearbeitenden Daten werden – im Rahmen der Anwendung des risikobasierten Ansatzes durch den einzelnen Finanzintermediär – im Rahmen von dessen (bei kleinen Finanz-KMU regelmässig äusserst rudimentär formulierten) Risikopolitik bestimmt. Dabei hat der einzelne Finanzintermediär einen sehr weiten Ermessensspielraum, den Art und den Umfang der zu bearbeitenden Daten über seine Kunden, Kontrollinhaber und wirtschaftlich Berechtigte zu bestimmen. Die Formulierung, wonach eine Informationspflicht bloss entfällt, wenn die Speicherung oder Bekanntgabe ausdrücklich im Gesetz (und nicht etwa in nachgeordneten Behördenrundschreiben oder Selbstregulierungen) vorgesehen ist, schützt

					damit Finanzintermediäre unzureichend. Die Bestimmung von Art. 14 Abs. 2 Bst. a VE-DSG müsste demnach lauten: „a. die Speicherung oder die Bekanntgabe der Daten ~~ausdrücklich im~~ durch Gesetz oder regulatorische Vorschrift vorgesehen ist oder gestützt auf entsprechende Vorschriften erlaubt ist;“
VSV	VE-DSG	14	3	a	Die Datenbearbeitung nach dem GwG folgt einem risikobasierten Ansatz. Dabei wird nicht ausdrücklich im Gesetz festgelegt, welche Daten gespeichert oder anderweitig zu bearbeiten sind. Art und Umfang der zu bearbeitenden Daten werden – im Rahmen der Anwendung des risikobasierten Ansatzes durch den einzelnen Finanzintermediär – im Rahmen von dessen (bei kleinen Finanz-KMU regelmässig äusserst rudimentär formulierten) Risikopolitik bestimmt. Dabei hat der einzelne Finanzintermediär einen sehr weiten Ermessensspielraum, den Art und den Umfang der zu bearbeitenden Daten über seine Kunden, Kontrollinhaber und wirtschaftlich Berechtigte zu bestimmen. Die Formulierung, wonach eine Informationspflicht bloss entfällt, wenn die Speicherung oder Bekanntgabe ausdrücklich im Gesetz (und nicht etwa in nachgeordneten Behördenrundschreiben oder Selbstregulierungen) vorgesehen ist, schützt damit Finanzintermediäre unzureichend. Die Bestimmung von Art. 14 Abs. 2 Bst. a VE-DSG müsste demnach lauten: „a. ein Gesetz oder eine Regulierung ~~im formellen Sinn~~ dies vorsieht; oder;“
VSV	VE-DSG	14	5		Wird im Sinne der vorstehenden Überlegungen zu Art. 13 des VE für Datenbearbeitungen gestützt auf Gesetz oder Regulierung bloss eine Informationspflicht durch Hinweis auf den Erlass, der Grundlage für die Datenbearbeitung bildet, als genügend erachtet, so ist es unsinnig, nachträgliche weitergehende nach Abs. 5 von Art. 14 zu verlangen. Die Bestimmung ist daher wie folgt zu ergänzen: „…unverhältnismässigen Aufwand zu erreichen. Die nachträgliche Benachrichtigung entfällt, wenn die Datenbearbeitung (unter Einschluss der Bearbeitung besonders schützenswerter Personendaten und des Profiling) aufgrund gesetzlicher oder regulatorischer Vorschrift erfolgte oder erfolgt.“
VSV	VE-DSG	15	Alle		Das GwG überlässt es den Finanzintermediären, ob sie den Entscheid über Aufnahme oder Ablehnung einer neuen Geschäftsbeziehung (teilweise) aufgrund einer automatisierten Datenbearbeitung vornehmen wollen. Zu den Entscheidungskriterien, bei denen solche Entscheide aufgrund einer automatisierten Datenbearbeitung erfolgt, gehören oft besonders schützenswerte Personendaten. So kann z.B. die geschäftspolitische Grundsatzentscheidung, keine Geschäftsbeziehungen mit politisch exponierten Personen im In- oder Ausland einzugehen, bzw. solche Geschäftsbeziehungen bei Erkennung einer politischen Exposition zu beenden, im Einzelfall automatisiert erfolgen, so dass Mitarbeitende keine

					Möglichkeit haben, solche Entscheidungen zu übersteuern. In solchen Fällen der offensichtlich zulässigen Betätigung der Vertragsfreiheit im Rahmen der unternehmensspezifischen Risikopolitik geht ein Informations- und Anhörungspflicht zu weit. Die Bestimmung würde überdies Finanzintermediäre zwingen, gegen Informationspflichten aus Art. 9 ff. GwG zu verstossen, wenn die eine automatisierte Ablehnung im Zusammenhang mit einer Verdachtsmeldung steht. Zudem geht die Bestimmung über Art. 22 DSGVO hinaus. Die Bestimmung ist entweder ersatzlos zu streichen, oder wenigstens ist Abs. 3 der Bestimmung wie folgt zu ergänzen: „Die Informations- und Anhörungspflicht entfällt, wenn die Datenbearbeitung (unter Einschluss der Bearbeitung besonders schützenswerter Personendaten und des Profiling) aufgrund gesetzlicher oder regulatorischer Vorschrift erfolgte oder erfolgt.“
VSV	VE-DSG	16	Alle		Die durch das GwG vorgegebenen Datenbearbeitungen führen mit Sicherheit zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person. Immerhin geht es um die systematische Bearbeitung von besonders schützenswerten Personendaten einer grossen Zahl von Personen und das Profiling. Weder das geltende DSG, noch der VE enthalten sinnvolle Regelungen für die Datenbearbeitung durch Finanzintermediäre aufgrund gesetzlicher und regulatorischer Vorgaben. Die erhöhte Gefährdung von Persönlichkeit und Grundrechten ist aber durch den Gesetzgeber, die Aufsichtsbehörden und die zugelassenen Selbstregulierungsträger gewollt. Im Falle des GwG handelte der Gesetzgeber in Nachachtung international anerkannter Grundsätze der OECD. Die Datenschutz-Folgenabschätzung wurde im Gesetzgebungsprozess getroffen. Die Risiken sind durch Gesetzgebung und Regulierung in Kauf genommen. Massnahmen zur Verringerung der Gefährdung bewegten sich automatisch im Dunstkreis der vorsätzlichen Schlechterfüllung der gesetzlichen und regulatorischen Pflichten. Aus diesem Grund ist es sinn- und zweckwidrig, dass rund 5‘000 dem GwG unterstehende Finanzintermediäre in der Schweiz, darunter rund 2‘000 unabhängige Vermögensverwalter, eine Datenschutz-Folgenabschätzung erstellen, darin festhalten, was die gesetzlichen und regulatorischen Verpflichtungen sind, und die Unmöglichkeit von risikomildernden Massnahmen beschreiben, und dieses Abschätzungen dem Beauftragten vorlegen, der offensichtlich keine Kompetenz hat, gegen die (vor allem im GwG) vorgesehen Datenbearbeitungen vorzugehen.

					Entsprechend ist Art. 16 durch einen zusätzlichen Abs. 5 zu ergänzen, zweckmässigerweise mit folgendem Wortlaut: „Die Pflichten nach dem Abs. 1 bis 4 entfallen, wenn die Datenbearbeitung (unter Einschluss der Bearbeitung besonders schützenswerter Personendaten und des Profiling) aufgrund gesetzlicher oder regulatorischer Vorschrift erfolgt.“
VSV	VE-DSG	17			Finanzintermediäre, die Daten aufgrund gesetzlicher oder regulatorischer Vorschriften bearbeiten, unterstehen entweder der Aufsicht der FINMA oder Aufsicht einer durch diese bewilligten und beaufsichtigten Selbstregulierungsorganisation. Die korrekte Bearbeitung von Personendaten nach den Aufsichtsgesetzen untersteht damit bereits der direkten oder indirekten Aufsicht durch die FINMA. Die Schaffung eines parallelen Aufsichts- und Repressionssystems durch den Datenschutzbeauftragten ist damit weder notwendig noch sinnvoll. Art. 17 verstösst sodann generell gegen das Nemo tenetur-Prinzip und damit gegen die EMRK, da eine unbefugte Datenbearbeitung nach Art. 179^{novies} VE-StGB mit Strafe bedroht werden soll. Entsprechend geht die Bestimmung auch über die DSGVO hinaus (Art. 33 DSGVO – unter Beachtung der Erwägungsgründe 85ff.). Art. 17 ist damit ersatzlos zu streichen. Soll die Bestimmung gleichwohl beibehalten werden, so sind deren Abs. 1 und 2 soweit nicht anwendbar zu erklären, als dass Daten gestützt auf gesetzliche oder regulatorische Vorschriften bearbeitet werden, und die entsprechende Geschäftstätigkeit einer Aufsicht unterliegt. Ein entsprechender Abs. 5 müsste lauten: „Die Absätze 1 und 2 finden keine Anwendung auf Verantwortliche, die Personendaten gestützt auf gesetzliche und regulatorische Vorschriften bearbeiten, sofern der Geschäftsbereich, in welchem die Daten bearbeitet werden, einer behördlichen Aufsicht oder der Aufsicht eines behördlich zugelassenen Selbstregulierungsträgers oder einer behördlich zugelassenen Aufsichtsorganisation unterliegt.“
VSV	VE-DSG	18			Die Bestimmung ist redundant, der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen. ¨ Die Bestimmung ist ersatzlos zu streichen.

VSV	VE-DSG	19		a	Die stipulierte Dokumentationspflicht würde für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. KMU im Finanzbereich verfügen nicht über ausgebaute Datensysteme, welche jede Datenbearbeitung in einem Log aufzeichnen, und so jede Veränderung von bearbeiteten Personendaten zu dokumentieren. Die Anschaffung entsprechender Datensysteme würde die allermeisten KMU im Finanzsektor finanziell überfordern. Die Bestimmung ist ersatzlos zu streichen.
VSV	VE-DSG	19		b	Die Bestimmung ist schlicht absurd und würde für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. KMU im Finanzbereich verfügen nicht über ausgebaute Datensysteme, welche jeden Datenbearbeitung in einem Log aufzeichnen, und so jede Veränderung von bearbeiteten Personendaten zu dokumentieren. Die Anschaffung entsprechender Datensysteme würde die allermeisten KMU im Finanzsektor finanziell überfordern. Die Bestimmung verlangt von den KMU im Finanzbereich zudem ihre Verschwiegenheit mit Bezug auf Verdachtsmeldungen nach Art. 9 ff. GwG zu verletzen. Die Vorschrift, betroffene Personen über Verletzungen des Datenschutzes zu orientieren, verstösst gegen das nemo tenetur-Prinzip, dies umso mehr als unbefugte Datenbearbeitungen neu im StGB erfasst werden sollen, und der VE-DSG zahlreiche weitere Strafbestimmungen vorsieht.
VSV	VE-DSG	20	1		Die Bestimmung widerspricht der Auskunftsverweigerungspflicht im Rahmen der Art. 9 ff. GwG. Die Bestimmung muss wie folgt geändert werden: „Vorbehältlich abweichender gesetzlicher oder regulatorischer Bestimmung kann jede Person ~~kann~~ vom Verantwortlichen kostenlos Auskunft… [Rest unverändert.]“
VSV	VE-DSG	21	2		Die Bestimmung widerspricht der Auskunftsverweigerungspflicht im Rahmen der Art. 9 ff. GwG. Die Bestimmung muss wie folgt geändert werden: „Vorbehältlich abweichender gesetzlicher oder regulatorischer Bestimmung muss der ~~Der~~ Verantwortliche ~~muss~~ angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt…[Rest unverändert.]“
VSV	VE-DSG	23	2	b	Die Finanzmarktregulierungen sehen die Pflicht zur Bearbeitung von Personendaten vor.. Vorab ist

					wiederum das GwG, und namentlich dessen Art. 3 ff., zu nennen. Diese Bearbeitungspflichten können und dürfen nicht durch die betroffene Person ausgehebelt werden. Die gesetzliche Pflicht besteht unabhängig von der betroffenen Person, deren Einwilligung, oft gar nicht eingeholt werden kann oder (im Falle gesetzlicher Berufsgeheimnisse) darf. Zwar ist es denkbar, die Einwilligung zur Bearbeitung ihrer Personendaten durch die direkte Vertragspartei des Finanzintermediärs einzuholen. Aber zu weiteren Personen (namentlich Kontrollinhabern und wirtschaftlich Berechtigung) besteht oft kein Kontakt der die Einholung einer genügenden Einwilligung möglich oder machbar erscheinen liesse. Das Vorliegen eines Rechtfertigungsgrundes nach Art. 24 VE verschafft den betroffenen Finanzintermediären keinen genügenden Schutz. Insbesondere in zivilrechtlichen Auseinandersetzungen könnten sie sich nur enthaften, wenn ihnen der Beweis des Rechtfertigungsgrundes gelingt. Sie würden also mit der Beweislast für die Rechtmässigkeit ihrer Meldungen belastet. Wird bei den gesetzlich vorgesehenen Meldungen dagegen von vornherein die Rechtmässigkeit im Datenschutzrecht festgelegt, erfolgt keine solche Beweisbelastung. Damit muss Abs. 2 Bst. b wie folgt angepasst werden: „b. wenn, vorbehältlich entgegen stehender gesetzlicher oder regulatorischer Pflicht zur Bearbeitung, Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden;“
VSV	VE-DSG	23	2	c	Die Finanzmarktregulierungen sehen zahlreichen Mitteilungen an Aufsichtsbehörden vor, die auch gegen den Willen betroffener Personen Personendaten umfassen. Vorab ist wiederum das GwG, und namentlich dessen Art. 9 ff., zu nennen. Zudem sieht das StGB in Art. 305ter Abs. 2 ein Melderecht vor, dass durch das DSG nicht ausgehebelt werden soll. Die entsprechenden Meldungen umfassen auch besonders schützenswerte Personendaten. Solche Mitteilungen dürfen von vornherein keine Persönlichkeitsverletzung darstellen. Das Vorliegen eines Rechtfertigungsgrundes nach Art. 24 VE verschafft den betroffenen Finanzintermediären keinen genügenden Schutz. Insbesondere in zivilrechtlichen Auseinandersetzungen könnten sie sich nur enthaften, wenn ihnen der Beweis des Rechtfertigungsgrundes gelingt. Sie würden also mit der Beweislast für die Rechtmässigkeit ihrer Meldungen belastet. Wird bei den gesetzlich vorgesehenen Meldungen dagegen von vornherein die Rechtmässigkeit im Datenschutzrecht festgelegt, erfolgt keine solche Beweisbelastung. Damit muss Abs. 2 Bst. c wie folgt angepasst werden: „c. wenn ohne entgegen stehende gesetzliche oder

					regulatorischer Pflicht Dritten besonders schützenswerte Personendaten bekannt gegeben werden;“
VSV	VE-DSG	23	2	d	Das Profiling ist den Finanzintermediären u.a. durch das GwG vorgeschrieben. Sie haben entsprechende Datenbearbeitungen ohne ausdrückliche Einwilligung der betroffenen Person durchzuführen und das Profiling auch periodisch zu wiederholen. Die Verweigerung der Einwilligung kann diese Pflichten nicht verändern oder aufheben. Die Pflicht zu Profiling kann auch nicht durch die Beendigung der Geschäftsbeziehung umgangen werden. Dies namentlich bei Vorliegen der Meldepflicht nach Art. 9 ff GwG. Das Vorliegen eines Rechtfertigungsgrundes nach Art. 24 VE verschafft den betroffenen Finanzintermediären keinen genügenden Schutz. Insbesondere in zivilrechtlichen Auseinandersetzungen könnten sie sich nur enthaften, wenn ihnen der Beweis des Rechtfertigungsgrundes gelingt. Sie würden also mit der Beweislast für die Rechtmässigkeit ihrer Meldungen belastet. Wird bei den gesetzlich vorgesehenen Meldungen dagegen von vornherein die Rechtmässigkeit im Datenschutzrecht festgelegt, erfolgt keine solche Beweisbelastung. Damit muss Abs. 2 Bst. d wie folgt angepasst werden: „d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person oder ohne entsprechende stehende gesetzliche oder regulatorischer Pflicht.“
VSV	VE-DSG	23	3		Da eine unbefugte Datenbearbeitung nach Art. 179^{novies} VE-StGB mit Strafe bedroht werden soll, ist der Passus „~~In Regel~~“ in Abs. 3 durch „Es“ zu ersetzen. Ohne entsprechende Korrektur wird sonst das strafrechtliche Bestimmtheitsgebot („nulla poena sine lege stricta“) verletzt. Ohnehin ist der unklare Vorbehalt des Regelfalls, ohne Definition dessen, was nicht Regelfall ist, ungeeignet, die erforderliche Rechtssicherheit bei der Datenbearbeitung zu schaffen – und damit ein rechtspolitisches Unding.
VSV	VE-DSG	24	2		Da eine unbefugte Datenbearbeitung nach Art. 179^{novies} VE-StGB mit Strafe bedroht werden soll, ist das Wort „~~möglicherweise~~“ in Abs. 2 zu streichen. Ohne entsprechende Korrektur wird sonst das strafrechtliche Bestimmtheitsgebot („nulla poena sine lege stricta“) verletzt. Ohnehin ist der Hinweis auf die mögliche (gesetzliche) Rechtfertigung nicht geeignet, die erforderliche Rechtssicherheit bei der Datenbearbeitung zu schaffen – und damit ein rechtspolitisches Unding.
VSV	VE-DSG	25	3		Die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor. Es soll unnötiger Swiss Finish geschaffen werden. Die Urteilsmitteilung ist zu streichen.

VSV	VE-DSG	50	1		Der vorgeschlagene Bussenrahmen von bis CHF 500‘000 für nicht schwerwiegende Verstösse gegen formale Vorschriften des DSG kann nur noch „als ausser Rand und Band“ bezeichnet werden. Der Bussenrahmen ist auf max. CHF 5‘000 für Ersttäter und maximal CHF 20‘000 für Wiederholungstäter festzulegen.
VSV	VE-DSG	50	2		Der vorgeschlagene Bussenrahmen von bis CHF 500‘000 für nicht schwerwiegende Verstösse gegen formale Vorschriften des DSG kann nur noch „als ausser Rand und Band“ bezeichnet werden. Der Bussenrahmen geht auch weit über das hinaus, was z.B. DSGVO für Unternehmen vorsieht: nämlich 2% des weltweiten Umsatzes des Unternehmens. Bei einem kleinen Finanz-KMU, das einen Jahresumsatz von CHF 500‘000 erzielt, wären das gerade Mal CHF 10‘000. Der Bussenrahmen ist auf max. CHF 5‘000 für Ersttäter und maximal CHF 20‘000 für Wiederholungstäter festzulegen.
VSV	VE-DSG	50	2	e	Verletzt das *nemo tenetur*-Prinzip und ist damit ersatzlos zu streichen.
VSV	VE-DSG	50	2	f	Eine automatische Strafwürdigkeit bei Nicht-Gehorsam gegen Verfügungen des Beauftragten ist eines transparenten Rechtsstaates schlicht unwürdig. Es soll dem Beauftragten überlassen werden, ob und inwieweit er Verfügungen mit einer sinnvollen Strafdrohung nach Art. 292 StGB verknüpfen will.
VSV	VE-DSG	50	3		Einmal schlägt die Verwaltung einen völlig ausufernden Strafkatalog bei fahrlässiger Begehung vor. Das würde zu einem weiteren unverhältnismässigen Ausufern des Verwaltungsstrafrechts führen. Es ist unnötig und rechtsstaatlich nicht erwünscht, das jedes auch nur denkbar, verwaltungsrechtlich unerwünschte Verhalten auch gleich noch strafbewehrt wird. Die Bestimmung ist ersatzlos zu streichen.
VSV	VE-DSG	51	1		Der vorgeschlagene Bussenrahmen von bis CHF 500‘000 für nicht schwerwiegende Verstösse gegen Sorgfaltspflichten nach dem des DSG kann nur noch „als ausser Rand und Band“ bezeichnet werden. Der Bussenrahmen geht auch weit über das hinaus, was z.B. DSGVO für Unternehmen vorsieht: nämlich 2% des weltweiten Umsatzes des Unternehmens. Bei einem kleinen Finanz-KMU, das einen Jahresumsatz von CHF 500‘000 erzielt, wären das gerade Mal CHF 10‘000.

					Der Bussenrahmen ist auf max. CHF 5‘000 für Ersttäter und maximal CHF 20‘000 für Wiederholungstäter festzulegen.
VSV	VE-DSG	51	1	c	Die Bestimmung stellt Fehlleistungen bei der Ermessensbetätigung unter schwere Strafe. Das ist rechtsstaatlich nicht zu rechtfertigen. Die Bestimmung ist ersatzlos zu streichen.
VSV	VE-DSG	51	1	d	Die Bestimmung stellt Fehlleistungen bei der Ermessensbetätigung unter schwere Strafe. Das ist rechtsstaatlich nicht zu rechtfertigen. Die Bestimmung ist ersatzlos zu streichen.
VSV	VE-DSG	51	1	e	Die Bestimmung stellt Fehlleistungen bei der Ermessensbetätigung unter schwere Strafe. Das ist rechtsstaatlich nicht zu rechtfertigen. Die Bestimmung ist ersatzlos zu streichen.
VSV	VE-DSG	51	1	f	Die Bestimmung stellt Fehlleistungen bei der Ermessensbetätigung unter schwere Strafe. Das ist rechtsstaatlich nicht zu rechtfertigen. Die Bestimmung ist ersatzlos zu streichen.
VSV	VE-DSG	51	2		Einmal schlägt die Verwaltung einen völlig ausufernden Strafkatalog bei fahrlässiger Begehung vor. Das würde zu einem weiteren unverhältnismässigen Ausufern des Verwaltungsstrafrechts führen. Es ist unnötig und rechtsstaatlich nicht erwünscht, das jedes auch nur denkbar, verwaltungsrechtlich unerwünschte Verhalten auch gleich noch strafbewehrt wird. Die Bestimmung ist ersatzlos zu streichen.
VSV	VE-DSG	52			Der VSV begrüsst die Einführung eines strafbewehrten allgemeinen Berufsgeheimnisses, das auch für uVV gilt.
VSV	VE-DSG	54			Materiell gehören die Strafbestimmungen des DSG in den Bereich des Verwaltungsstrafrechts, da es überwiegend um Verstösse gegen Verfahrensvorschriften und Vorschriften zum Verhalten gegenüber

					Bundesbehörden geht. Die Verfolgung und Beurteilung strafbarere Handlungen gehört damit dem Verwaltungsstrafrecht unterstellt.
VSV	VE-DSG	55			Die Verjährungsfrist soll die allgemeine des Art. 109 StGB sein. Das ist ausreichend. Eine längere Verjährungsfrist ist in der schnelllebigen Welt der Datenbearbeitung sinn- und zwecklos sowie rechtsstaatlich höchst fragwürdig. Sie ist nicht zu rechtfertigen. Die Bestimmung ist ersatzlos zu streichen.
VSV	VE-DSG	56		a	Solche Staatsverträge greifen unmittelbar in die Rechte betroffener Personen und Datenbearbeitern ein. Von Verfassung (Art. 166 BV) wegen unterliegen solche Staatsverträge der Ratifikation durch referendumspflichtigen Bundesbeschluss.
VSV	VE-DSG	59			Das Übergangsrecht ist unvollständig. Wir verweisen auf die einleitenden Einführungen zu diesem Thema. Insbesondere ist die Behandlung "altrechtlicher" Datenbestände (namentlich auch bei der Bearbeitung von besonders schützenswerten Personendaten und dem regelmässig durchzuführenden Profiling) unklar. Sind die neuen Bestimmungen unmittelbar mit Inkrafttreten des revidierten Gesetzes anzuwenden, so wären Finanzintermediäre u.U. daran gehindert, ihre Pflichten nach dem GwG ordnungsgemäss zu erfüllen, ohne gegen Bestimmungen des dem formellen Gesetz nachgeordneten Verordnungs- und Rundschreibenrecht der FINMA bzw. gegen einzuhaltende Selbstregulierung zu verstossen. Sollen die Vorgaben des DSG (namentlich Einwilligungen von Kunden) auch uneingeschränkt für Finanzintermediäre gelten, dann bräuchte es hier ausdrückliche längere Übergangsfristen. Diese müssten sich im Bereich von mindestens fünf Jahren bewegen.
VSV	VE-ZPO	99	3	d	Art. 25 VE-DSG verweist in allgemeiner Form auf die Art. 28g – 28l ZGB. Damit bleibt unklar, ob diese Klagen auch als Klagen nach dem DSG gelten, wenn es um Fragen des Datenschutzes geht. Der Katalog von Art. 25 Abs. 1 Bst. a-c ist offensichtlich nicht abschliessend. Das Datenschutzrecht dient dem Persönlichkeitsschutz, vermögensrechtliche Aspekte des Persönlichkeitsschutzes, insbesondere Schadenersatzforderungen, sind demnach konsequent von der verfahrensrechtlichen Privilegierung Ausnehmen von Schadenersatzklagen.

					Die Bestimmung ist deshalb wie folgt zu ergänzen: „Ausgenommen bleiben Verfahren in den Schadenersatz oder Genugtuung verlangt werden.“
VSV	VE-ZPO	113	2	g	Art. 25 VE-DSG verweist in allgemeiner Form auf die Art. 28g – 28l ZGB. Damit bleibt unklar, ob diese Klagen auch als Klagen nach dem DSG gelten, wenn es um Fragen des Datenschutzes geht. Der Katalog von Art. 25 Abs. 1 Bst. a-c ist offensichtlich nicht abschliessend. Das Datenschutzrecht dient dem Persönlichkeitsschutz, vermögensrechtliche Aspekte des Persönlichkeitsschutzes, insbesondere Schadenersatzforderungen, sind demnach konsequent von der verfahrensrechtlichen Privilegierung Ausnehmen von Schadenersatzklagen. Die Bestimmung ist deshalb wie folgt zu ergänzen: „Ausgenommen bleiben Verfahren in den Schadenersatz oder Genugtuung verlangt werden.“
VSV	VE-ZPO	114		f	Art. 25 VE-DSG verweist in allgemeiner Form auf die Art. 28g – 28l ZGB. Damit bleibt unklar, ob diese Klagen auch als Klagen nach dem DSG gelten, wenn es um Fragen des Datenschutzes geht. Der Katalog von Art. 25 Abs. 1 Bst. a-c ist offensichtlich nicht abschliessend. Das Datenschutzrecht dient dem Persönlichkeitsschutz, vermögensrechtliche Aspekte des Persönlichkeitsschutzes, insbesondere Schadenersatzforderungen, sind demnach konsequent von der verfahrensrechtlichen Privilegierung Ausnehmen von Schadenersatzklagen. Die Bestimmung ist deshalb wie folgt zu ergänzen: „Ausgenommen bleiben Verfahren in den Schadenersatz oder Genugtuung verlangt werden.“

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
VSV	Keine Bemerkungen aus Sicht der uVV.

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
VSV	Keine Bemerkungen aus Sicht der uVV.

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
VSV	9	Die Regulierungsfolgenabschätzung, welche mit der Vernehmlassungsvorlage vorgelegt wird, und die entsprechenden Ausführungen über die Auswirkungen der neuen Regulierungen sind kaum mehr als ein schlechter Witz. Erwarteter zusätzlicher Aufwand wird nicht näher erhoben, zusätzliche Kosten werden weder konkret evaluiert noch geschätzt. Die in ihren finanziellen Auswirkungen nicht im Ansatz dargestellten Aufwände und Kosten werden schliesslich nur in höchster Abstraktheit dargestellten Vorteilen gegenübergestellt. Eine wirtschaftliche Analyse dieser angeblichen Vorteile fehlt dementsprechend auch. Die abschliessend Würdigung „Die Kosten für die Umsetzung der neuen Pflichten des Verantwortlichen dürften durch diese Vorteile aufgewogen werden.“ basiert auf keinerlei auch nur im Ansatz nachvollziehbarer Grundlage. Der VSV verlangt, dass für das tiefgreifende Projekte einer Totalrevision des DSG eine umfassende und konkrete Regulierungsfolgenabschätzung vorgenommen wird, welche sich insbesondere auch mit den wirtschaftlichen, insbesondere auch den finanziellen Folgen für die Wirtschaft und insbesondere für die zahlreichen Klein- und Kleinstunternehmen in der Schweiz auseinandersetzt.
VSV	9	Es ist offensichtlich, dass im Rahmen der Ausarbeitung der Vernehmlassungsvorlage kein Gedanke an die zahlreichen Unternehmen „verschwendet“ wurde, die aufgrund regulatorischer Vorschriften – insbesondere im Finanzsektor – in grossem Umfang Personendaten, darunter auch besonders schützenswerte Personendaten bearbeiten müssen, und Profiling durchführen müssen. Der VSV verlangt, dass bei der weiteren Bearbeitung der Vorlage, die Auswirkungen der einzelnen Bestimmungen auf diese Unternehmen gezielt untersucht, und die Vorlage zu einem revidierten DSG nicht mehr als „schöngeistiges“ Standalone-Projekt behandelt wird, sondern in die Rechtsordnung eingepasst wird, wobei auf die zahlreichen wirtschaftspolizeilichen Regulierungen des Bundesrechts die notwendige Rücksicht genommen wird.

		Der vorgelegte VE und seine Erläuterungen zeigen klar, dass hier bisher nur im Elfenbeinturm gewerkelt wurde.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
VSV	13	Im Erläuterungsbericht wird festgehalten, es genüge eine "allgemeine Information" im beschriebenen Sinn (vgl. S. 55). Der Wortlaut von Art. 13 VE widerspricht dem allerdings total.
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Amstutz Jonas BJ

Von: Patrick Kessler <info@vsv.ch>
Gesendet: Donnerstag, 30. März 2017 14:20
An: Amstutz Jonas BJ
Betreff: Vernehmlassungsantwort Datenschutz
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de (1).doc; 2017_03_30_Vernehmlassungsantwort.pdf

Sehr geehrter Herr Amstutz

Wir senden Ihnen im Anhang unsere Vernehmlassungsantwort zum Gesetzesentwurf Totalrevision Datenschutzgesetz.

Wir gehen davon aus, dass wir die Unterlage nicht postalisch einreichen müssen. Ansonsten bitten wir um eine kurze Rückmeldung.

Freundliche Grüsse

Patrick Kessler
Präsident

VSV ASVAD
Verband des Schweizerischen Versandhandels
l'Association Suisse de Vente à Distance

Verband des Schweizerischen Versandhandels
3000 Bern

Der **Geschäftssitz** befindet sich am
Bahnhofplatz 1
3011 Bern

Tel +41 31 312 40 35
Mob +41 79 290 40 24
skype: kessler.patrick

www.versandhandel.ch
info@vsv-versandhandel.ch

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Verband des Schweizerischen Versandhandels / l'Association de Vente à Distance

Abkürzung der Firma / Organisation : VSV ASVAD – www.vsv.ch

Adresse : Bahnhofplatz 1, 3011 Bern

Kontaktperson : Patrick Kessler

Telefon : 058 310 07 17

E-Mail : info@vsv.ch

Datum : 30. März 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 . Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
VSV ASVAD	Der VSV ASVAD hat angesichts des rasanten technologischen Wandels Verständnis für die Vorlage einer Totalrevision des Datenschutzgesetzes. Äquivalenz mit der EU wird als Teilziel akzeptiert, darf aber nicht als ausschliessliche Maxime des Entwurfes dienen. Den nun vorliegenden des neuen DSG lehnen wir ab bzw. **weisen diesen zur grundlegenden Überarbeitung zurück**. Der vorliegende Entwurf nimmt weder auf die Digitalisierungsstrategie des Bundes Rücksicht, noch verfolgt die Regulierung die globalen Entwicklungen in Sachen Datenschutz. Der Vorentwurf enthält Komponenten eines neuen «SWISS FINISH», was zu Standortnachteilen für in der Schweiz ansässige Unternehmen führt. Gleichzeitig wurde die Gelegenheit den alten, bestehenden «SWISS FINISH» aus dem bestehenden (und bereits recht fortschrittlichen) Datenschutzgesetz zu eliminieren. Der Entwurf **benachteiligt eindeutig KMU und bevorteilt Grossunternehmen**, die Vorgaben formalisieren die Datenbearbeitung in einer nicht akzeptablen Art und Weise. Der Gesetzesentwurf geht in keiner Weise auf die Unterscheidung zwischen «**Profiling**» und «**Gruppenbildung**» ein. Das vorliegende DSG verliert keinen einzigen Gedanken an die echte Fragestellung rund um Big Data – WIE IST MIT GRUPPEN VON MEHREREN PROFILEN UMZUGEHEN? Das Ziel von Big Data Bearbeitung ist nicht das individuelle Profil zu erstellen, sondern aus vielen Daten (auch Personendaten), Gruppen abzubilden, welche sich ähnlich verhalten. Diese «Gruppenbildung» kann bei einer Dimension von 2 Personen = Gruppe durchaus Rückschlüsse auf Individuen zulassen, hingegen ist eine Gruppe, welche aus 4 – 5 Personen besteht schon sehr stark anonymisiert bzw. man kann keine direkten Rückschlüsse auf eine Einzelperson ziehen, entsprechend ist ein erhöhter Datenschutzaufwand nicht notwendig. In Konsequenz geht der Vorschlag nicht auf die Möglichkeiten der Anonymisierung und **Pseudonymisierung** von Daten ein – ein erheblicher Mangel im Vergleich mit anderen Gesetzeswerken. Das vorliegende Gesetz nimmt zudem einzig und alleine Rücksicht auf europäische Rechtsnormen, welche in keiner Weise das Rechtsverständnis der Schweiz wiederspiegeln. Es **lässt globale Entwicklungen völlig ausser Acht**, es wird im Bericht sogar darauf verzichtet auf führende Datennationen wie USA und China einzugehen. Mit dem «Mut zur Lücke» hat man auf Vergleiche mit USA und China offenbar bewusst und berechnend verzichtet. Gerade dieser fehlende Vergleich deutet darauf hin, dass man sich nur auf die EU ausrichtet – ein aus unserer Sicht völlig verkehrter und vergangenheitsorientierter Ansatz. Dem Schweizer Unternehmen werden mit diesem Entwurf Auflagen erteilt, internationale insbesondere asiatische aber auch amerikanische Unternehmen werden sich keinen Deut um dieses Gesetz kümmern (können) – der Bericht gesteht die **problematische internationale Rechtsdurchsetzung** auch ein.

	Die **Regulierungsfolgeabschätzung** der PWC wurde zu einem Zeitpunkt vorgenommen als der Gesetzesentwurf noch nicht vorgelegen hat. Entsprechend **wertlos** ist die unterlegte Studie von PWC. Die darin gemachten Aussagen korrelieren in keiner Weise mit den Analyseresultaten des VE-DSG seitens verschiedenster Verbände. Das Gesetz ist KMU-feindlich und **bevorteilt Gross- und Grossunternehmen**, welche international tätig sind (sog. **Log-In Giganten** wie Google, Facebook, Amazon etc.). Nur in der Schweiz tätigen Unternehmen werden damit Hürden auferlegt, welche mit normalem Ressourceneinsatz nicht mehr zu bewältigen sind und einen Wettbewerbsnachteil gegenüber international agierenden Unternehmen schaffen. In verschiedenen Paragraphen stellen wir einen **«SWISS FINISH»** fest, obwohl dieser gemäss Bericht Punkt 1.7.4 gerade nicht angestrebt werden sollte. Der Entwurf beinhaltet **unverständliche Strafnormen für Privatpersonen bzw. Angestellte von Firmen**. Die Firmen werden damit aus der Haftung entlassen und Risiken auf Angestellte umgewälzt. Wir können nachvollziehen, dass schwere Straftaten im Bereich des Datenmissbrauchs auf Ebene des Individuums hart bestraft werden sollen. Formfehler und kleinste Versehen jedoch als Straftatbestand zu betrachten und mit hohen Bussen zu belegen kann kaum Kern der Datenschutzrevision sein. Hier wurde ganz einfach nicht im Verständnis unseres Rechtssystems gearbeitet. Wir unterstützen hier den konzeptionellen Gegenvorschlag der economiesuisse. Hingegen wird auf Bundesebene jegliche Strafnorm vermisst. Auch ein Bundesangestellter (natürlich auch Kantons – und Gemeindeangestellter) kann Missbrauch im Bereich Datenschutz betreiben, entsprechend müsste mit gleichen Ellen gemessen werden, hier wird offenbar bewusst differenziert. Der vorliegende Entwurf lässt völlig ausser Acht, dass damit in Zukunft JEDES in der Schweiz tätige Unternehmen (welches mit natürlichen Personen zu tun hat) de facto dazu gezwungen wird, signifikante Investitionen in Software und Prozesse zu tätigen, operative Zusatzkosten aufgebürdet bekommt ohne auch nur den geringsten Nutzen zu erzielen, weder für das Unternehmen selber noch für den Konsumenten. Das Gesetz ist technokratisch und **mit Vergangenheitsbezug** aufgesetzt worden. Die zukünftigen technologischen (und somit internationalen) Entwicklungen finden keinen Niederschlag (dezentrale Datenhaltung – Stichwort: Blockchain oder Erleichterungen, wenn gespeicherte Daten vom Kunden jederzeit eingesehen werden können). Der Gesetzesentwurf selber und insbesondere der Erläuterungsbericht zum Entwurf zeigen auf, dass ein «normaler Mensch» das Gesetz kaum mehr versteht und selbst Spezialisten damit zu kämpfen haben. Am Schluss bleiben mehr Fragen offen als beantwortet werden. Der vorliegende Entwurf ist **fundamental zu überarbeiten**, zumal den Gesetzgebern offenbar wichtig scheint, bei strafbaren Handlungen auf das bearbeitende Individuum und nicht das beauftragende Unternehmen durchzugreifen. Risiken im Bereich des Datenschutzes sollen damit in Zukunft von den natürlichen Personen verantwortet werden und nicht mehr von den Unternehmen – umso dringender wäre ein klares, einfach verständliches Gesetz. Der vorliegende Entwurf hat in dieser Form das Potential den Datenstandort Schweiz gegenüber dem Europäischen Umland signifikant zu

	benachteiligen und gegenüber den echten Wettbewerbern im globalen Umfeld chancenlos zu machen. Angesichts des grossen Korrektur- und Änderungsbedarfs gehen wir soweit und fordern nach Erstellung des Vernehmlassungsberichtes eine zweite Vernehmlassungsrunde bzw. eine Anhörung der betroffenen Kreise (wozu wir den Online-Handel definitiv zählen). Wir befürchten ansonsten eine Änderungs-Antragsschlacht in Kommission und Parlament – die Revision des DSG ist zu wichtig, als dass wir uns als Wirtschaftsstandort einen «Schiffbruch» erlauben können. Hinweis: Zwecks Visualisierung haben wir sämtliche Gesetzesparagraphen mit einem SWISS FINISH «rot» markiert.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
VSV ASVAD	DSG	1			Für uns erschliesst sich nicht in aller Konsequenz, dass juristischen Personen völlig ausgeschlossen werden. Haben nicht auch juristische Personen bzw. deren Repräsentanten Rechtssicherheit und ein minimales Mass an Datenschutz verdient? **Begründung:** Datenschutz bekommt auch für Firmen immer grössere Relevanz. Gerade unter standortstrategischen Gesichtspunkten (Datentresor Schweizer Alpen) ist der generelle Ausschluss von juristischen Personen nochmals zu hinterfragen. Ebenso sollte ein Unternehmen über Einsichts- bzw. Änderungsrechte von gespeicherte Daten verfügen. Auch Unternehmen unterliegen automatisierten Entscheidungsprozessen und müssen das Recht auf Korrektur von Daten haben. Mit Weglassung der juristischen Personen im DSG wird den Unternehmen diesbezüglich jegliche Schutzwürdigkeit aberkannt!
VSV ASVAD **Fehler! Verweisquelle konnte nicht gefunden werden.**	DSG	2			**Geltungsbereich generell:** Es fehlt eine klare Bestimmung, welche besagt, dass das Datenschutzrecht für in der Schweiz wohnhafte / gemeldete Personen gilt! Es ist klarzustellen, dass bei einer Regelung jedes Unternehmen, egal wo es seinen Sitz hat, die Schweizer Datenschutzgesetze zu befolgen hat. **Ansonsten ist das Gesetz für den Konsumenten nutzlos!** *Mit den im Bericht (Seite 42 unten – Räumlicher Geltungsbereich) ausgeführten Erklärungen / Begründungen öffnet man dem Missbrauch durch Unternehmen mit Sitz im Ausland Tür und Tor!*
VSV ASVAD	DSG	3			**SWISS FINISH:** Die vorliegende Definition von Profiling geht weiter als die Definition in der Deutschen Datenschutz Grundverordnung. Konkret bedeutet dies, dass fast jeder Umgang mit Daten als Profiling beurteilt wird und somit der Einwilligungs- und Anzeigepflicht unterliegt. Somit erleidet der Standort Schweiz einen ganz klaren Wettbewerbsnachteil gegenüber dem Standort EU. Die Definition Profiling ist anzupassen, Artikel 3 als Ganzes zu revidieren **(siehe auch einleitende Bemerkungen – es fehlen**

					Pseudonymisierung und Abgrenzung Gruppenbildung)
VSV ASVAD	DSG	3		c. 4.	Der Begriff der biometrischen Daten ist zu präzisieren: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Bilder in Zeitungen wären damit ausgenommen (der vorgesehene Wortlaut würde dazu führen, dass solche Bilder unter den Begriff der „biometrischen Daten“ fallen.
VSV ASVAD	DSG	3		f	**Profiling: Schlechte, ungenaue Definition welche Fragen offenlässt:** **Interpretationsfrage zum Verständnis unserer Kritik:** Wenn Personenprofile verwendet werden um generische Gruppen zu bilden (z.B. männliche Käufer während der letzten 6 Monate mit einem Umsatz > 100 CHF) wäre diese Aktion nach vorliegendem Entwurf als Profiling zu werten. Es fehlt generell die Definition der **Pseudonymisierung / Anonymisierung** (ohne Rückschlussmöglichkeit auf ein Individuum) **Die vorgeschlagene Definition und die damit einhergehende Regelung (siehe dazu Anmerkungen zu Art. 23 unten) des „Profiling“ werden abgelehnt. Die Definition geht ohne Not weit über diejenige der EU-DSGVO (Art. 4 Ziff. 4) hinaus (SWISS FINISH).**
VSV ASVAD	DSG	3		h	**Verantwortlicher:** Mit dieser Definition wird jede Verantwortung auf eine Person abgestellt und die juristische Person aus der Verantwortung entlassen. Hier muss unbedingt auch der Dateninhaber als Verantwortlicher definiert werden können (wie im SEV 108 vorgesehen). Warum wird das Bundesorgan separat erwähnt und wie ist ein Bundesorgan definiert? Ist das auch eine Privatperson oder wird dort von einem Amt / Gemeinde / Kanton gesprochen?
VSV ASVAD	DSG	3			**Fehlende Definition:** Es fehlt eine Definition zu Anonymisierung bzw. Pseudonymisierung von Daten. Dieses Mittel wird global angewendet um Einzeldatensätze oder Gruppen von Datensätzen unkenntlich zu machen. Das DSG hat

					dies in keiner Weise berücksichtigt!
VSV ASVAD	DSG	4	3		«Personendaten dürfen nur zu **einem bestimmten** und für die Person **klar** erkennbaren Zweck beschafft werden…» Diese Formulierung ist gut gemeint aber nicht haltbar, das Gesetz widerspricht sich damit in verschiedener Hinsicht selber. Zum einen dürfen Personendaten für Werbung verwendet aber auch für eine Kreditprüfung weitergegeben werden. Verbesserungsvorschlag: *«Personendaten dürfen nur ~~zu einem bestimmten und~~ für die Person ~~klar~~ erkennbaren Zwecke beschafft werden»*
VSV ASVAD	DSG	4	5		**Antrag: 1. Satz Streichen** «… muss überprüfen, ob die Daten richtig sind….». oder bitte in der Verordnung ausführen mit welchen Mitteln diese Prüfung vorgenommen werden muss.
VSV ASVAD	DSG	4	5		«Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden.» Dieser Satz macht keinen Sinn: Unrichtige (=falsche?) oder unvollständige Daten können nicht erforderlich sein. Wir empfehlen den Passus anzupassen auf *«Falsche oder unvollständige Personendaten müssen korrigiert oder ergänzt werden, andernfalls sind die Daten zu vernichten.»*
VSV ASVAD	DSG	4	6		In Anlehnung an unsere Bemerkung zu DSG 3 «Profiling» ist dieser Artikel zu korrigieren (Profiling löschen) oder aber das Profiling anderes zu definieren. *«… Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen.»*

					Die vorgeschlagene Änderung hinsichtlich des überaus zentralen Begriffs der „Einwilligung" ist unter Einbezug des erläuternden Berichts unklar. Gemäss erläuterndem Bericht (S. 47) ermöglicht die Neuformulierung eine terminologische Annäherung an die DSGVO. Es wird allerdings nicht klargestellt, ob damit eine inhaltliche Annäherung bezweckt wird. Die Definition ist nicht nur, aber in besonders ausgeprägter Form gerade für die Werbebranche von fundamentaler Bedeutung, weshalb eine klare Regelung und damit Rechtssicherheit erforderlich ist**. Die Übernahme der gegenüber der E-SEV 108 unnötig strengen Vorgaben der EU-DSGVO in Bezug auf die „Freiwilligkeit der Einwilligung" (Art. 7 Abs. 4) hätte jedenfalls eine massive Verschärfung der Rechtslage gegenüber dem geltenden Recht sowie eine erhebliche Beschränkung der Vertragsfreiheit zur Folge, die unnötig und daher abzulehnen ist.** Der E-SEV 108 (Art. 5 Abs. 2) verlangt denn auch lediglich, dass die Einwilligung freiwillig sein muss („free consent"), ohne eine derart strenge Interpretation, wie sie die EU-DSGVO enthält, vorzuschreiben. **In der Botschaft muss deshalb eine entsprechende Klarstellung aufgenommen werden**. **Darüber hinaus sind die Ausführungen im erläuternden Bericht zur „ausdrücklichen Einwilligungen" unklar bzw. unvollständig.** Es geht daraus letztlich nicht hervor, welche Anforderungen konkret an eine solche Einwilligung gestellt werden, was gerade aufgrund des (noch) übermässig weit gefassten Begriffs des Profiling und dessen Bedeutung für die Werbebranche besonders problematisch ist**. Es ist daher in der Botschaft auch klar zu stellen, dass – wie nach geltendem Recht – eine Einwilligung dann ausdrücklich ist, wenn die Datenbearbeitung, in welche eingewilligt wird, also z.B. das Profiling, bspw. in der Datenschutzerklärung beim Namen genannt wird und es insofern nicht genügen würde, wenn bloss aus den Umständen auf ein Profiling geschlossen werden müsste.**
VSV ASVAD	DSG	5			Es kann technisch nicht sichergestellt werden, dass Daten im Netz nicht über ausländische Server / Hoster laufen. Dieser Fall ist von der «Bekanntgabe ins Ausland» auszunehmen. Nur explizite Datenlieferungen an ausländische Dienstleister, Mutter- oder Tochtergesellschaften sollen davon betroffen sein.

VSV ASVAD	DSG	6	1	b	Die Regelung zur Bekanntgabe ins Ausland geht teilweise weiter als diejenige der EU-DSGVO (SWISS FINISH). Insbesondere muss daher die Ausnahmeregelung für die Bekanntgabe im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags angepasst werden. Entsprechend der EU-Regelung (Art. 49 Abs. 1 lit. c) muss in der Schweiz eine Bekanntgabe auch dann erlaubt sein, wenn ein Vertrag lediglich im Interesse der betroffenen Person abgeschlossen worden ist.
VSV ASVAD	DSG	7	4		Der Artikel ist unverständlich und nicht in Übereinstimmung mit dem erläuternden Bericht. Gegenüber dem alten Artikel wurde «Dritte» durch neu «Er» ersetzt. Das Wort «Er» ist in diesem Kontext undefiniert!
VSV ASVAD	DSG	8			Wir begrüssen grundsätzlich den Gedanken der Selbstregulierung. Allerdings kann nicht der EDÖB alleine als (de facto) gesetzgebende Instanz definiert werden. Die Genehmigungsinstanz ist genau zu definieren und zu erweitern.
VSV ASVAD	DSG	8	1		Das Genehmigungsverfahren kann nicht dem Datenschützer alleine unterliegen, die Genehmigungsinstanz ist genau zu definieren und zu erweitern. Im Weiteren muss eine Beschwerdeinstanz benannt werden, falls die beschlossene Selbstregulierung nicht akzeptiert wird. Wir schlagen daher vor, dass Branchenverbände Vorschläge unterbreiten und dem EDÖB ein Bewilligungsrecht eingeräumt wird. Der Artikel 8 soll dahingehend geändert werden: *1 Der Beauftragte Branchenverbände erarbeiten zusammen mit dem Beauftragten Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren.* *2 Der Beauftragte kann die Empfehlungen der Branchenverbände genehmigen.* *3 Er veröffentlicht die von ihm genehmigten Empfehlungen der guten Praxis.*
VSV ASVAD	DSG	8	1		Falls obenstehender Vorschlag kein Gehör findet, beantragen wir mindestens folgende Anpassung: *«Er zieht dazu die ~~interessierten~~ Kreise bei…» ersetzen durch «Er zieht dazu die betroffenen Parteien in*

					ausgewogenem Verhältnis bei» Weiter müssten bei Beibehalten der Entwurfsformulierung die möglichen Rechtsmittel gegen solche «gesetzgebende» Entscheide klar definiert werden.
VSV ASVAD	DSG	9	2		Wir begrüssen diese Möglichkeit ausdrücklich. Es ist auf bestehende Selbstregulierungen durch die bestehenden Branchen aufzubauen.
VSV ASVAD	DSG	12			Die Einführung einer Regelung zu Daten verstorbener Personen ist im Hinblick auf die Angemessenheit des Schweizer Datenschutzrechts nicht zwingend erforderlich und führt für die Unternehmen zu einem erheblichen administrativen Mehraufwand (SWISS FINISH). Insbesondere für den Bereich der nicht besonders schützenswerten Daten ist auf die Regelung zu verzichten.
O	DSG	13			SWISS FINISH: Hier wird mit übertriebener Formalität gearbeitet. SEV 108 ist grosszügiger und muss im Interesse des Datenstandortes Schweiz angewendet werden.
VSV ASVAD	DSG	13			«… über die Beschaffung von Personendaten… « ersetzen durch *«… über die Beschaffung* ***von besonders schützenswerten*** *Personendaten gemäss Artikel 3 Bst c»* ➔ die alte Formulierung hat genau diese Differenzierung gemacht.
VSV ASVAD	DSG	13	2		Hinsichtlich des Zeitpunkts der Information ist für den Online-Kontext eine Klarstellung erforderlich. Denn beim Zugriff auf eine Website wird regelmässig eine Bearbeitung von IP-Adressen erfolgen (Erfassung in Log-Datei, Zählung der Website-Zugriffe etc.) und dies in der Regel bereits bevor der Nutzer allfällige Informationen hierzu z.B. in einer Datenschutzerklärung zur Kenntnis nehmen kann. Aufgrund der Tatsache, dass IP-Adressen je nach Einzelfall Personendaten darstellen können und dass eine vorgängige Information hier technisch grundsätzlich nicht möglich ist, muss klargestellt werden, dass die ausreichend kenntlich gemachte Information in einer Datenschutzerklärung nach Abruf der Website als rechtzeitig gilt.
VSV ASVAD	DSG	15	1		«… informiert ~~die betreffende Person~~, wenn eine Entscheidung erfolgt, … « ersetzen durch «… informiert ***in den AGB***, wenn eine Entscheidung erfolgt ….und diese erhebliche rechtliche Wirkungen ~~oder~~

					~~erhebliche Auswirkungen auf die betroffene Person~~ hat»
VSV ASVAD	DSG	15	2		«Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung ***mit erheblicher rechtlicher Wirkung*** ~~und zu den bearbeiteten Personendaten~~ *zu äussern*» Der Passus betr. den zu bearbeitenden Personendaten ist überflüssig, da gemäss Artikel 4 Abs 5 Daten aktuell und korrekt sein müssen. Basis für automatisierte Entscheidungen sind Daten, entsprechend kann die Datenkorrektur einziges Recht der Privatperson sein.
VSV ASVAD	DSG	16			Die Anknüpfung an das Vorliegen „**erhöhter Risiken**“ führt zu einem viel zu weit gefassten Anwendungsbereich und geht unverständlicherweise über die Vorgaben in der EU-DSGVO (Art. 35) hinaus (SWISS FINISH). Der Entwurf und die Erläuterungen bleiben denn auch unklar, was ein „erhöhtes Risiko“ sein soll. Jedes noch so kleine Risiko kann als „erhöht“ gegenüber keinem Risiko angesehen werden. **Diese Formulierung ist schon deshalb untauglich und zu streichen.** Bleibt es bei dieser Formulierung, würde diese zu einem übermässigen Aufwand führen, der sowohl für die Unternehmen als auch für den EDÖB nicht zu bewältigen ist. Denn, wie aus dem erläuternden Bericht hervorgeht, könnte eine solche Pflicht zur Datenschutz-Folgeabschätzung letztlich bei jeder Übermittlung in Länder wie die USA, jedem Profiling und jeder Bearbeitung von besonders schützenswerten Daten bestehen. Dies würde für die Werbebranche zu massiven Kosten führen, da die Pflicht bspw. auch für das Profiling zur Einblendung personalisierter Werbung oder beim Web-Tracking bestehen würde. Entsprechend der EU-Regelung sollte daher zumindest auf Datenbearbeitungen mit „hohem Risiko“ (oder besser „besonders hohem Risiko“) abgestellt werden. Dabei sollten auch diejenigen Fälle, in denen die Pflicht besteht, (zumindest beispielhaft) konkretisiert und Ausnahmen vorgesehen werden. Ausgenommen werden sollten namentlich Fälle, in welchen die Betroffenen mit den Datenbearbeitungen einverstanden sind. Mit der vorgeschlagenen Regelung wäre die Meldepflicht derart weit gefasst, dass der Aufwand weder durch die Unternehmen noch den EDÖB bewältigt werden kann. Schliesslich ist auch die Frist von drei Monaten zur Beurteilung durch den EDÖB länger als diejenige in der EU-DSGVO (Art. 36 Abs. 2). Das

					Abwarten dieser Frist nicht praktikabel und führt zu einer erheblichen Einschränkung der Handlungsfreiheit der Unternehmen und letztlich zu einer Lähmung der Wirtschaft. Die Frist muss daher entsprechend erheblich verkürzt werden. Wir unterstützen hierbei den Vorschlag der economiesuisse.
VSV ASVAD	DSG	16	1		«Führt die vorgesehene Datenbearbeitung voraussichtlich….» ergänzen um «Führt die vorgesehene Datenbearbeitung ***von besonders schützenswerten Personendaten*** voraussichtlich…»
VSV ASVAD	DSG	17			Nach der vorgeschlagenen Regelung besteht gegenüber dem EDÖB grundsätzlich für jede „unbefugte Datenbearbeitung“ eine Meldepflicht. Daher hat eine Meldung im Grundsatz bei jedem auch noch so geringfügigen Verstoss zu erfolgen. Dabei handelt es sich wiederum um ein schweizerisches Überschiessen (SWISS FINISH), welches zudem viel weitergeht, als zum Schutz der Betroffenen erforderlich ist. Die vorgesehene Einschränkung auf Fälle, die voraussichtlich nicht zu einem „Risiko für die Persönlichkeit“ des Betroffenen führen, vermag den Anwendungsbereich sodann auch nicht hinreichend zu begrenzen. Entsprechend der Vorgabe im E-SEV 108 (Art. 7 Abs. 2) ist die Meldepflicht daher auf Verletzungen zu beschränken, welche die Rechte der Betroffenen „schwerwiegend“ („seriously“) gefährden könnten. Bei der vorgeschlagenen Meldepflicht zeigt sich ferner auch deutlich, dass die vorgesehene Sanktionsregelung, welche auf die Bestrafung natürlicher Personen fokussiert, falsch ist. So werden Mitarbeiter vollkommen unangebracht in eine Drucksituation versetzt, sofern sie Kenntnis von einer Verletzung erlangen: Entweder denunzieren sie den zuständigen Mitarbeiter oder machen sich andernfalls unter Umständen gar selbst strafbar. Dies hätte nachhaltige Auswirkungen auf die interne Organisation und Governance rund um datenschutzrechtliche Risiken innerhalb eines Unternehmens. Dieses müsste letztlich immer damit rechnen, dass einzelne Mitarbeiter entsprechende Meldungen machen. Aufgrund der persönlichen strafrechtlichen Verantwortung der Mitarbeiter könnten auch keine Vorgaben an die Ausübung der entsprechenden Meldepflichten gemacht werden.
VSV ASVAD	DSG	19			Der vorliegende Text impliziert grosse formale Aufwände für alle Unternehmen, welche auch nicht besonders schützenswerte Personendaten bearbeiten! Die EU Verordnung sieht in Bezug auf die Dokumentationspflicht eine Ausnahme für KMU bis 250 Mitarbeiter vor. VE DSG umfasst alle Unternehmen und wird somit zu einer Belastung für KMU und somit

					ein Innovationskiller für den Standort CH. Die vorgeschlagene Dokumentationspflicht ist damit zu weit gefasst und führt für Unternehmen zu einem erheblichen und unnötigen Aufwand. **Die Regelung darf keinesfalls über das in der EU-DSGVO (Art. 30) vorgeschriebene Verzeichnis der Datenbearbeitungen hinausgehen.** Damit ein solches Verzeichnis überhaupt seinen Zweck erfüllen kann, muss es jedenfalls auf regelmässige Datenbearbeitungen beschränkt sein, andernfalls müsste bereits jegliche Korrespondenz darin erfasst werden. Darüber hinaus sind, wie auch im Rahmen der EU-DSGVO (Art. 30 Abs. 5), entsprechende Ausnahmen vorzusehen. In der aktuell vorgesehenen Form stellt auch diese Bestimmung ein schweizerisches Überschiessen **(SWISS FINISH).** Wir beantragen die Dokumentationspflicht für Unternehmen zu streichen, welche nur «nicht besonders schützenswerte Daten» bearbeiten.
VSV ASVAD	DSG	20	1		**SWISS FINISH:** «…. kostenlos ….» Diese Formulierung kann ein Unternehmen in den Ruin treiben. Kostenlos ist nur dann denkbar, wenn falsche Informationen gespeichert werden. Sogar der SEV 108 spricht von «nicht übermässigen Kosten» und auch die Deutsche Verordnung spricht von «angemessenem Entgelt». Es ist davon auszugehen, dass diese Rechte inskünftig zunehmend und in einem intensiveren Ausmass genutzt werden als bislang. Hier ist die Einschätzung der PWC im Rahmen der Regulierungsfolgeabschätzung in besonderem Ausmass unrealistisch. Es sollte zumindest eine Aufwandsentschädigung für Auskünfte angesetzt werden können.
VSV ASVAD	DSG	20	3		Im erläuternden Bericht wird genau formuliert, dass ein Algorithmus nicht offengelegt werden muss. Dies sollte entsprechend auch im Gesetz genau formuliert werden. Das Wort «Zustandekommen» impliziert aber, dass gerade der Entscheidungsprozess offengelegt werden muss. Wir stellen einen Widerspruch zwischen Gesetz und erläuterndem Bericht fest, denn automatisierte Einzelentscheidungen gehören unter Umständen zu den Geschäftsgeheimnissen. Abs. 3 ist deshalb zu korrigieren: «… Informationen über das Ergebnis, ~~das Zustandekommen~~ und die Auswirkungen der Entscheidung.»

VSV ASVAD	DSG	23			Das generelle Erfordernis der ausdrücklichen Einwilligung für das Profiling stellt eine der problematischsten Schweizer Verschärfungen dar und ist zwingend zu streichen (SWISS FINISH). Für die Werbewirtschaft hat diese Anforderung erhebliche Konsequenzen, welche unnötig sind. Denn nach dem E-SEV 108 ist eine entsprechende Vorgabe nicht verlangt. Ferner ist auch nach der EU-DSGVO nicht für jegliche Form des Profiling eine Einwilligung erforderlich. Aber auch in der Sache besteht keine Notwendigkeit, das Profiling per se als Persönlichkeitsverletzung einzustufen. Solange die Datenbearbeitungsgrundsätze eingehalten werden, ist nicht ersichtlich, wieso neben der Information stets zusätzlich auch eine Einwilligung erforderlich sein soll. Wird diese Vorschrift Gesetz verunmöglicht sie faktisch einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung / Marketing und stellt eine Bedrohung für den Standort Schweiz dar. Profiling und damit personalisierte Werbung wäre dann nur noch den grossen (insbesondere internationalen) Log-in Giganten wie Facebook, Google, Apple und Co. vorbehalten. Diese Unternehmen können sich meist problemlos auf eine ausdrückliche Einwilligung im Rahmen der Account-Registrierungen stützen. Das Ergebnis wäre sodann auch aus kartellrechtlichen Überlegungen höchst problematisch.
VSV ASVAD	DSG	23	3		Definition: «allgemein zugänglich gemacht». Dieser Begriff war in der Vergangenheit (d.h. vor 20 Jahren) relativ klar abzugrenzen. In Zeiten der Digitalisierung fällt die Abgrenzung schwerer. Was heisst im aktuellen und zukünftigen Kontext «allgemein zugänglich gemacht»?
VSV ASVAD	DSG	24	2	C1	**Schützenswerte Daten:** Bei einem Kreditgesuch ist immer die Nationalität des Kreditnehmers zu erfassen. Eine Nationalität lässt Rückschlüsse auf eine ethnische Zugehörigkeit zu. Ist das Erheben der Nationalität im Zuge einer Kreditprüfung mit dieser Formulierung untersagt?
VSV ASVAD	DSG	24	2	C3	**Volljährigkeit:** Eine Volljährigkeit kann häufig erst mit einer Datenprüfung festgestellt werden (oder eben auch nicht). Hier ist die Formulierung so zu wählen, dass es bei einer Kreditprüfung Pflicht ist, die Volljährigkeit zu prüfen. Der im Bericht erwähnte Moneyhouse-Fall hat mit dieser Formulierung u.E. nichts zu tun. Dort geht es darum ob Kinder in Datenbanken geführt werden sollen oder nicht und ob das Geburtsdatum als Merkmal legitim ist.

					Online-Versandhändler führen in den meisten Fällen für den Kauf auf Rechnung eine Kreditprüfung durch. Dabei ist Volljährigkeit häufig ein entscheidendes Merkmal für das Zustandekommen eines Vertrages. Wir weisen weiter darauf hin, dass für bestimmte Vertragszwecke die Volljährigkeitsprüfung gar gesetzlich gefordert wird (Tabakwaren, Alkohol etc.). Insofern beantragen wir Absatz 3 zu streichen.
VSV ASVAD	DSG	29	4		An wen dürfen Bundesbehörden Name, Vorname, Adresse und Geburtsdatum bekannt geben? Hat ein Unternehmen somit ebenfalls das Recht diese nicht schützenswerten Informationen ohne Einhaltung von Formalitäten zu speichern bzw. zu bearbeiten?
VSV ASVAD	DSG	39	1		«… Revisionsstelle eines Handelsunternehmens tätig sein.» Diese Formulierung ist nicht nachvollziehbar sein. Der EDÖB darf also nicht Revisionsstelle des Online-Shops seines Patenkindes sein, hingegen dürfte er als Revisionsstelle eines Datenhändlers fungieren. Wir beantragen eine konsequente Formulierung und den zweiten Satz im ersten Absatz vollständig zu streichen. Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. ~~Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglieder der Geschäftsleitung etc.…~~»
VSV ASVAD	DSG	50 / 51			**Generell:** Hier wäre eine Strafbestimmung gefordert, welche ganz klar zwischen Unternehmen und Privatpersonen unterscheidet. Privatpersonen/Angestellte sollen nur dann belangt werden, wenn Vorsatz (oder im normalen Sprachgebrauch «Missbrauch») nachgewiesen werden kann. Strafen für formale Fehlhandlungen, fahrlässige nicht Einhaltung von Rechtsvorschriften etc. müssen in der Verantwortung der Unternehmen bleiben. Die Strafbestimmungen müssen grundsätzlich überarbeitet werden. Überhaupt ist die Strafnorm in keiner Weise stimmig und logisch. Es sieht an dieser Stelle (auch grammatikalisch) so aus, als ob in letzter Minute etwas ein-/umgebaut wurde.

					Wir unterstützen in Bezug auf die Strafnormen das von economiesuisse unterbreitete Konzept. In jedem Falle sind auch Unternehmen mit in die Verantwortung einzubeziehen.
VSV ASVAD	DSG	50			**SWISS FINISH** «…. werden private Personen bestraft…» Artikel 50 besagt, dass nur private Personen bestraft werden sollen, nicht jedoch juristische Personen. **Dies Formulierung hat das Potential den Werkplatz Schweiz nachhaltig zu schädigen und Datenbearbeitung an unseren Standorten zu unterbinden.** Am Schluss soll also der Arbeitnehmer das Risiko der Datenbearbeitung tragen und nicht das Unternehmen, welches mit den Daten arbeitet. Der ganze Artikel strotzt von Formalitätsstrafen, welche in dieser Art und Weise völlig übertrieben sind und ganz klar KMU feindlich sind. Für ein KMU sind sich solch horrende Strafen existenzgefährdend, für Grossunternehmen wie Google, Facebook, Microsoft und Co. hingegen banal.
VSV ASVAD	DSG	50			Die Schweiz läuft Gefahr mit diesen Strafbestimmungen gegen die SEV 108 zu verstossen. Es war kaum im Interesse der SEV 108 nur private Personen zu bestrafen.
VSV ASVAD	DSG	50	2		Grammatik: Dieser Absatz ist grammatikalisch sehr schlecht aufgebaut. Insbesondere die Aufzählungen in den Buchstaben a – e passen nicht zur Einleitung des Absatz 2.
VSV ASVAD	DSG	51			**SWISS FINISH** «…. werden private Personen bestraft…» Artikel 51 besagt, dass nur private Personen bestraft werden sollen, nicht jedoch juristische Personen. **Dies Formulierung hat das Potential den Werkplatz Schweiz nachhaltig zu schädigen und Datenbearbeitung an unseren Standorten zu unterbinden.** Am Schluss soll also der Arbeitnehmer das Risiko der Datenbearbeitung tragen und nicht das Unternehmen, welches mit den Daten arbeitet. Der ganze Artikel strotzt von Formalitätsstrafen, welche in dieser Art und Weise völlig übertrieben sind und ganz klar KMU feindlich sind. Für ein KMU sind sich solch horrende Strafen existenzgefährdend, für

					Grossunternehmen wie Google, Facebook, Microsoft und Co. hingegen banal.
VSV ASVAD	DSG	52			Gemäss Bericht und Gesetz soll neu für den Umgang mit Daten eine Schweigepflicht für Privatpersonen eingeführt werden. Dies ist einerseits nachvollziehbar, wenn es um besonders schützenswerte Daten geht. Hingegen ist der gewählte Begriff «geheime» Daten in diesem Kontext nicht definiert bzw. der Begriff wird im gesamten DSG an dieser Stelle erstmalig verwendet!
VSV ASVAD	DSG	53			Geschäftsbetriebe werden gemäss dem Entwurf weniger stark belangt als Privatpersonen. Dies bedarf dringend einer grundsätzlichen Überarbeitung der ganzen Strafbestimmungen.
VSV ASVAD	DSG	59			Neu 2. Absatz einfügen: «Daten welche vor Inkrafttreten dieses Gesetzes bearbeitet worden sind, gelten für die Dauer von 10 Jahren als «eingewilligte» Daten im Sinne der Artikel 4 Abs. 6, 13 und 15. Die betroffene Person kann die Bearbeitung dieser Daten jederzeit widerrufen.»

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	

Fehler! Verweisquelle konnte nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln")

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
VSV ASVAD	Zusammen-fassung	Seite 5: «Ein hoher international anerkannter Schutzstandard…» Der mit dem Gesetz verfolgte Schutzstandard ist einzig und alleine in der EU anerkannt, nicht aber im Rest der Welt!
VSV ASVAD	Zusammen-fassung	Seite 6: «… der Datenschutz für juristische Personen abgeschafft» Auch juristische Personen - insbesondere deren Mitarbeiter - verdienen einen Datenschutz.
VSV ASVAD	Zusammen-fassung	Seite 6: «… die auf einer rein automatisierten Datenbearbeitung beruhen» Mit Blick nach vorne werden in Zukunft 99.5 % aller Datenbearbeitungen automatisch erfolgen. In Konsequenz muss immer jede betroffene Person über die Entscheidungen informiert werden. Ist das wirklich im Sinne des Konsumenten?
VSV ASVAD	Zusammen-fassung	Seite 6: «Die Revision soll die Selbstregulierung bei den Verantwortlichen fördern» Diese Aussage widerspricht dem aufgelegten Gesetz in vielerlei Hinsicht. Die Freiheit der Selbstregulierung entzieht sich unserer Beurteilung des Gesetzesentwurfs.
VSV ASVAD	Zusammen-fassung	Seite 14: «Hingegen ist die Schweiz nicht verpflichtet, die Verordnung (EU) 2016/679 zu übernehmen» Die Schweiz hat keine Pflicht die EU-Regelung zu übernehmen, tut es aber trotzdem bereitwillig und überschiessend. Warum?
VSV ASVAD	Zusammen-fassung	Seite 18 – Kapitel 1.4.1 **Wir loben die Absicht einer Trennung von Unternehmen, deren Zweck in der Datenbearbeitung liegt (z.B. Google bzw. Log-In Giganten) von Unternehmen, welche Daten mit geringem Risiko bearbeiten (z.B. Handel). Im Gesetz zeigt sich diese Unterscheidung dann leider nicht mehr.**
VSV ASVAD	Zusammen-fassung	Seite 19: Profiling vs. Persönlichkeitsprofil vs. Gruppenprofile Gerade diese Unterscheidung scheint uns relevant, auch wenn sie der Gesetzgeber nicht sehen möchte. Unsere Definitionen sehen deshalb leicht differenzierter aus und wir schlagen vor, diese Differenzierung im Gesetz aufrecht zu berücksichtigen:

		• Profiling ist eine Tätigkeit mit dem Ziel unbekannte Personen zu «profilieren» und ein Gesicht zu geben (identifizieren). • Persönlichkeitsprofil ist statisch und beruht auf vorhandenen Gegebenheiten ohne die Anreicherung/Kombinatorik von/mit Fremddaten. • Gruppenprofile: Eine bestimmte Menge an Personen bekommt eine Gruppenprofilklassierung (zwecks Werbe-Ansprache, Priorisierung) Gemäss VE DSG ist nun eine Gruppenprofilklassierung (Scoring) eine Profilierungsaktivität! Das heisst jedes Scoring führt zu einer mitzuteilenden Personeninformation, das wäre absoluter Unsinn.
VSV ASVAD	Zusammen-fassung	Seite 19: Meldung von Datensammlungen Wir sind der Meinung, dass Datensammlungen mit besonders schützenswerten Daten weiterhin gemeldet werden müssten. Dies ist gerade für den Handel bei der Auswahl von Dienstleistern/Datenanbietern ein wichtiges Auswahl- und Differenzierungsmerkmal
VSV ASVAD	Zusammen-fassung	Seite 20: Strafrechtliche Sanktionen Die Ausgestaltung ist ausgesprochen KMU-feindlich und bevorteilt Grossunternehmen. Ein Grossunternehmen verkraftet eine Busse von bis zu 500'000 CHF unter Umständen sehr leicht, während es für ein KMU existenzbedrohend sein kann
VSV ASVAD	Zusammen-fassung	Seite 21: Beweislastumkehr Wir begrüssen ausdrücklich, dass auf eine Beweislastumkehr verzichtet wird, es entspricht nicht dem Schweizer Rechtsverständnis
VSV ASVAD	Zusammen-fassung	Seite 21: Kollektive Rechtsdurchsetzung Wir begrüssen ausdrücklich, dass auf eine kollektive Rechtsdurchsetzung verzichtet wird, es entspricht nicht dem Schweizer Rechtsverständnis.
VSV ASVAD	Zusammen-fassung	Seite 23 – Kapitel 1.7.2 Wir unterstützen die Feststellung, dass insbesondere das A-Segment mit den vorgeschlagenen Datenschutzvorschriften zu kämpfen haben wird (siehe Einleitung). Es ist jedoch ein Trugschluss, dass kleinere Unternehmen weniger mit Daten arbeiten als

		grosse Unternehmen.
VSV ASVAD	Zusammen-fassung	Es fehlen Rechtsvergleiche zu den grössten Datenverarbeitern der Gegenwart – den USA und China. Diese Weglassung ist nicht zu akzeptieren, stehen doch Schweizer Unternehmen gerade im Bereich Datenverarbeitung/-speicherung aber auch im Handel und Industrie in direkter Konkurrenz zu Anbietern aus diesen Staaten. Der «Mut zur Lücke» ist in dieser Situation unangebracht.
Fehler! Verweisquelle konnte nicht gefunden werden.		
Fehler! Verweisquelle konnte nicht gefunden werden.		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
VSV ASVAD	Gesetz Seite 42	Seite 42 Diese Erklärung ist mangelhaft und zeigt die absolute Schwäche des Gesetzes. Datenschutz ist keine räumlich abgrenzbare Aufgabe. Wenn ein Gesetz der Privatperson nutzen soll, dann ist diese Person in den Mittelpunkt zu stellen und alle haben sich daran zu halten. Ansonsten braucht es kein Gesetz! Ebenso ist sicherzustellen, dass die Gerichtsbarkeit möglich ist. Die auf Seite 42 angeführte Feststellung ist eine Kapitulationserklärung – ein solches Gesetz ist wertlos!
VSV ASVAD	Gesetz Seite 46	Zweckbindung und Erkennbarkeit Wir begrüssen ausdrücklich die Möglichkeit der zweckgebundenen Weiternutzung (Werbung) der Kundenadresse bei Onlinebestellungen
VSV ASVAD	Gesetz Seite 47	Einwilligung generell: Das vorliegende Gesetz bevorzugt ganz klar sogenannte Log-In Giganten wie Facebook, Google, Amazon, Microsoft etc. Log-In Giganten und Applikationsanbieter haben hier gegenüber Schweizer KMU Unternehmen in den vergangenen Jahren einen Wettbewerbsvorteil erarbeitet, welcher nun mit einem strengen «Einwilligungsgesetz» zementiert wird. Es ist deshalb vom Grundsatz her zu kritisieren, dass die Schweiz der «Log-In» Manie hinterherläuft. Ein viel praktikablerer und KMU freundlicherer Weg wäre eine konsequente Opt-Out Strategie zu verfolgen. Dies ist eine Grundsatzfrage und vor allem hinsichtlich der technologischen Entwicklungen abzuwägen: Dazu kann man einfach nur feststellen, dass das tägliche Leben mit dem vorliegenden Gesetz in den nächsten Jahren vor allem daraus bestehen wird, Opt-Ins abzugeben! Wir bezweifeln, dass dieser eingeschlagene Weg zielführend sein wird.
VSV ASVAD	Gesetz Seite 48	Einwilligung: Ist ein einfaches Opt-In ausreichend bzw. ausdrücklich?
VSV ASVAD	Seite 48	Bekanntgabe ins Ausland Wir gehen davon aus, dass eine «Datenlagerung» im Ausland ebenfalls unter diesen Artikel fällt. Ein Inhaber einer Datensammlung kann nicht in jedem Falle erkennen wo Daten genau gelagert / gehalten werden. Er benutzt dazu unter Umständen Cloud Services, bei welchen nicht in jedem Zeitpunkt offensichtlich ist, wo die Daten effektiv gehalten werden und ob die Daten überhaupt an einem

		Ort gehalten werden. Insbesondere bei dezentraler Datenhaltung und technologischer Aufteilung der Daten, ist das «1:1» Verhältnis nicht mehr gegeben und die Vorgaben des Gesetzes sind in solchen Fällen schlicht nicht mehr einzuhalten.
VSV ASVAD	Seite 52 8.1.2.4	Auftragsbearbeitung (letzter Absatz) Gemäss Bericht ist die betroffene Person über die übertragene Auftragsbearbeitung (Auftragsbearbeiter darf einem anderen Auftragsbearbeiter übertragen) zu informieren. Dies geht aus dem Gesetzestext Artikel 13 Absatz 4 nicht wie im Bericht erwähnt hervor.
VSV ASVAD	Seite 52 8.1.2.5	Empfehlungen der guten Praxis Im Grundsatz begrüssen wir das Vorgehen mit einer Selbstregulierung. Es fehlt im Bericht und Gesetz jedoch der Hinweis, dass die Selbstregulierung nur mit einem ausgewogenen Gremium funktionieren kann. Wenn wie gesetzlich vorgesehen «interessierte Kreise» etwas entwerfen besteht das Risiko der Ideologisierung der Selbstregulierung.
VSV ASVAD	Seite 53	Einhaltung Empfehlung der guten Praxis Wir begrüssen die Möglichkeit der Selbstregulierung durch Verbände ausdrücklich
VSV ASVAD	Seite 56 8.1.3.1	Informationspflicht bei der Beschaffung von Personendaten Es wird hier nicht ganz klar, wie weit die Bestimmung reichen soll. Wir gehen davon aus, dass eine reine Adressbeschaffung keine Informationspflicht bei Privatpersonen auslöst. Erst eine Ergänzung / Anreicherung von nicht schützenswerten Personendaten sollte der Informationspflicht unterstellt werden.
VSV ASVAD	Seite 57/58	Ausnahme von der Informationspflicht Die Ausnahmen sind enger zu umschreiben. Das Wort «unverhältnismässiger» Aufwand ist zu beziffern bzw. zu definieren.
VSV ASVAD	Seite 59	Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung Dieser Paragraph ist in dieser Konstellation und Definition wertlos. Fast alle Entscheide in Systemen werden heutzutage automatisiert nach bestimmten Prozessvorgaben und Kriterien gefällt. Solche Entscheide tragen in vielen Fällen sogar Geschäftsgeheimnisse in sich und können je nach Ausprägung auch mit dem Geschäftsmodell gleichgesetzt werden.
VSV ASVAD	Seite 60	Absatz 2 – Anhörung Dieser Absatz gehört nicht in ein Gesetz. Wir kennen Vertragsfreiheit in der Schweiz und diese wird gemäss Bericht auch mit

		diesem Absatz nicht angetastet. Insofern macht es keinen Sinn, hier ein gesetzliches Anhörungsrecht einzuräumen. Die einseitige Willens- bzw. Meinungsäusserung ist jederzeit auch ohne diese Regelung möglich. Wie sieht es bei der Anhörung betr. Bonitätsprüfung aus (Prüfung zwecks Angebot Kauf auf Rechnung)?
VSV ASVAD	Seite 60 - 62	Datenschutz-Folgeabschätzung 1. Es ist nicht klar für welche Bearbeitung eine Datenschutz-Folgeabschätzung vorgenommen werden muss 2. In welcher Form Muss die Datenschutz-Folgeabschätzung erfolgen? Wir sind der Auffassung, dass nur bei der Bearbeitung von besonders schützenswerten Daten eine Datenschutz-Folgeabschätzung notwendig ist und alle anderen Bearbeitungen davon ausgenommen werden können. 3. Was passiert, wenn der Beauftragte gleichzeitig der Verantwortliche ist? (Beispiel KMU mit 10 Angestellten)
VSV ASVAD	Seite 64	Datenschutzfreundliche Voreinstellungen 1. Wir sind nicht einverstanden mit der Feststellung, dass das Anlegen eines Benutzerkontos schon zu einer umfassenderen Bearbeitung von Personendaten führt. Jede Online-Bestellung führt zu einem Zusammenführen von Einkaufshistorie und Kunde, das Anlegen eines Benutzerkontos oder Benutzerprofils ist eine reine administrative Tätigkeit, welche nicht zwingend zu umfassenderen Daten führt! 2. Nicht eingegangen wird hier auf das Thema Cookies / Nachverfolgung von Kundenbewegungen.
VSV ASVAD	Seite 65	Dokumentationspflicht Es wird hier offensichtlich, dass eine klare Unterscheidung zwischen «normaler Datenbearbeitung» und «Bearbeitung von besonders schützenswerten Daten» fehlt. Die Dokumentationspflicht wird immer über die gesamte Datenbearbeitung «gestülpt». Damit wird jedes Unternehmen in Bezug auf seine Datenbearbeitung dokumentationspflichtig, auch wenn es nur eine Adresse oder

		eine Selektion einer Adresse für einen Werbeaussand betrifft.
VSV ASVAD	Seite 66	Auskunftsrecht Der Grundsatz weicht von der Vorgabe der SEV 108 ab und ist unbegründet. Selbst strenge Gesetzgebungen wie das Deutsche Datenschutzgesetz sehen keine kostenlose Auskunft vor! Dieser Grundsatz und SWISS FINISH wird den Standort Schweiz für Datenbetreiber äusserst unattraktiv machen und steht diametral gegen die Digitalisierungsbemühungen des Bundesrates in der Landschaft!
VSV ASVAD	Seite 88	Übergangsbestimmungen Die Übergangsbestimmungen müssen insbesondere für Altdaten ergänzt worden. Wir sind mit der bestehenden Formulierung einverstanden, verlangen aber eine Ergänzung. Altdaten müssen weiterhin verwendet werden können. Dies sollte über eine erweiterte Formulierung in den Übergangsbestimmungen ersichtlich werden. Wir schlagen vor, Altdaten mit einer Klausel während 10 Jahren als «eingewilligt» zu deklarieren, natürlich immer mit der Möglichkeit des Konsumenten die Datenbearbeitung zu widerrufen. Ohne diese Formulierung werden viele Unternehmen in kürzester Zeit vor existentiellen Problemen oder dem Richter stehen.
Fehler! Verweisquelle konnte nicht gefunden werden.		

Amstutz Jonas BJ

Von: Maria Winkler <maria.winkler@itandlaw.ch>
Gesendet: Freitag, 10. März 2017 13:48
An: Amstutz Jonas BJ
Cc: heribert.grab@siemens.com; renate.lang@ch.schindler.com; werner.wyss@zkb.ch; Severine.Knuesli@swisscom.com; christoph.hofer@axonactive.ch; stefano.longoni@viollier.ch; David.Rosenthal@homburger.ch
Betreff: Stellungnahme zum VE-DSG
Anlagen: 2017-03 - 10_VUD_Stellungnahme_VE_DSG_def.pdf
Signiert von: maria.winkler@itandlaw.ch

Sehr geehrter Herr Amstutz

Im Namen des Vereins Unternehmens-Datenschutz VUD stelle ich Ihnen unsere Stellungnahme zum Vorentwurf des revidierten DSG zu.

Bei Fragen können Sie sich gerne an mich wenden.

Freundliche Grüsse

mag. iur. Maria Winkler
Geschäftsstelle Verein Unternehmens-Datenschutz VUD

IT & Law Consulting GmbH
Grafenaustrasse 5
6300 Zug
Tel. +41 41 711 74 08
Fax +41 41 711 74 07
maria.winkler@itandlaw.ch
www.itandlaw.ch

VUD | Verein Unternehmens-Datenschutz

Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Vorbemerkungen

Der Verein Unternehmens-Datenschutz VUD ist ein Zusammenschluss der betrieblichen Datenschutzbeauftragten von mehr als 50 Unternehmen der Schweiz, welcher der selbständigen und unabhängigen Meinungsbildung verpflichtetet ist. Der VUD ist eine Plattform, welche sich dem Austausch von Know-how widmet und auf diese Weise die Entwicklung von Best Practices im Bereich Datenschutz unterstützt.

Der VUD nimmt im Folgenden unter Einhaltung der Vernehmlassungsfrist Stellung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz. Der VUD beschränkt sich in seiner Stellungnahme im Wesentlichen auf die Bestimmungen, welche für Private anwendbar sind.

Artikel	Bemerkungen
Allgemeine Bemerkungen zum VE-DSG	Der Vorentwurf verwendet verschiedene Begriffe, die ungenügend definiert und / oder ungenügend von anderen Begriffen abgegrenzt werden (z.B. Daten, Dritte, Empfängerin und Empfänger, etc.). Der Entwurf muss formell überarbeitet werden, da teilweise Aufzählungen nicht korrekt oder nicht kohärent sind. Die deutsche und die französische Version des VE-DSG stimmen in einigen Bestimmungen nicht überein (Art. 9 VE-DSG). Die Bestimmungen zum betrieblichen Datenschutzbeauftragten wurden gestrichen, was der VUD bedauert und was insbesondere auch im Hinblick auf die gemäss dem erläuternden Bericht beabsichtigte Förderung der Selbstregulierung unverständlich erscheint. Die Funktion des betrieblichen Datenschutzbeauftragten kann heute in der Schweiz als etabliert angesehen werden, obwohl nach dem geltenden DSG keine entsprechende gesetzliche Verpflichtung besteht. Im Interesse der Reduktion des administrativen Aufwands für Unternehmen sollte denjenigen Unternehmen, die einen betrieblichen Datenschutzbeauftragten bezeichnen, gewisse Erleichterungen (z.B. betr. Meldepflichten) gewährt werden.
Art. 1 Abs. 2 VE-DSG	Im Zweckartikel sollte auch der **Schutz der Wettbewerbsfähigkeit** der Schweiz ausdrücklich erwähnt werden, zumal im erläuternden Bericht wiederholt explizit darauf hingewiesen wird, dass das ein Ziel der Revision sei (vgl. z.B. S. 5, 9,10).

Artikel	Bemerkungen
Geltungsbereich Art. 2	Bei hängigen Verfahren soll das DSG – wie im geltenden Recht – nicht anwendbar sein. «Dieses Gesetz soll nicht anwendbar sein auf hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren.»
Begriffe Art. 3 VE-DSG	**Personendaten** sind nur mehr Daten von **natürlichen Personen**, die Daten **juristischer Personen** sind vom Geltungsbereich des DSG ausgenommen. Der VUD begrüsst diese Anpassung im Sinn einer Angleichung an das EU-Recht.
	Statt vom «**Inhaber der Datensammlung**» ist nun vom «**Verantwortlichen**» die Rede. Als Verantwortlicher gilt die private Person oder das Bundesorgan, das über den Zweck, die Mittel und den Umfang der Datenbearbeitung entscheidet. Gemäss erläuterndem Bericht müssen daher **2 Kriterien** erfüllt sein: Verantwortlicher ist, wer einerseits festlegt, zu welchen Zwecken die Daten bearbeitet werden und andererseits, mit welchen Mitteln dies erfolgt. Das entscheidende Kriterium ist somit, wer über die Mittel zur beabsichtigten Datenbearbeitung bestimmt. Dies kann insbesondere im Zusammenhang mit der **Auftragsdatenbearbeitung** zu **Abgrenzungsschwierigkeiten** führen. Wenn das outsourcende Unternehmen keinen Einfluss auf die konkreten Mittel hat, mit denen der Outsourcingnehmer die Daten bearbeitet (was insbesondere bei grossen international tätigen Dienstleistern der Fall sein wird), dann wird sich aufgrund dieser Bestimmung die Frage stellen, wer als Verantwortlicher zu gelten hat und welche Rechtsfolgen damit verbunden sind. Im Rahmen der Vernehmlassung sollte eine **Klärung** herbeigeführt werden.
	Neu eingeführt wird der Begriff des «**Auftragsbearbeiters**». Generell wurden im VE-DSG gewisse Pflichten neu auch dem Auftragsbearbeiter zugewiesen, andere wiederum nur dem Verantwortlichen. Dabei ist für uns kein durchgehendes Konzept zu erkennen. Dies sollte geklärt werden. Hinzu kommt, dass es uns an vielen Stellen unpassend erscheint, nebst dem Verantwortlichen auch den Auftragsbearbeiter in die Pflicht zu nehmen, da er letztlich nur nach Weisung des Verantwortlichen handelt und handeln darf.
	Im Vorentwurf wird an verschiedenen Stellen der Begriff des «Empfängers» verwendet, ohne dass klar ist, was der Unterschied zum «Dritten» ist. **«Empfänger»** ist eine natürlich oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die gestützt auf eine spezialgesetzliche Grundlage personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger. Der VUD ist der Meinung, dass der Begriff des Empfängers zu definieren und von dem des Dritten abzugrenzen ist, falls er beibehalten wird. Falls es keine Definition für «Empfänger» gibt, ist in den betreffenden Gesetzesbestimmungen dieser Ausdruck zu streichen und durch «Dritte» zu ersetzen.
	Genetische Daten werden neu bei der Definition der besonders schützenswerten Personendaten aufgeführt. Nach Auffassung des VUD sollten nur diejenigen **genetischen Daten** dazu zählen, die den Zweck haben, eine natürliche Person eindeutig zu identifizieren. Dies sollte so in lit. c übernommen werden. Dasselbe gilt für **biometrische Daten**. Dort

Artikel	Bemerkungen
	genügt es derzeit, dass sie es erlauben, eine Person eindeutig zu identifizieren. Jedes Foto einer Person tut dies. Das ist viel zu breit.
	Der Begriff des **Persönlichkeitsprofils** soll gestrichen und stattdessen der Begriff des «**Profilings**» eingeführt werden, was **zu begrüssen** ist. Das Persönlichkeitsprofil war eine schweizerische Besonderheit, die in der praktischen Anwendung immer wieder zu Schwierigkeiten führte. Das Profiling stellt im Gegensatz zum Persönlichkeitsprofil auf den Vorgang der Auswertung von Daten für bestimmte Zwecke ab und ist auch in der DSGVO enthalten. Im Gegensatz zur DSGVO und E-SEV 108 liegt ein Profiling nach dem VE-DSG aber • nicht nur bei einer automatisierten, sondern **bei jeder Auswertung von Daten** vor und • sie liegt auch dann vor, wenn Daten ausgewertet werden, die **keine Personendaten** sind, sofern die Auswertung zu dem **Zweck** erfolgt, wesentliche persönliche Merkmale zu analysieren oder Entwicklungen insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit Intimsphäre oder Mobilität vorherzusagen. Der Einbezug der Auswertung von «Daten», die keine Personendaten sind in den Begriff Profiling erfolgt gemäss dem erläuternden Bericht aus dem Grund, weil es heute möglich sei, Daten ohne persönlichen Bezug so auszuwerten, dass anschliessend Personendaten vorliegen. **Daten, welche aufgrund des Profilings entstehen**, sind gemäss erläuterndem Entwurf grundsätzlich **Personendaten** im Sinn von Art. 3 Buchstabe a VE-DSG (Seite 44). Der **Einbezug von anderen Daten** in die Definition des **Profilings** ist nach Auffassung des VUD **abzulehnen**. • Das Datenschutzgesetz bezieht sich grundsätzlich nur auf Personendaten und die Ausweitung der Bearbeitung anderer Daten ist bereits wegen der Definition der Personendaten, welche auch die Daten einbezieht, bei denen die betroffene Person **bestimmbar** ist, **überflüssig**. • Andererseits führt der Einbezug anderer Daten insbesondere im Hinblick auf die **Pflichten**, die dem Verantwortlichen (und allenfalls dem Auftragsbearbeiter) im Vorentwurf im Zusammenhang mit dem Profiling überbunden werden, zu Problemen, die in der Praxis wohl nicht so einfach zu lösen sein werden. So stellt ein Profiling **ohne die ausdrückliche Einwilligung der betroffenen Person** eine **Persönlichkeitsverletzung** dar (Art. 23 Abs. 1 Bst. d VE-DSG). Dies auch dann, wenn das Profiling keine unmittelbaren Auswirkungen auf die betroffene Person hat (siehe den erläuternden Bericht zu Art. 15 VE-DSG, Seite 59). Es stellt sich hier beispielsweise die Frage, ob und wenn ja wann eine solche Einwilligung eingeholt werden muss, wenn beispielsweise Geodaten ausgewertet und diese erst später der betroffenen Person zugeordnet werden. • Wenn zudem nicht nur die automatisierte sondern **jede Auswertung von Daten** zu den genannten Zwecken als Profiling gilt, dann muss wohl für jede manuelle Durchsicht von Daten eine ausdrückliche Einwilligung der betroffenen Person eingeholt werden, was praktisch unmöglich sein wird. Der Begriff des Profilings sollte daher analog zur DSGVO nur die **automatisierte Auswertung von Daten** umfassen und **nur die Auswertung von Personendaten**.

Artikel	Bemerkungen
Zweckbindung Art. 4 Abs. 3 VE-DSG Grundsätze	Personendaten dürfen nur zu einem bestimmten und für die betroffene Person **klar erkennbaren Zweck** beschafft werden; **sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist**. Mit dieser Bestimmung wird, analog zu den Bestimmungen der EU, der Grundsatz eingeführt, dass Personendaten auch zu einem Zweck verwendet werden dürfen, der mit dem ursprünglichen Zweck **kompatibel** ist. Dies ist **zu begrüssen**. Der Betonung auf die "klare" Erkennbarkeit ist jedoch zu streichen, da seine Bedeutung nicht klar ist. Wie stark ein Zweck hervorgehoben bzw. darauf aufmerksam gemacht werden muss, ergibt sich aus dem damit verbundenen Risiko, der Ungewöhnlichkeit, etc. Bedeutet "klare" Erkennbarkeit z.B., dass sich ein Zweck nicht mehr aus den Umständen ergeben kann? Genügt eine Gesetzesbestimmung, damit eine Bearbeitung "klar" erkennbar ist?
Datenrichtigkeit Art. 4 Abs. 5 VE-DSG	Die geltende Bestimmung in Art. 5 DSG ist klarer als der neue Vorschlag. Falls der neue Vorschlag übernommen werden soll, ist die Verpflichtung *«[…] und wenn nötig nachgeführt wurden»* zu streichen, weil der Einschub (i) unklar und (ii) überflüssig ist. Ferner ist in den Erläuterungen klarzustellen, dass keine Vernichtungspflicht besteht, wenn gesetzliche und/oder regulatorische Aufbewahrungsvorschriften bestehen.
Einwilligung Art. 4 Abs. 6 VE-DSG	Neu schreibt das DSG vor, dass eine gültige Einwilligung **eindeutig** zu erfolgen hat. Was dies genau bedeutet, wird im erläuternden Bericht nicht erklärt. Die Erläuterungen weisen vielmehr darauf hin, dass die Neuformulierung eine terminologische Annäherung an den E-SEV 108 und die DSGVO ermöglicht. Da die Frage der Eindeutigkeit einer Willenserklärung bereits durch das bestehende Recht geregelt wird und davon nicht abgewichen werden soll, wirft die Ergänzung mehr Fragen auf als sie beantworten will. Sie sollte daher gestrichen werden. Es kann in der Botschaft geklärt werden, dass der Schweizer Begriff der Einwilligung alle Voraussetzungen der E-SEV 108 erfüllt. Ferner sind die Ausführungen der Erläuterungen zum Vorentwurf hinsichtlich der Frage der **Ausdrücklichkeit** nicht klar, sondern verwirren eher. Sie sollten geklärt werden. Wir verweisen auf Rz. 30 ff. in Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017. Schliesslich ist der VUD der Ansicht, dass das Erfordernis der Ausdrücklichkeit einer Einwilligung für ein **Profiling** sich nicht rechtfertigt. Der Begriff des Profiling ist zwar "gefühlt" etwas Bedrohliches, aber bei Lichte betrachtet erfasst der Begriff in der Mehrheit harmlose Alltagshandlungen.
Bekanntgabe ins Ausland Art. 5 VE-DSG	Die Bestimmung von Art. 5 Abs. 2 VE-DSG ist widersprüchlich und unklar. Es sollte klargestellt werden, dass Daten nur ins Ausland übermittelt werden dürfen, wenn entweder die Voraussetzungen von Abs. 2 oder eine der Ausnahmen von Abs. 3 vorliegen. Zudem sollte in den Erläuterungen klargestellt werden, dass der Angemessenheitsbeschluss des Bundesrats analog zu Art. 45 Abs. 1 DSGVO nicht nur die Gesetzgebung von Staaten, sondern auch von Gebieten, Sektionen oder internationalen Organisationen betreffen kann.

Artikel	Bemerkungen
	Es wird neu zwischen "spezifischen" und "standardisierten" **Garantien** unterschieden, wobei letztere offenbar auch von einem Datenbearbeiter selbst stammen können (und sie entsprechend der Genehmigung durch den EDÖB unterliegen). Es ist allerdings nicht klar, worin der Unterschied besteht. Die Unterscheidung macht aus Sicht der Praxis auch keinen Sinn. In aller Regel sind «spezifische» Garantien in Verträgen enthalten. Es ist praxisfern, wenn nun sämtliche Verträge, die solche Klauseln enthalten, dem EDÖB vorgelegt werden müssen. Zumal der EDÖB dem Öffentlichkeitsgesetz BGÖ untersteht und ein erhebliches Risiko besteht, dass diese Verträge qua BGÖ eingesehen werden können. Es ist lediglich zwischen vom EDÖB anerkannten Standardverträgen und anderen Verträgen und Garantien zu unterscheiden, die einer genaueren Prüfung bedürfen, falls an der Genehmigungspflicht festgehalten wird. Die Frist von sechs Monaten (Abs. 5), die zudem durch die Nachforderung von Informationen durch den EDÖB beliebig verlängerbar ist, macht ein Genehmigungsverfahren äussert unpraktikabel und führt zu unzumutbaren Verzögerungen bei Auslandstransfers. Eine Frist von 30 Tagen sollte genügen; sie tat es bisher auch.
Bekanntgabe ins Ausland in Ausnahmefällen Art. 6 Abs. 1 lit. a VE-DSG	Der Terminus „Einzelfall“ impliziert eine allzu starke Einschränkung und führt in der Praxis zu Unklarheiten in der Anwendung. Nach allgemeinen Grundregeln genügt es, wenn die betroffene Person mit Bezug auf bestimmte wiederkehrende Sachverhalte generell gültig zustimmen kann, mithin nicht nur für einen aktuellen Einzelfall, sondern auch mit Wirkung für analoge künftige Fälle. Dies entspricht heutiger anerkannter Praxis. Wir empfehlen deshalb die Streichung dieses Begriffs. Anpassungsvorschlag: ….. *die betroffene Person ~~im Einzelfall~~ eingewilligt hat*;
Art. 6 lit. b VE-DSG	Die Bearbeitung im **Zusammenhang mit Verträgen** sollte wie in der DSGVO auch Datenbearbeitungen erfassen, die lediglich im Interesse der betroffenen Person abgeschlossen oder sonst in die Vertragsabwicklung involviert sind (z.B. Kontaktpersonen), und nicht nur die Bearbeitung von Daten des Vertragspartners selbst. Die Meldepflicht von Datentransfers gestützt auf Abs. 1 Bst. b, c und d geht viel zu weit und scheint nicht sinnvoll. Der EDÖB wird zudem nicht über die Kapazitäten verfügen, diese Meldungen zu bearbeiten. Diese Bestimmung sollte daher gestrichen werden. Der Satz in Buchstabe f) ist unverständlich formuliert, so dass sich nicht erschliesst, was hier gesagt werden will.

Artikel	Bemerkungen
Art. 6 Abs. 1 lit. c VE-DSG	Um schwierige Abgrenzungsfragen auszuschliessen, sollten in Art. 6 Abs. 1 lit. c Ziff. 2 VE-DSG die Begriffe „Gericht“ sowie „Verwaltungsbehörde“ gestrichen werden. Massgebend ist, dass die Datenbearbeitung zur „Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen“ erfolgt. Die hierfür zuständigen ausländischen Behörden können aus historischen Gründen unterschiedlich organisiert sein sowie verschiedene Bezeichnungen tragen und sich nicht in eine der beiden Kategorien zuordnen lassen. Da es sich um ausländische Stellen und Verfahren handelt, dürfen deshalb nicht allein schweizerische Traditionen massgebend sein. Vielmehr ist die Klausel offen zu formulieren, um auch wesentlich von Schweizer Traditionen abweichende Verfahrensformen zur Rechtsdurchsetzung zu erfassen. Zu diesem Zweck ist der Satzteil «… *vor einem Gericht oder einer Verwaltungsbehörde* …» ersatzlos u streichen.
Art. 6 Abs. 1 lit. d VE-DSG	Vgl. Ausführungen zu Art. 6. Abs. 1 lit. a VE-DSG. Anpassungsvorschlag: *«…. die Bekanntgabe ~~im Einzelfall~~ notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen* …»
Art. 6 Abs. 2 VE-DSG	Die Verpflichtung, den EDÖB trotz Ausnahmetatbestand zu informieren, ist unverhältnismässig und überdies auch kontraproduktiv, da Ausnahmetatbestände i.d.R. zeitkritisch sind und keinen Aufschub dulden. Zudem würde diese breite Pflicht zu einer unverhältnismässig grossen Anzahl Meldungen führen, deren Bewältigung für den EDÖB schwierig sein dürfte. Schliesslich würde der EDÖB über heikle Verfahren und (Geschäfts-)Geheimnisse informiert, ohne dass ein (datenschutzrechtlicher) Grund dafür vorliegen würde. Zudem ist diese Pflicht dem EU Recht (inkl. E-SEV 108) fremd und somit ein Swiss Finish. Deshalb ist Abs. 2 ersatzlos zu streichen.
Auftragsdatenbearbeitung Art. 7 VE-DSG	Der Verantwortliche muss sich neu auch vergewissern, dass der **Auftragsbearbeiter** sowohl die **Datensicherheit** als auch die **Rechte der betroffenen Person** gewährleisten kann. Es ist unklar, welche Pflichten dem Auftragsbearbeiter damit überbunden werden sollen. Zudem kann der Auftragsbearbeiter nicht sämtliche Rechte der betroffenen Personen gewährleisten, daher ist diese Bestimmung zu streichen bzw. auf die Gewährleistung der Datensicherheit zu beschränken. Gemäss Abs. 4 darf der Auftragsbearbeiter die Datenbearbeitung ohne eine **schriftliche Zustimmung des Verantwortlichen** keinem weiteren Auftragsbearbeiter übertragen. Diese strengen Formanforderungen sind praxisfremd. Es genügt, eine dokumentierte Zustimmung zu verlangen, die Schriftlichkeit gemäss Art. 13 OR ist nicht erforderlich. Sie muss zudem in genereller Weise möglich sein; diese Variante ist im Gesetz vorzusehen, falls sie nur mit einem Veto-Recht des Verantwortlichen akzeptiert werden soll. Diese Anpassungen bringen neu erheblich **mehr Aufwand** beim Outsourcing der Datenbearbeitung.
Empfehlungen der guten Praxis Art. 8 und 9 VE-DSG	Im Gegensatz zu den Regelungen in der DSGVO (Art. 40 und 41), nach der eine Ausarbeitung von Verhaltensregeln nur durch Verbände und andere Vereinigungen vorgesehen ist, kann nach dem VE-DSG **der EDÖB selbst** solche Empfehlungen ausarbeiten. Dies **widerspricht** dem Zweck von «Verhaltensregeln», die bereits in der EU-Datenschutzrichtlinie 95/46/EG vorgesehen waren und die auf dem **Gedanken der Selbstregulierung** beruhen.

Artikel	Bemerkungen
	Zudem besteht ein **Risiko**, dass der EDÖB das Mittel von «Empfehlungen der guten Praxis» dazu nutzen kann, seiner eigenen Interpretation von datenschutzrechtlichen Fragen mehr Gewicht zu verleihen. Er ist zwar verpflichtet, die interessierten Kreise beizuziehen, er ist aber nach dem Wortlaut der Norm nicht verpflichtet, deren Inputs auch zu berücksichtigen. Zudem stellt sich die Frage der Rechtsstaatlichkeit, da gegen Empfehlungen, die der EDÖB erlässt, kein Rechtsmittel ergriffen werden kann bzw. nur sehr eingeschränkter Rechtsschutz besteht. Die «Empfehlungen der guten Praxis» sollten analog zu den Regelungen in der EU als Mittel der Selbstregulierung von den Verantwortlichen ausgehen und allenfalls durch den EDÖB (oder eine zuständige Aufsichtsbehörde) genehmigt werden. Die genauen Rechtswirkungen dieser Empfehlungen sind unklar. Gemäss erläuterndem Bericht ist die Einhaltung der Empfehlungen freiwillig. Wer sie jedoch einhält, der «befolgt diejenigen Datenschutzvorschriften, welche die Empfehlungen konkretisieren». Es ist daher davon auszugehen, dass in dem Fall, in dem man **nachweisen** kann, dass man sich an die Empfehlungen hält, eine gesetzliche Vermutung besteht, dass der Verantwortliche sich gesetzeskonform verhält. Dies sollte ausdrücklich so geregelt werden.
Daten einer verstorbenen Person Art. 12 VE-DSG	Diese Regelung auf alle Datenbearbeitungen der Unternehmen aller Branchen (z.B. Banken, Spitäler, klinische Forschung, Behörden) auszudehnen wird zu **grossen Aufwänden** bzw. zu **Rechtsunsicherheit** führen. Dies insbesondere auch, da Abs. 3 der Bestimmung besagt, dass **Amts- oder Berufsgeheimnisse** nicht geltend gemacht werden können (wie schaut es jedoch mit der Strafbarkeit aus?). Streitfälle mit Erben, die gegen oder unabhängig von der Erbengemeinschaft vorgehen, sind ebenfalls vorprogrammiert; sie sollen zudem sogar mehr Rechte haben als die betroffene Person selbst. Und wie kann eine verstorbene Person ein "überwiegendes Interesse" haben? Der VUD vertritt die Auffassung, dass diese Fragen, so tatsächlich ein Regelungsbedarf besteht, in den betreffenden Spezialgesetzen zu regeln sind, weshalb Art. 12 VE-DSG ersatzlos gestrichen werden sollte. Mit Datenschutz hat diese Bestimmung nichts zu tun.
Informationspflicht bei der Beschaffung von Personendaten Art. 13 VE-DSG	Die Informationspflicht wird auf **alle Personendaten** ausgeweitet, was zu erheblichem **Mehraufwand** für die Unternehmen führen wird. In den Erläuterungen sollte präzisiert werden, dass bei allfälligen Änderungen keine Nachinformation erfolgen muss. Art. 13 Abs. 3 VE-DSG verwendet die Begriffe «Dritter» und «Empfängerinnen und Empfänger», ohne diese genau zu definieren. Unklar ist auch, warum eine Differenzierung zwischen «Beschaffung» und «Bearbeitung» gemacht wird. Der gesamte Absatz ist unklar formuliert, was insbesondere die Abgrenzung der Pflichten des Verantwortlichen und des Auftragsdatenbearbeiters betrifft. Der VUD ist daher der Meinung, dass Abs. 3 ersatzlos zu streichen ist. Art. 13 Abs. 4 VE-DSG geht weit über die DSGVO hinaus und ist als «Swiss Finish» abzulehnen. Die Bestimmung, die übrigens ebenfalls unklar formuliert ist, ist zu streichen.

Artikel	Bemerkungen
	Generell führt diese Vorschrift zu noch umfangreicheren Informationen durch AGB und Datenschutzerklärungen und dadurch zu mehr Aufwand und einer Überflutung der betroffenen Personen mit Informationen, welche den Nutzwert reduzieren wird. Art. 13 Abs. 5 VE-DSG: Diese Regelung ist viel strenger als die Regelung in der EU-DSGVO. Sie verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Unmittelbar nach der Beschaffung werden die Daten gespeichert und wohl erst nachher überhaupt gelesen. Diese praxisfremde Regelung sollte mit einer Regelung in Anlehnung an die GDPR ersetzt werden.
Ausnahmen von der Informationspflicht Art. 14 VE-DSG	Die Berufung auf ein überwiegendes privates Interesse ist weiterhin nicht möglich, wenn die Daten einem Dritten weitergegeben werden (was z.B. auch eine Konzerngesellschaft sein kann). Für diese Einschränkung gibt es keinen Grund und sie sollte gestrichen werden. Sie würde in manchen Fällen und ganz besonders in Konzernverhältnisse zu einem enormen administrativen Mehraufwand, der in der Sache aber nicht zu mehr Transparenz für die Betroffenen führt. Um ein anderes Beispiel zu nennen: Journalisten könnten künftig keine Recherchen durchführen ohne nicht jede einzelne Person, über die sie Daten erhalten, darüber ausführlich zu informieren, da sie sich nicht auf die Ausnahmen berufen können. Die Fälle, in denen ein überwiegendes privates Interesse in der Regel besteht, sollten analog zu Art. 24 VE-DSG aufgeführt werden (vgl. die Ausführungen zum Auskunftsrecht). Es ist unklar, was genau mit dem Begriff der «Übermittlung» in Abs. 4 gemeint ist. Dies sollte klargestellt werden.
Informationspflicht bei automatisierten Einzelentscheidungen Art. 15 VE-DSG	Der VE-DSG unterscheidet im Gegensatz zur DSGVO und zur E-SEV 108 stärker zwischen dem Profiling und den automatisierten Einzelentscheiden. Die Informationspflicht nach Art. 15 VE-DSG muss erfüllt werden, wenn die automatisierte Einzelentscheidung rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat und unterscheidet sich damit im Wortlaut von Art. 22 DSGVO und Art. 8 Abs. 1 Bst. a der E-SEV 108. Während die E-SEV 108 nur auf «**erhebliche Auswirkungen**» Bezug nimmt, spricht die DSGVO davon, dass die automatisierte Einzelentscheidung rechtliche Wirkungen entfaltet oder die betroffene Person in ähnlicher Weise erheblich beeinträchtigt. Beide Bestimmungen machen daher vom Wortlaut her klar, dass die Pflichten des Verantwortlichen nur greifen, wenn die Auswirkungen der automatisierten Entscheidung **erheblich** sind. Der Wortlaut von Art. 15 VE-DSG deutet hingegen darauf hin, dass die Pflichten des Verantwortlichen **immer** greifen, wenn die automatisierte Entscheidung **rechtliche Wirkungen** für die betroffene Peron entfaltet, ohne dass diese erhebliche Auswirkungen haben müssen.

Artikel	Bemerkungen
	Die **Voraussetzungen** für das Kriterium «rechtliche Wirkungen» sollten besser geklärt und es sollte klargestellt, dass auch diese einen gewissen **Schweregrad** erreichen müssen, damit die Informationspflicht greift. Um die Vorteile, die automatisierte Entscheidungen für die Unternehmen bringen, nicht durch übermässige administrative Aufwände zunichtegemacht werden, müssen die Rahmenbedingungen der Information und Anhörung (insbesondere deren Inhalt und der Zeitpunkt) genauer geklärt werden. Zudem ist unklar, welche Folgen die Äusserung der betroffenen Person hat.
Datenschutz-Folgenabschätzung Art. 16 VE-DSG	Die Durchführung einer Datenschutz-Folgenabschätzung muss erfolgen, wenn eine Datenbearbeitung **voraussichtlich zu einem erhöhten Risiko führt**. Die Frage, ob ein erhöhtes Risiko vorliegen kann, kann allenfalls erst nach der Durchführung einer Datenschutz-Folgenabschätzung beantwortet werden, was unbefriedigend ist. Eine solche Prüfung wird aber nötig sein, da die Bestimmung strafbewehrt ist. Dies wird dazu führen, dass in der Praxis auch für Bearbeitungen, für die keine formale Datenschutz-Folgeabschätzung erforderlich ist, eine solche durchgeführt werden muss, was nicht Sinn der Sache ist, da es unnötigen Aufwand darstellt. Es ist ferner klarzustellen, dass ein Risiko für eine **Persönlichkeitsverletzung** (vgl. Abs. 2 VE-DSG) bestehen muss und nicht bloss irgendein Risiko für irgendetwas. Gemäss erläuterndem Bericht ist ein erhöhtes Risiko immer dann gegeben, wenn die spezifischen Eigenschaften der geplanten Datenbearbeitung darauf schliessen lassen, dass die Verfügungsfreiheit der betroffenen Person über ihre Daten erheblich eingeschränkt wird oder werden kann, was einen extrem weiten Anwendungsbereich für diese Bestimmung eröffnet. Bereits das Versenden einer kritischen E-Mail, das Verfassen eines kritischen Medienbeitrags oder die Durchführung einer internen Untersuchung wegen Hinweisen auf rechtswidrige Handlungen im Betrieb können nach diesen tiefen Anforderungen genügen. Dies ist nicht sachgerecht. Um Rechtsunsicherheiten zu vermeiden, müssen die Voraussetzungen, bei deren Vorliegen eine Datenschutz-Folgenabschätzung durchgeführt werden muss, genauer geregelt werden. Als Beispiel dafür können die Bestimmungen von § 10 IDG (ZH) i.V.m. §24 IDV (ZH) genannt werden. Zudem ist es nicht die Aufgabe des Auftragsbearbeiters, die Datenschutz-Folgenabschätzung vorzunehmen. Der Auftragsbearbeiter muss aus der Bestimmung gestrichen werden. Die in Art. 16 Abs. 3 VE-DSG enthaltene Meldepflicht muss zudem gestrichen oder zumindest auf den Fall eingeschränkt werden, dass im Rahmen der Datenschutz-Folgenabschätzung wesentliche Risiken festgestellt wurden und diese auch nach Ergreifung angemessener Massnahmen bestehen bleiben. Die vorgesehene Regelung würde zu massenhaften Meldungen an den EDÖB führen, die er allein mangels Ressourcen nicht in der Lage ist zu bearbeiten. Zudem muss klar geregelt werden, welche Informationen an den EDÖB weitergeleitet werden und wie mit diesen insbesondere bei Informationszugangsgesuchen nach dem Öffentlichkeitsgesetz (BGÖ) umgegangen wird. Datenschutz-Folgenabschätzungen von Unternehmen werden häufig Geschäftsgeheimnisse enthalten, an denen auch die Konkurrenzunternehmen interessiert sind. Die Frist von drei Monaten, die dem EDÖB für die Prüfung der Massnahmen zur Verfügung stehen, sind in der Praxis vollkommen untauglich und führen dazu, dass wichtige Projekte ungebührlich lang verzögert werden. Diese Bestimmung

Artikel	Bemerkungen
	muss gestrichen bzw. durch eine angemessene kürzere Frist ersetzt werden. Unter Hinweis auf die Aufgaben des EDÖB gestützt auf Art. 49 lit. a VE-DSG soll der kooperative Austausch zwischen privaten Personen und dem EDÖB weiter gefördert und zu proaktivem Handeln motiviert werden. Zudem sollten Unternehmen, die einen **betrieblichen Datenschutzbeauftragten** bezeichnet haben, von der Meldepflicht generell ausgenommen sein.
Meldung von Verletzungen des Datenschutzes Art. 17 VE-DSG	Im Gegensatz zur DSGVO und E-SEV 108 findet die Bestimmung im Vorentwurf auf jede Datenschutzverletzung Anwendung. Für eine derart weitgefasste Meldepflicht gibt es keinen Anlass. Der **Begriff des Data Breach** sollte daher analog der DSGVO formuliert werden; hier ist eine Kompatibilität auch aus praktischen Überlegungen sinnvoll. Die DSGVO erfasst lediglich Sicherheitsverstösse, die zu einem Verlust des Gewahrsams an den Daten führt. Der VUD erachtet die parallele Strafbewehrung der Meldepflicht wie der Verletzung der Datensicherheit für rechtsstaatlich bedenklich, da es die Mitarbeiter zwingt, einander gegenseitig ans Messer zu liefern. Wird das Unternehmen selbst sanktioniert, verletzt die Bestimmung den ***nemo tenetur* Grundsatz** direkt. Es sollte geprüft werden, ob eine Meldung nicht zu einer Strafbefreiung führt. Ferner hält der VUD es für sinnvoll, die Meldung nur dann zu verlangen, wenn eine **Vielzahl von Personen** betroffen ist, und nicht schon jede falschgeleitete E-Mail. Aufwand und Nutzen stehen sonst in keinem Verhältnis, auch seitens des EDÖB. Vorangesagtes macht zudem um so mehr Sinn, wenn der unbestimmte Begriff **voraussichtlich** Kriterium sein soll, dass eine allfällige Verletzung nicht gemeldet werden muss, weil sie **allenfalls** nicht zu einem Risiko führt. In der Folge werden die Unternehmen gezwungen sein, jegliche Art und Umfang von Verletzungen dem EDÖB zu melden, um keiner Sanktion ausgesetzt zu sein. Dies bedeutet sowohl für die Unternehmen als auch den EDÖB einen nicht zu rechtfertigenden Aufwand. Der Begriff der **Unverzüglichkeit** einer Meldung ist weiter zu klären und abzuschwächen. Eine Meldung sollte ohne unnötigen Verzug erfolgen. Eine schnelle Meldung bringt in der Sache nichts, wenn die Hintergründe und Auswirkungen eines Data Breachs noch nicht geklärt sind. Der EDÖB kann ohnehin nicht mehr tun als das betroffene Unternehmen. Die Pflichten des **Auftragsbearbeiters** sind auf jene des Verantwortlichen abzustimmen; derzeit besteht hier eine wenn auch nur sprachliche Differenz (keine Information über einen Verlust von Daten).
Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen Art. 18 VE-DSG	Die Formulierung von Art. 18 VE-DSG ist unklar und geht über die in Art. 25 DSGVO enthaltenen Anforderungen hinaus. Der VUD vertritt zudem die Auffassung, dass Art. 18 VE-DSG systematisch zu Art. 11 VE-DSG gehört bzw. bereits durch das geltende Recht gedeckt ist, zumindest Privacy by Design. Die Bestimmung sollte gestrichen und in Art. 11 VE-DSG integriert werden, wobei nicht über die Anforderungen der DSGVO hinauszugehen ist.

Artikel	Bemerkungen
Dokumentationspflicht Art. 19 VE-DSG	Inhalt und Ausmass der Pflicht zur Dokumentation der Datenbearbeitung gemäss lit. a sollte auf das Führen eines Verzeichnisses aller Datenverarbeitungen beschränkt werden, für die der Verantwortliche zuständig ist. Die Dokumentationspflicht sollte keinesfalls über die in Art. 30 DSGVO enthaltenen Pflichten hinausgehen. Weitergehende Dokumentationspflichten führen zu einem unverhältnismässigen Aufwand für die Wirtschaft, ohne einen entsprechenden Mehrwert für den Datenschutz zu bringen. Die Informationspflicht von Art. 19 lit. b VE-DSG darf nach Meinung des VUD höchstens für die Berichtigung, Löschung und Vernichtung von Daten gelten, nicht jedoch für die Verletzung des Datenschutzes und die Einschränkung der Bearbeitung nach Art. 25 Abs. 2 oder 34 Abs. 2 VE-DSG. Zudem ist der Auftragsdatenbearbeiter aus dieser Bestimmung zu streichen, da ihm Pflichten auferlegt werden, die er in der Regel nicht erfüllen kann, da er nicht über die erforderlichen Informationen verfügt (beispielsweise über die Richtigkeit der Daten). Wir verweisen zudem auf Rz. 69 ff. in Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017.
Information der Empfänger von Personendaten Art. 19 VE-DSG	Die Pflicht, die Empfänger von Personendaten über die Berichtigung, Löschung, etc. zu informieren, erscheint vom Grundgedanken nachvollziehbar, geht aber viel zu weit, da ständig Berichtigungen, Löschungen, etc. stattfinden, deren Mitteilung an Empfänger keinerlei Sinn macht (z.B. wenn Daten gelöscht werden, weil sie nicht mehr benötigt werden). Die Pflicht zur Information sollte auf Fälle beschränkt werden, in welchen die **betroffene Person dies verlangt** und ein **schützenswertes Interesse** hat. Will der Verantwortliche dem nicht nachkommen, soll er überwiegende eigene und Dritte Interessen dem entgegenhalten können. Der Verweis auf einen "unverhältnismässigen Aufwand" genügt nicht, da dieser Begriff erstens sehr eng ausgelegt werden soll, und es zweitens auch andere Interessen auf dem Spiel stehen können, die einer Information der Drittempfänger entgegenstehen. Dass die Pflicht zur Information auch eine solche über **Datenschutzverstösse** umfasst, ist nicht nachvollziehbar und sie verstösst gegen den Grundsatz **nemo tenetur**, dass diese Bestimmung gleichzeitig strafbewehrt ist. Sie geht sogar weiter als die Pflicht zur Information der betroffenen Person selbst. Die DSGVO sieht auch keine solche Information vor. Sie ist daher zu streichen. Die einzelnen **Modalitäten** der Pflicht sind völlig unklar. Wie hat die Information zu erfolgen? Wer ist zu den Empfängern der Daten zu zählen, z.B. schon jede Person, die eine E-Mail erhalten hat mit einer Information, die sich nachträglich als falsch herausgestellt hat und korrigiert worden ist? Verlangt die Norm, dass ein Unternehmen ein Protokoll von Empfängern führt (d.h. seinerseits zusätzliche Personendaten bearbeitet), und wie lange? Die Norm ist auch in dieser Hinsicht auf ein vernünftiges Mass zu beschränken. Die Verpflichtung des **Auftragsbearbeiters** ist in jedem der Fälle zu streichen. Es ist nicht seine Aufgabe, sondern jene des Verantwortlichen. Der Auftragsbearbeiter hat lediglich Instruktionen auszuführen.
Auskunftsrecht Art. 20 VE-DSG	Es fehlt weiterhin an **Massnahmen zur Bekämpfung des Missbrauchs des Auskunftsrechts**, so namentlich eine zweckentfremdete Nutzung zur Beweismittelausforschung, die heute an der Tagesordnung ist und die Unternehmen

Artikel	Bemerkungen
	massiv belastet. Da das DSG neu auch während Gerichtsverfahren gilt, dürften die Missbräuche noch weiter zunehmen. Das Auskunftsrecht ist so anzupassen, dass es für die (datenschutzfremde) Beweismittelausforschung nicht mehr interessant ist, z.B. indem der Auskunftspflichtige wählen kann, die Auskunft nicht mehr in Form einer Kopie an den Auskunftssuchenden zu erstatten, sondern an eine dritte Stelle, welche die Verletzung des Datenschutzes stellvertretend prüft oder wo die Unterlagen eingesehen, aber nicht mitgenommen werden können. Es ist die Möglichkeit, **Ausnahmen von der Kostenlosigkeit** für Auskunftsersuchen vorzusehen, festzuhalten. In der DSGVO müssen Auskunftsersuchen ebenfalls nicht zwingend kostenlos sein. Im Auskunftsrecht ist neu eine Pflicht zur **Begründung jeglicher Entscheide** versteckt, welche auf einer Bearbeitung von Personendaten basieren, und zwar nicht nur im Falle von automatisierten Einzelentscheiden (Abs. 3). Dies greift massiv in die Freiheit eines Unternehmens ein und geht deutlich über das hinaus, was die DSGVO verlangt oder sinnvoll erscheint. Das Auskunftsrecht ist diesbezüglich auf **automatisierte Einzelfallentscheide** zu beschränken und zwar auf solche, denen eine betroffene Person tatsächlich unterworfen ist (und auf die sie daher hinzuweisen ist). Geschieht dies nicht, wird auch dieses Auskunftsrecht primär der Ausforschung und Schikane dienen. Zu erwähnen ist, dass auch für das Auskunftsrecht, welches auf Art. 14 VE-DSG verweist, die uneingeschränkte Berufung auf **überwiegende private Interessen** zwingend ist; die wichtigsten Fälle sind zudem exemplarisch aufzuzählen (z.B. keine Herausgabe von Korrespondenz mit dem eigenen Anwalt, Geschäftsgeheimnisse, Unterlagen zur internen Meinungsbildung, Sicherheitsinteressen, Unterlagen, die der Auskunftssuchende schon hat).
Art. 23 VE-DSG	Das Erfordernis der **Einwilligung für ein Profiling** ist zu streichen, da es aus Sicht des VUD keinen Grund gibt, an dieses zusätzliche Anforderungen zu stellen. Es besteht weder im bestehenden Recht, noch wird es europarechtlich gefordert. Zwar gibt es heikle Profilings, aber der Vorgang wird emotional deutlich überbewertet. Er umfasst auch zahlreiche, völlig harmlose Vorgänge (z.B. Geldbezug an einem Bankomaten), selbst wenn der Begriff auf automatisierte Profilings beschränkt wird (z.B. Berechnung des Alterskapitals einer Person gemäss BVG), für die neu strengere Voraussetzungen und durch den vorgeschlagenen Wortlaut neu als Persönlichkeitsverletzung gelten würden. Das erscheint nicht sachgerecht, insbesondere vor dem Hintergrund, dass bereits in der Anwendung der Bearbeitungsgrundsätze das mit einer Datenbearbeitung verbundene Risiko für die betroffene Person zu berücksichtigen ist. In der Botschaft ist darauf zu achten, dass zu **Art. 23 Abs. 3** nicht abermals der Hinweis erfolgt, dass auch in diesen Fällen die Bearbeitungsgrundsätze einzuhalten sind. Dies ist falsch, denn in diesen Fällen wird vermutet, dass gerade keine Persönlichkeitsverletzung vorliegt, selbst wenn diese nicht eingehalten wurden.
Art. 24 VE-DSG	Statt in Abs. 2 davon zu sprechen, dass ein überwiegendes Interesse "möglicherweise gegeben" ist, ist die bisherige Formulierung zu verwenden. Dass in den aufgezählten Fällen ein überwiegendes Interesse normalerweise gegeben ist, ist unbestritten. Ein Gericht sollte davon nur **in begründeten Fällen** abweichen.

Artikel	Bemerkungen
	Der Rechtfertigungsgrund des Abschlusses und der **Abwicklung des Vertrags** sollte auch die Bearbeitung von Daten weiterer, in den Vertrag involvierten Personen umfassen, wie z.B. Begünstigte (z.B. Empfänger eines Geschenks) und mit der seitens des Vertragspartners mit der Abwicklung des Vertrags betraute Personen (z.B. Kontaktperson für Rückfragen).
Art. 27 VE-DSG	Da die Bestimmung neu eine Grundlage in einem formellen Gesetz verlangt, wenn ein **automatisierter Einzelfallentscheid** erfolgen soll, werden Bundesorgane künftig ihre Prozesse nicht mehr automatisieren dürfen, selbst wenn dies aus Gründen der Effizienz sachgerecht ist, da die erwähnten Grundlagen regelmässig fehlen und auch im Vorentwurf nicht vorgesehenen sind. Ein Beispiel ist die heute bei einigen Krankenkassen weitgehend automatisierte Beurteilung von Rückerstattungsanträgen bei der gesetzlichen Krankenversicherung. Diese werden wieder manuell abgewickelt werden müssen, was zu deutlichen Mehrkosten führt. Das ist nicht sachgerecht.
Art. 43 VE-DSG	Für die Ausdehnung der Kompetenzen des EDÖB über den Datenschutz hinaus auf **andere Rechtsgebiete** (Abs. 2) besteht kein Raum. Der EDÖB verfügt nicht über das zur Durchsetzung etwaiger Datenexportbeschränkungen anderer Gesetze erforderliche Know-how.
Art. 44 VE-DSG	Zwar ist nur die private Person, gegen welche sich ein Verfahren richtet, Partei, aber dennoch wird dem EDÖB in Art. 41 Abs. 5 VE-DSG erlaubt bzw. verpflichtet, auch **anderen Personen über einen Fall zu berichten** und so die Geheim- und Privatsphäre des Unternehmens zu verletzen. Dies ist einzuschränken. Vorsorgliche Massnahmen im Bereich der Datenbearbeitung können massive Konsequenzen für Unternehmen haben, ja können einen Betrieb lahmlegen. Die Erfahrungen haben gezeigt, dass der EDÖB vorsorgliche Massnahmen auch ohne vertieftes Abwägen der Folgen solcher verlangt. Eine unabhängige Überprüfungsmöglichkeit ist daher entscheidend, und bis diese stattfindet, muss eine **aufschiebende Wirkung** bestehen. Es sollte dem Gericht überlassen sein zu entscheiden, die aufschiebende Wirkung zu entziehen.
Strafbestimmungen Art. 50-55 VE-DSG	Die vorgesehenen Strafbestimmungen sind abzulehnen. Sie führen zu einer **nicht sachgerechten Kriminalisierung** der mit Datenschutz befassten Mitarbeiter. Sie werden dazu führen, dass die gesetzlich gewollten Spielräume bei der Datenbearbeitung aus Angst vor persönlicher Bestrafung nicht ausgeschöpft werden und sehr viel mehr Bürokratie betrieben werden wird als sinnvoll. Statt sich auf die Einhaltung des Datenschutzes zu fokussieren (die Verletzung der Bearbeitungsgrundsätze wird nicht sanktioniert), werden alle Ressourcen auf die Einhaltung der formalen, mit Strafe bedrohten flankierendem Massnahmen konzentriert werden, was dem Datenschutz einen Bärendienst erweist. Es wird zudem schwieriger werden, Fachleute für die betreffenden Stellen in den Unternehmen zu gewinnen, da sie sich einem Strafbarkeitsrisiko aussetzen. Eine Versicherung ist nicht erlaubt. Profitieren werden vor allem die externen Rechtsberater, was die Kosten massiv nach oben treiben wird. Die Regelung ist auch von behördlicher Seite ineffizient, da künftig zwei parallele Verfahren geführt werden müssen, eines vom EDÖB und eines von den kantonalen Strafverfolgungsbehörden, die zudem nicht über das erforderliche Know-how verfügen. Ferner ist bei diversen der Antragsdelikte unklar, wer überhaupt antragsberechtigt ist bzw. von wem der Strafantrag ausgehen sollte (z.B. bei einer unterlassenen Datenschutzfolgeabschätzung).

Artikel	Bemerkungen
	Zudem stellt sich insbesondere bei Pflichten, die auf **Ermessensentscheidungen** beruhen, die Frage, inwieweit sich diese überhaupt dazu eignen, bestraft zu werden. Als Beispiele können hier die Verstösse gegen Art. 11 (Sicherheit von Personendaten), Art. 16 (Datenschutz-Folgeabschätzung), Art. 18 (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen) sowie Art. 19 Abs. 1 (Dokumentation der Datenbearbeitungen) genannt werden. So muss beispielsweise die Dokumentationspflicht nach Art. 19 Abs. 1 VE-DSG so erfüllt werden, «dass den Informations- und Meldepflichten nachgekommen werden kann» und eine Datenschutz-Folgenabschätzung nach Art. 16 VE-DSG muss durchgeführt werden, «wenn die Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die betroffene Person führt». Das strafrechtliche Bestimmtheitsgebot erscheint jedenfalls nicht eingehalten. Auf die Verletzung des Grundsatzes **nemo tenetur** im Zusammenhang mit den Meldepflichten wurde bereits hingewiesen. Dieses Problem besteht auch im Zusammenhang mit den Kooperationspflichten gegenüber dem EDÖB, soweit es Verhalten betrifft, die für die betroffenen Personen bzw. Unternehmen zu einer Sanktionierung führen können. Die Bestrafung **fahrlässigen Verhaltens** ist nicht sachgerecht und auch europarechtlich nicht erforderlich. Dieses wird die vorstehend beschriebenen unerwünschten Folgen verstärken. Die Begehung des Tatbestandes durch fahrlässiges Verhalten ist daher komplett **zu streichen**. Eine Sanktionierung sollte nach Ansicht des VUD primär das **Unternehmen** betreffen. Die diesbezügliche Regelung im Vorentwurf nützt nichts, da die Mitarbeiter sich nicht darauf verlassen können, dass sie zur Anwendung gelangt. Auch ist die Grenze mit CHF 100'000 zu tief. Sie sollte bei CHF 250'000 bis 500'000 liegen. Warum die **Verfolgungsverjährung** auf fünf Jahre ausgedehnt wird, ist ebenfalls nicht nachvollziehbar. Für die Verschärfung der heute in Art. 35 DSG geregelten **beruflichen Schweigepflicht** besteht kein Anlass. Die Norm ist so zu belassen, wie sie ist. Die vorgeschlagene Anpassung würde zahlreiche Unternehmen zur Befolgung eines scharfen Berufsgeheimnisses zwingen, für das kein Bedarf besteht und das in der Praxis auch nicht gelebt würde. So ist nicht einzusehen, warum ein Online-Shop den faktisch selben Geheimhaltungspflichten wie ein Arzt oder Anwalt unterliegen soll.
Art. 59 VE-DSG	Die **Übergangsbestimmungen** sind ungenügend. Bedarf für solche gibt es auch bei etlichen anderen der geänderten Regelungen. Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, analog der Regelung der DSGVO.
Unbefugte Datenbeschaffung Art. 179novies StGB	Es ist mindestens in der Botschaft klarzustellen, dass mit "unbefugter" Datenbeschaffung (weiterhin) eine Datenbeschaffung gegen den Willen des Verantwortlichen einer Datenbearbeitung gemeint ist, und nicht eine gegen den Datenschutz verstossende Datenbearbeitung.
Art. 139 Abs. 3 IPRG	Die Wahlmöglichkeiten zur Anwendbarkeit des Schweizer Rechts gehen schon heute sehr weit. Sie erlauben es neu einer betroffenen Person, die DSGVO selbst dort zur Anwendung zu bringen, wo diese von sich aus gar nicht angewendet

Artikel	Bemerkungen
	werden will, etwa wenn ein Schweizer Unternehmen die Daten von Kunden aus der Schweiz bearbeitet, dies aber unter Beizug eines Outsourcing-Providers in der EU tut. Obwohl in der Sache selbst kein Bezug zur EU besteht, könnte ein Schweizer Kunde aufgrund von Art. 139 IPRG die Anwendung der DSGVO verlangen. Es ist daher darin vorzusehen, dass ein ausländischer Erfolgsort nicht allein damit begründet werden kann, dass die Daten im betreffenden Land gespeichert sind.
ZPO	Die Befreiung von **Gerichtskosten** für Datenschutzverfahren ist eine unnötige Belastung der Kantone. Sie wird den Datenschutz nicht fördern.

Verein Unternehmens-Datenschutz VUD, März 2017

Amstutz Jonas BJ

Von: Baumgartner, Leo <Leo.Baumgartner@warnerbros.com>
Gesendet: Mittwoch, 5. April 2017 16:26
An: Amstutz Jonas BJ
Betreff: Stellungsnahme zur Totalrevision Datenschutzgesetz
Anlagen: Totalrevision-des-Datenschutzgesetzes_Stellungnahme_Warner Bros.docx

Sehr geehrte Damen und Herren

In der Beilage finden Sie unsere Stellungsnahme.

Best Regards
Leo Baumgartner
Warner Bros. Entertainment Switzerland GmbH
Distributor for 20th Century Fox Films
Tel. +41 44 495 77 01
Mobile +41 79 691 16 91

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : Warner Bros. Entertainment Switzerland GmbH

Abkürzung der Firma / Organisation : WBCH

Adresse : Mürtschenstr. 25, 8048 Zürich

Kontaktperson : Leo Baumgartner, Geschäftsführer

Telefon : +41 44 495 77 01

E-Mail : leo.baumgartner@warnerbros.com

Datum : 4. April 2017

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
AVCH	Die Neuregelung des Datenschutzrechts gemäss VEDSG betrifft die Bearbeitung personenbezogener Daten, insbesondere Privater, in zahllosen Bereichen. Vielfach ist nicht ersichtlich, ob und wie der Entwurf diese Vielfalt der Lebensbereiche berücksichtigt und „Kollateralschäden", ungewollte Beeinträchtigungen üblicher Abläufe und Geschäfte, vermeiden soll. Im Gegenteil, sieht der VEDSG nicht nur verschärfte Anforderungen an die Datenbearbeitung vor, sondern zudem eine masslose strafrechtliche Verantwortlichkeit für die Einhaltung dieser Pflichten, die teils völlig unbestimmt und auch im Einzelfall durch den Verantwortlichen gar nicht genau bestimmbar sind. Jeder, der in solchen Bereichen personenbezogene Daten bearbeitet, würde jederzeit mit einem Bein vor dem Strafrichter stehen. Das widerspricht elementaren rechtsstaatlichen Grundsätzen. Für AudioVision steht in diesem Zusammenhang im Vordergrund, den Inhabern von Urheber- und verwandten Schutzrechten *die Durchsetzung ihrer Rechte in rechtsstaatlichen Verfahren – namentlich vor Zivilgerichten und im Strafprozess – zu ermöglichen.* Betroffen sind aber nicht nur Urheberrechtsinhaber, sondern jede und jeder Rechtssuchende. Die *Vorbereitung und das Führen gerichtlicher Verfahren* ist ohne mehr oder weniger weitgehende Bearbeitung personenbezogener Daten durch Private nicht möglich. Typischerweise diese geht mit der Notwendigkeit einher, Daten auch ohne Kenntnis des Tatverdächtigen bzw. Anspruchsgegners zu bearbeiten. Die Vorbereitung und das Führen solcher Prozesse und Verfahren wäre nach den Regeln des VEDSG absehbar massiv erschwert, ggf. schlicht unmöglich. Schon der „Logistep"-Entscheid des Bundesgerichts (BGE 136 II 508) hat seit Jahren zu einem völligen *Stillstand der Rechtsdurchsetzung gegen Urheberrechtsverletzungen* im Internet geführt. Anstatt diesem Missstand abzuhelfen, würde der VEDSG diese Situation – für Inhaber von Urheberrechten wie für beliebige andere Geschädigte – noch verschlimmern. Geradezu eine Zumutung ist es vor diesem Hintergrund, dass der Bericht zum VE (S. 46) dezidiert darauf beharrt, auch für die Zukunft die Erhebung von IP-Adressen zur Aufklärung von Urheberrechtsverletzungen per se, ohne Rücksicht auf die Umstände, zu Zweckbindungsverstössen zu

	erklären. *Das Handeln verletzter Rechteinhaber, welche die nötigen Belege zum Führen rechtsstaatlicher Verfahren erheben, wird damit explizit ins Unrecht gesetzt.* Weitere Regelungen erschweren oder verunmöglichen die Kommunikation zwischen Rechtsvertretern und Klientschaft (zumal ausländischer) in solchen Verfahren. Dieser Entwurf ist zurückzuweisen und gesamthaft zu überarbeiten, um rechtsstaatlichen Grundsätzen zu genügen und das Führen rechtsstaatlicher Verfahren nicht zu verunmöglichen. Andernfalls wäre das Datenschutzrecht gegen die Rechtsdurchsetzung als „Täter-Schutzrecht“ instrumentalisierbar.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
AVCH	VEDSG	2	2	lit. c	**Nicht-Anwendbarkeit auf gerichtliche/behördliche Verfahren** Abweichend vom bisherigen Recht (Art. 2 Abs. 2 lit. c DSG, vgl. dazu etwa Maurer-Lambrou/Kunz in BSK-DSG Art. 2 N 26, Botschaft DSG BBl. 88 II 413 ff., 442) sind *nicht mehr Gerichtsverfahren* (Zivilprozesse, Strafverfahren und verwaltungsrechtliche Verfahren höherer Instanz) *als solche* vom **Anwendungsbereich des Gesetzes** ausgenommen, sondern nurmehr die Datenbearbeitung durch die Justizbehörden und Gerichte. Im Umkehrschluss wird die *Datenbearbeitung durch Verfahrensparteien* dem VEDSG vorbehaltlos unterstellt. Dies, obwohl *„die Rechte der Parteien und Verfahrensbeteiligten in diesem Fall allein vom Prozessrecht beherrscht“* sein sollten, wie der Bericht zum VE zutreffend festhält (S. 40; so z. B. nach Art. 95-99 StPO). Z. B. erlangen Verfahrensparteien durch *Akteneinsicht,* durch die *Rechtsschriften* der Gegenparteien etc. Einblick in personenbezogene Daten, die sie selbstverständlich zur Wahrung ihrer Rechte im Verfahren auch *weiter bearbeiten,* ggf. *an Dritte* (Parteien untereinander, Rechtsvertreter an Klientschaft etc.) weitergeben müssen. Wie anhand der einzelnen – teils verschärften – Vorschriften des VEDSG zu zeigen ist, würde die Verfahrensvorbereitung und -führung im Zusammenspiel dieser Vorgaben unmöglich bzw. das Risiko schwerwiegender Sanktionsfolgen unüberschaubar. Soweit die Datenbearbeitung durch private Verfahrensparteien unter den Anwendungsbereich geltender
AVCH	VEDSG	3			

					Verfahrensordnungen (auch kantonaler; denn die private Datenbearbeitung untersteht auch insoweit dem DSG) fällt, ist diese (weiterhin) per se ***vom Geltungsbereich des DSG auszunehmen.*** *In Art. 2 Abs. 2 VEDSG ist auch die Bearbeitung personenbezogener Daten durch die Verfahrensparteien im Rahmen der durch das eidgenössische oder kantonale Prozess- und Verfahrensrecht bestimmten Verfahren vom Anwendungsbereich des VEDSG vollständig auszunehmen.* Soweit die Datenbearbeitung durch private Verfahrensparteien ausserhalb dieses Anwendungsbereichs (z. B. in der vorprozessualen Vorbereitung und der Führung solcher Verfahren) an sich unter den Geltungsbereich des DSG fällt, ist diese durch einen ***Rechtfertigungsgrund*** vom weitreichenden Unrechtsurteil des VEDSG auszunehmen (dazu unten, Abschnitt zu „Per se widerrechtliche Datenbearbeitungen, Art. 23 Abs. 2 lit. b, c und d VEDSG).
AVCH	VEDSG	5, 6			**Datenbekanntgabe ins Ausland** Während grundsätzlich die **Datenbekanntgabe ins Ausland** ohne angemessenen Datenschutz nur unter Geltung vertraglicher Garantien oder unternehmensinterner Datenschutzvorschriften zulässig ist, die neu in jedem Falle von EDÖB bewilligt werden müssen – teils mit langen Bearbeitungsfristen –, enthält Art. 6 Abs. 1 lit. c Ziff. 2 hiervon – zutreffend – eine **Ausnahme für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gerichten und** neu auch **Verwaltungsbehörden.** Die entsprechende, bestehende Vorschrift (Art. 6 Abs. 2 lit. d DSG) findet hauptsächlich betreffend die Verfahrensführung im Ausland Aufmerksamkeit. Daher scheint die Klarstellung ratsam, dass dies auch bei entsprechenden Verfahren vor *inländischen Gerichten und Verwaltungsbehörden* gilt; z. B. bei der Information ausländischer Klientschaft über den Gang eines sie betreffenden Verfahrens in der Schweiz.

					Diese Klarstellung ist um so bedeutsamer, als auch der Verstoss gegen diese Pflichten nach Art. 50 Abs. 2 lit. a und Abs. 4 mit Busse bis CHF 500‘000 – selbst bei nur fahrlässiger Begehung bis CHF 250‘000 **strafbar sein soll.** *In Art. 6 Abs. 1 lit. c Ziff. 2 ist zu ergänzen: „[…] vor in- und ausländischen Gerichten und Verwaltungsbehörden“.*
AVCH	VEDSG	13	1-2		**Informationspflicht bei Datenbeschaffung** Anstelle des bisherigen Transparenzprinzips (Erkennbarkeit) soll prinzipiell **bei jeder Beschaffung von Personendaten der Betroffene aktiv informiert** werden; u. a. über den die Kategorien bearbeiteter Daten und den Zweck der Bearbeitung. Es liegt auf der Hand, dass dies mit der Vorbereitung und Führen von Zivilprozessen oder z. B. einer Strafanzeige nicht vereinbar ist; insbesondere, wenn der Erfolg der Rechtsdurchsetzung von der Ermittlung weiterer Sachverhalte durch Strafverfolgungsbehörden oder einer geeigneten Prozessstrategie abhängt. Der Verantwortliche wäre im Ergebnis verpflichtet, *dem Beschuldigten oder der Gegenpartei seine prozessualen Schritte anzukündigen* und zugleich *die ihm verfügbaren Informationen offenzulegen.* Die Ausnahme in Art. 14 Abs. 2 lit. b nützt nichts (zumal sie restriktiv auszulegen wäre; Bericht S. 58): Hier geht es nicht darum, ob die Information *möglich* ist, sondern dass sie die Rechtsdurchsetzung vereiteln würde (vgl. Art. 14 Abs. 4 lit. 2 Ziff. 2 VEDSG, der aber nur Bundesorganen hilft). Auch die Ausnahmen in Art. 14 Abs. 3 lit. b und Abs. 4 lit. a helfen nicht: Auf **überwiegende Interessen Dritter** kann sich der Verantwortliche in der Regel nicht berufen (auch sollen hier Datenschutz-Interessen, nicht Rechtsdurchsetzungs-Interessen, im Vordergrund stehen; Bericht S. 58). Auch **eigene überwiegende Interessen** würden unter erhöhter Rechtsfertigungslast stehen (Bericht S. 58); und wären
AVCH	VEDSG	14	2-3		

					ganz unbeachtlich, wenn die Daten dafür auch weitergegeben werden müssten, was in der Verfahrensvorbereitung, wie gezeigt, regelmässig unvermeidbar ist. Dies ist um so unhaltbarer, als der hier vorprogrammierte Verstoss nach Art. 50 Abs. 1 lit. a und Abs. 4 mit Busse bis CHF 500‘000 – selbst bei nur fahrlässiger Begehung bis CHF 250‘000 **strafbar sein soll.** *In Art. 14 Abs. 2 ist mit neuer lit. c zu ergänzen, dass die Informationspflicht auch entfällt, wenn die Information die Durchsetzung von Rechten in einem behördlichen oder gerichtlichen Verfahren beeinträchtigen oder gefährden würde.*
AVCH	VEDSG	16			**Datenschutz-Folgenabschätzung** Unter der blossen Voraussetzung, dass die vorgesehene Datenbearbeitung *voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person* führen können, wäre der Verantwortliche per se verpflichtet, eine **Datenschutz-Folgenabschätzung** vorzunehmen, darin die geplante Bearbeitung zu umschreiben und den EDÖB darüber zu unterrichten. Es liegt auf der Hand, dass diese Voraussetzung bei der Vorbereitung und Führung eines Zivilprozesses häufig, einer Strafanzeige praktisch stets gegeben sein wird (z.B. kann eine Strafanzeige eine Hausdurchsuchung und letztlich eine Freiheitsstrafe für den Betroffenen nach sich ziehen). Mit anderen Worten, *hätten Verfahrensparteien in aller Regel die Verfahrensführung dem EDÖB offenzulegen* und dessen – innerhalb von drei Monaten vorgebrachten – Einwände zu berücksichtigen. Das kann nicht die Absicht der Bestimmung sein. Dies ist um so unhaltbarer, als auch der Verstoss gegen diese Pflichten nach Art. 50 Abs. 1 lit. c und Abs. 4 mit Busse bis CHF 500‘000 – selbst bei nur fahrlässiger Begehung bis CHF 250‘000 **strafbar sein soll.**

					In Art. 16 ist klarzustellen, dass die Pflicht zur Datenschutz-Folgenabschätzung und deren Offenlegen gegenüber dem EDÖB bei der Datenbearbeitung zur Vorbereitung und Führung gerichtlicher Verfahren nicht gilt.
AVCH	VEDSG	20			**Datenschutz-Auskunftsbegehren (Art. 20 i. V. m 21 und 14 VEDSG)** Die schon im geltenden Recht kaum befriedigende Situation, dass **Datenschutz-Auskunftsbegehren** zu nach Art. 8 DSG einer „Pre-Trial Discovery" ausgenutzt werden können, würde verschärft statt bereinigt; v.a. mit dem Wegfall der Ausnahme des Art. 2 Abs. 2 lit. c für Verfahrensparteien. Diese könnten ggf. gezwungen werden, ihre Verfahrens-Handakten oder Klageentwürfe sowie die Herkunft der Daten (Informanten, Zeugen) der Gegenpartei offenzulegen. Sogar wenn der Verantwortliche das Risiko eingeht, sich auf eine Ausnahme nach Art. 14 zu berufen, müsste er dem Betroffenen deren Grund angeben (Art. 21 Abs. 2 VE). D.h. er käme auf keine rechtmässige Weise umhin, der Gegenpartei seine Verfahrensabsichten offenzulegen. Die Ausnahmen, zu denen auf Art. 14 VE verwiesen wird, decken wie gezeigt die Prozessvorbereitung und -führung nicht ausreichend ab. Dies ist um so unhaltbarer, als auch der damit vorprogrammierte Verstoss nach Art. 50 Abs. 1 lit. a und Abs. 4 mit Busse bis CHF 500'000 – selbst bei nur fahrlässiger Begehung bis CHF 250'000 **strafbar sein soll.** Würde z.B. der Kläger der Gegenpartei, oder der Anzeigeerstatter dem Tatverdächtigen, auf dessen Auskunftsbegehren hin gewisse Informationen aus prozesstaktischen Gründen verheimlichen, müsste er dies *im vollen Risiko* tun, dass jener das zum Anlass einer Strafanzeige gegen den Kläger bzw. Anzeigeerstatter nehmen kann; und dass diesem eine Bestrafung bis zu CHF 500'000 droht, falls seine Rechtfertigung aus überwiegendem eigenem Interesses in der Abwägung misslingt. Ein solches Risiko bei
AVCH	VEDSG	21			
AVCH	VEDSG	14			

					der Vorbereitung der Rechtsdurchsetzung, notabene durch eine in ihren Rechten verletzte Person gegenüber dem mutmasslichen Verletzer, ist rechtsstaatlich nicht hinnehmbar. *Entsprechend der Informationspflicht, muss (analog zu Art. 14 Abs. 2 Ziff. 2 VE) auch die Auskunftspflicht mit neuer lit. c in Art. 14 Abs. 2 entfallen, wenn die Auskunft die Durchsetzung von Rechten in einem behördlichen oder gerichtlichen Verfahren beeinträchtigen oder gefährden würde.* *Dieser Ausnahmefall muss (analog Art. 21 Abs. 2 Satz 2 VE), auch berechtigen, von einer Begründung der berechtigten Auskunftsverweigerung abzusehen.*
AVCH	VEDSG	23	2	lit. b, c und d	**Per se widerrechtliche Datenbearbeitungen** **A. Datenbearbeitung entgegen ausdrücklicher Willenserklärung** **Art. 23 Abs. 2 lit. b i. V. m. Art. 3 lit. c VEDSG** Die **Bearbeitung von Personendaten entgegen einer ausdrücklichen Willenserklärung des Betroffenen** soll per se eine Persönlichkeitsverletzung, mithin einen Rechtsverstoss, darstellen (Bericht, S. 68 f.). Damit könnte die Partei eines Rechtsstreits oder der einer Rechtsverletzung Verdächtige seiner Gegenpartei *durch ein einfaches Verbot* der Datenbearbeitung die Vorbereitung des Verfahrens *massiv erschweren*. Gerechtfertigt wäre diese dann regelmässig einzig durch ein überwiegendes privates Interesse, wobei im VE kein konkretisierender Rechtfertigungsgrund dessen Feststellung erleichtert. Ob der Verantwortliche rechtmässig oder unrechtmässig handelt, lässt sich also nur unter offener
AVCH	VEDSG	24	2		

					Interessenabwägung – d.h. aus seiner Warte oft gar nicht – gesichert feststellen. Dieses Risiko, für den Zugang zu rechtsstaatlichen Verfahren Unrecht begehen zu müssen, ist nicht haltbar. *Begehren zusammengefasst unter Abschnitt* **C***.* **B. Bekanntgabe besonders schützenswerter Personendaten** **Art. 23 Abs. 2 lit. c i. V. m. Art. 3 lit. c VEDSG** Auch die **Bekanntgabe besonders schützenswerter Personendaten** soll per se einen Rechtsverstoss darstellen. Darunter fallen unter anderem Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, die – neben anderem – im Verfahren eine Rolle spielen müssen. *Im Strafverfahren* ist sogar jede Information betreffend den Beschuldigten *naturgemäss besonders schützenswert*. Verfahrensvorbereitung und –führung bedingen in aller Regel den Einbezug verschiedener Personen (Rechtsvertreter, Berater, weitere Parteien, Experten), mithin eine *Bekanntgabe solcher Personendaten an Dritte*. Es liegt daher auf der Hand, dass z.B. die Vorbereitung oder das Führen eines Strafverfahrens gegen eine Person diese Merkmale regelmässig erfüllen wird. Auch in diesem Fall ist die Rechtfertigung aufgrund einer offenen Güterabwägung mit ungewissem Ausgang im Einzelfall nicht tauglich, um den Zugang zum rechtsstaatlichen Verfahren nicht seinerseits ins Unrecht zu rücken. Auf die Ausführungen zu **Art. 23 Abs. 2 lit. b VE** wird verwiesen. *Begehren zusammengefasst unter Abschnitt* **C***.*

					C. "Profiling" ohne ausdrückliche Einwilligung **Art. 23 Abs. 2 lit. d i. V. m. Art. 3 lit. f VEDSG** Auch **"Profiling" ohne ausdrückliche Einwilligung des Betroffenen** soll per se einen Rechtsverstoss, darstellen. Darunter wäre jede Auswertung von Personendaten, aber *auch nicht personenbezogener Daten* zu verstehen, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Es liegt auf der Hand, dass z.B. die *Vorbereitung* oder das Führen *eines Zivil- oder Strafverfahrens* gegen eine Person *diese Merkmale regelmässig erfüllen wird*. Die Einwilligung kann in vielen Fällen, namentlich von Beschuldigten oder Gegenparteien, nicht eingeholt werden, ohne die Verfahrensführung in Frage zu stellen. Auch in diesem Fall ist die Rechtfertigung aufgrund einer offenen Güterabwägung mit ungewissem Ausgang im Einzelfall nicht tauglich, um den Zugang zum rechtsstaatlichen Verfahren nicht seinerseits ins Unrecht zu rücken. Auf die Ausführungen zu **Art. 23 Abs. 2 lit. b VE** wird verwiesen. **D. Begehren zu Art. 24 Abs. 2 VEDSG** Soweit die Datenbearbeitung durch private Verfahrensparteien, z. B. in der Verfahrensvorbereitung und -führung, nicht direkt unter das jeweilige Verfahrensrecht (und damit an sich unter den Geltungsbereich des DSG) fällt, ist diese durch einen Rechtfertigungsgrund vom Unrechtsurteil des VEDSG auszunehmen, um Wertungskonflikte und teils absurde Rechtsfolgen auszuschliessen. Die Rechtfertigung müsste im Sinn einer (widerlegbaren) Vermutung gelten *(„grundsätzlich" statt „möglicherweise")*, um nicht jede Datenbearbeitung zu solchen Zwecken von vornherein ins Unrecht zu setzen. Anwendungsbereich geltender Verfahrensordnungen (auch kantonaler; denn die private

					Datenbearbeitung untersteht auch insoweit dem DSG) fällt, ist diese (weiterhin) per se vom auszunehmen. *In Art. 24 Abs. 2 VEDSG ist ein ausreichender Rechtfertigungsgrund aufzunehmen, wonach es im Sinn einer Vermutung **grundsätzlich** durch ein überwiegendes privates Interesse gerechtfertigt ist, wenn ein Privater personenbezogene Daten bearbeitet zu dem alleinigen Zweck, ein durch das eidgenössische oder kantonale Prozess- und Verfahrensrecht geregeltes gerichtliches oder behördliches Verfahren vorzubereiten und zu führen, in welchem der Betroffene als Partei, Parteivertreter, Zeuge oder in anderer verfahrensrechtlich geregelter Stellung in Betracht kommt; dies einschliesslich der Bearbeitung und (im Rahmen dieses Zwecks) der Weitergabe **besonders schützenswerter Daten** sowie als **Profiling** zu qualifizierender Vorgänge.*
AVCH	VEDSG	25	2		**Bearbeitung ungesicherter Informationen** Der Betroffene soll in jedem Fall einen Anspruch haben, ungewisse bzw. **ungesicherte Informationen** in den Händen eines anderen mit **„Bestreitungsvermerk“** zu versehen und deren **Bearbeitung einzuschränken**. Daten, die in Vorbereitung und Führung von Verfahren bearbeitet werden, sind *stets ungesichert.* Es ist gerade Sache der Verfahren, den relevanten Sachverhalt zunächst festzustellen. Das heisst, über die (Un-) Richtigkeit wird das Gericht oder die Behörde nach den verfahrensrechtlich geltenden Bestimmungen zu befinden haben. Es wäre absurd, könnte z.B. der Beklagte dem Kläger auferlegen, Sachverhaltsdarstellungen in Verfahrensschriften bereits selbst mit „Bestreitungsvermerken“ zu versehen; oder ihn daran hindern, gewisse umstrittene Tatsachen den Behörden oder Gerichten vorzutragen. *Diese Vorschrift sollte keine Anwendung finden auf Daten, die allein zur Vorbereitung oder*

					Führung eines gerichtlichen oder behördlichen Verfahrens bearbeitet werden; sei es durch die Ausnahme der Verfahren in Art. 2 Abs. 2 und die Rechtfertigung der Verfahrensführung in Art. 24 Abs. 2, oder speziell in Art. 25 Abs. 2.
AVCH	VEDSG	41			**Untersuchung, Edition, Durchsuchung durch EDÖB** Bei blossen **Anzeichen für einen Verstoss** gegen Datenschutzvorschriften – welche nach dem oben Gesagten in Vorbereitung und Führung von Gerichts- und Behördenverfahren kaum zu vermeiden wären – soll der EDÖB eine **Untersuchung** eröffnen (Abs. 1), vom Verantwortlichen die **Edition** betreffender Akten verlangen (Abs. 2) sowie ohne Vorankündigung und **ohne richterliche Anordnung** die **Privatwohnung oder die Geschäftsräume** des Verantwortlichen **durchsuchen** können (Abs. 3). Das geht – entgegen dem Bericht (S. 78) – deutlich über die bisherigen Kompetenzen des EDÖB und v.a. deren rechtsstaatlichen Rahmen hinaus (u.a. mit der Hausdurchsuchungsbefugnis, aber auch in der weit unbestimmteren Voraussetzung der „Anzeichen“). Nicht nur wird hier praktisch ohne rechtsstaatliche Schutzmechanismen (die verwaltungsrechtliche Beschwerde bietet kaum ausreichenden Schutz) schwerstes Geschütz gegen den Verantwortlichen aufgefahren und der EDÖB zu einer *Ermittlungsbehörde ohne richterliche Aufsicht* umfunktioniert. Diese Kompetenzen wären nach dem VE noch nicht einmal eingeschränkt, wenn die Datenbearbeitung ihrerseits einen prozessualen Hintergrund hat. Diese Kompetenzen einer Datenschutzbehörde sind abwegig und ersatzlos zu streichen.
AVCH	VEDSG	50			**Strafandrohungen bei Verfahrens-/Sorgfaltspflichtverletzungen** Auch in den anderen als den vorgenannten Fällen ist eine Strafandrohung in der nun vorgesehenen Höhe von bis zu CHF 500‘000 Busse für die Verletzung verschiedenster Sorgfalts- und Verfahrenspflichten eine

					völlige Verkehrung der Verhältnisse und kein geeignetes, schon gar kein verhältnismässiges Instrument des Datenschutzes. Dies um so mehr, als die meisten der hier unter Strafandrohung gestellten Verstösse – zumal nach den strengeren Anforderungen des VEDSG, z. B. der generellen Informationspflicht - ausgesprochen offene Abwägungen und weite Beurteilungsspielräume voraussetzen, also praktisch keiner davon dem Bestimmtheitserfordernis für eine Strafnorm genügt. Zudem weist keiner dieser Tatbestände einen konkreten Bezug zu tatsächlichen Verletzungen der geschützten Rechtsgüter, d. h. Beeinträchtigungen der Betroffenen. auf. Diese stellen also allesamt abstrakte Gefährdungsdelikte dar, was sowohl zur Schwere der möglichen Beeinträchtigungen, als auch zur gar nicht begründeten Präventivwirkung ausser Verhältnis steht. *Die Strafnormen des DSG sind entweder im bisherigen, regulären Bussenrahmen zu belassen oder an präzise, abwägungs-/wertungsfreie Tatbestandsvoraussetzungen zu knüpfen, die dem Bestimmtheitsgebot genügen.*
AVCH	VEDSG	52			**Strafrechtlicher Geheimnisschutz** Hiernach soll mit bis zu drei Jahren strafbar sein, wer beruflich erlangte und zu eigenen (!) kommerziellen Zwecken bearbeitete Personendaten bekannt gibt. Nicht nur würde ein so weitgehender strafrechtlicher Geheimnisschutz völlig aus dem Rahmen des betsehenden, qualifizierten Geheimnisschutzes (z.B. Berufsgeheimnis der Anwälte etc., Art. 321 STGB; Amtsgeheimnis, Art. 320 StGB; Geschäftsgeheimnis, Art. 162 StGB, jeweils bis 3 Jahre). Das Konzept, den Berufsgeheimnisschutz undifferenziert auf sämtliche beruflich-kommerziellen Datenbearbeitungen zu erstrecken (Bericht S. 85 f.) ist verfehlt. Der Tatbestand ist sowohl den *Voraussetzungen* als auch dem *Adressaten und Zweck bzw. Kontext der Weitergabe* nach so offen, dass

					massenhaft Vorgänge des geschäftlichen Alltags strafbar würden – unter anderem auch die „beruflich“ (z. B. im Rahmen der Abklärungen eines in seinen Rechten verletzten Unternehmens) „zu kommerziellen Zwecken“ (nämlich zur Wahrung dieser Rechte) erhobener Daten, die (z.B. dem Anwalt, der Strafverfolgungsbehörde, dem Gericht, weiteren Geschädigten etc.) „bekanntgegeben“ werden. *Diese Strafnorm ist ersatzlos zu streichen. Bestimmten Schutzbedürfnissen in der elektronischen Datenbearbeitung wäre durch einzelne, spezifische qualifizierte Schutztatbestände nach dem Vorbild der bestehenden Berufsgeheimnisse nachzukommen.*
AVCH	VE-StGB	179novies			Auch dies ist ein viel zu unbestimmter neuer Straftatbestand, der zahllose Vorgänge des Alltagslebens unter Strafe stellen, bzw. den Verantwortlichen das unabsehbare Risiko möglicher Strafbarkeit auferlegen würde. Für die „Beschaffung“ „nicht jedermann zugänglicher“ Personendaten genügt es bereits, dass z. B. geschädigte Parteien untereinander ihre Erkenntnisse über den Schädiger, aber auch Unternehmen ihr Wissen über einen bestimmten Geschäftspartner austauschen u. dgl. Ob dies „unbefugt“ ist, würde sich nur aus den zahllosen offenen Abwägungsnormen des VEDSG entnehmen oder eben nicht entnehmen lassen, wie dem überwiegenden eigenen Interesse. Diese Strafnorm hält rechtsstaatlichen Grundsätzen nicht stand und ist *ersatzlos zu streichen.*

Wasser Energie Telekom

Versorgt mit Lebensqualität

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Zug, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DDSG)

Sehr geehrte Frau Bundesrätin

Sie haben am 21. Dezember 2016 interessierte Kreise eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nimmt die WWZ Telekom AG gerne wahr.

Die WWZ Telekom AG ist ein Anbieter von Telekommunikationsnetzinfrastrukturen und -dienstleistungen. Wir leisten damit einen grossen Beitrag an die digitale Vernetzung der Schweiz und deren Bevölkerung. Unser Kerngeschäft ist die Datenverarbeitung. Diese Daten erfüllen zunehmend und überwiegend die Voraussetzungen von Personendaten bzw. Daten, die zu einer Identifikation einer Person führen könnten. Datenschutz und Datensicherheit, sowie die entsprechenden Regulierungen sind daher für uns eine der wichtigsten Geschäftsgrundlagen. Entsprechend besteht eine hohe Betroffenheit, wenn diesbezüglich neue Regulierungen zur Diskussion stehen.

Gerne nehmen wir wie folgt Stellung, wobei wir zunächst auf einige grundsätzliche Punkte eingehen, ehe wir – wie verlangt – zu den einzelnen Bestimmungen des VE-DSG Stellung beziehen und Anträge stellen:

A. Grundsätzliche Bemerkungen

1. Chancen der Digitalisierung und damit auch Chancen der Datenbearbeitung

Die Digitalisierung bietet für die Zukunft ein enormes Entwicklungspotential und sollte durch unterstützende Rahmenbedingungen – gerade im Bereich Datenbearbeitung – gefördert werden. Die Schweiz sollte ein Wirtschaftsstandort für digitale Geschäftsmodelle sein und grösstmögliche Freiräume für die Datenbearbeitung zulassen. Grundsätzlich sollte jede Form von Datenbearbeitung zulässig sein und die informelle Selbstbestimmung sollte über Auskunfts- und Kontrollrechte realisiert werden. Ein Regulierungskonzept darf nicht der Vorstellung folgen, eine „Datenbearbeitung"

durch Unternehmen sei *per se* anrüchig. Ein modernes Datenschutzgesetz ist weiter auch kein spezielles Konsumentenschutzrecht.

Die im Vorentwurf vorherrschende „Verbots- und Bestrafungskultur" sollte deshalb so nicht umgesetzt werden. Die Datenschutzgesetzgebung ist bisher – und gemäss VE-DSG noch mehr – als Konsumentenschutzgesetzgebung stark von gesetzlichen Einschränkungen für Unternehmen geprägt, die jedoch in der Praxis durch Einwilligungserklärungen der Datensubjekte übersteuert werden können. Dies führt heute gesamthaft nicht zu mehr Datenschutz, sondern nur zu aufwendigeren Einwilligungsverfahren und damit höheren Transaktionskosten bei der Geschäftsabwicklung.

Wir begrüssen eine Stärkung des Rechts auf informelle Selbstbestimmung, lehnen jedoch die Stossrichtung ab, dass zukünftig einzelfallbezogene Zustimmungserklärungen eingeholt werden müssen. Für eine wirtschaftliche Geschäftsabwicklung muss es möglich sein, in einem Vertragsverhältnis eine pauschale Einwilligung über allgemeine Geschäftsbedingungen abzuschliessen. Die Grundlagen dazu genügen im UWG.

2. Gleichwertigkeit des Datenschutzes in der CH und in der EU

Datenschutzregulierung ist heute kein nationales Thema mehr. Die modernen Kommunikationsnetze und die technologischen Entwicklungen machen den Datenverkehr zu einem globalen Thema. Ein freier Datenverkehr ist aus unserer Sicht unbedingt zu erreichen, insbesondere durch eine gegenseitige institutionelle Anerkennung eines gleichwertigen Datenschutzes mit möglichst vielen Ländern. Allen voran natürlich mit der Europäischen Union und den USA. Damit können für Unternehmen hohe administrative Hürden und Kosten vermieden werden. Dabei sind die notwendigen Bestimmungen für eine Gleichwertigkeit im Datenschutz umzusetzen.

2.1 Unnötiger „Swiss Finish"

Ein Grund für die Revision des DSG ist gemäss Erläuterungsbericht des EJPD/BJ die Entwicklung des Datenschutzes im europäischen Raum. Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) EuDSGVO in Kraft. Zudem gilt die EU-Richtlinie 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen. Die DSG-Revision soll die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Die Annäherung würde zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür bilden, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht (obschon unserer Ansicht nach dies auch das bestehende DSG weiterhin tun würde). Die Revision des Schweizer DSG geht aber in mehreren Fällen über das Schutzniveau der EU hinaus, was nicht nachvollziehbar ist. Beispiele für diesen Swiss Finish sind:

a) Art. 13 Abs. 3 und 4 VE-DSG sehen eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein Versanddienstleister) sowie bei der Weitergabe von jeglichen Personendaten vor. Für den Adressaten solcher Informationen führt dies in einer zunehmend über digitale Geschäftsprozesse gesteuerten Gesellschaft zu einer Informationsflut. Nicht einmal die EU-Richtlinie 680/2016 vom 27. April 2016 sieht diesen Detaillierungsgrad vor.

b) Art. 16 Abs. 3 VE-DSG sieht eine Informationspflicht des Datenschutzbeauftragten über die Datenschutz-Folgeabschätzungen in jedem Fall vor. Die EU-Richtlinie 680/2016 hingegen fordert dies in Art. 27 und 28 nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen.

c) Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung (Art. 25). Diese besagt lediglich, dass gewisse Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen.

d) Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EuDSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell.

e) Auch der Ansatz des VE-DSG betreffend Profiling geht über die Bestimmungen der EuDSGVO und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der EuDSGVO noch der Konvention. Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren. Die Bedingung einer vorgängigen ausdrücklichen Einwilligung bei jeder Art von Profiling schiesst über das Ziel hinaus. Profiling soll nicht bereits bei dessen Erstellung schutzrelevant werden.

f) Überschiessende Informationspflichten (z.B. Art. 6 Abs. 2 oder Art. 13 Abs. 5 VE-DSG), die Geschäftsgeheimnisse betreffen können (gemäss Art. 6 Abs. 2 VE-DSG informiert der EDÖB über heikle Verfahren und Geschäftsgeheimnisse, ohne dass ein datenschutzrechtlicher Tatbestand dazu vorliegen müsste). Diese Pflicht ist dem EU Recht (inkl. E-SEV 108) fremd.

Wir lehnen Bestimmungen ab, die über das Mass der europäischen Regelungen hinausgehen. Es besteht keine Notwendigkeit für einen «Swiss Finish». Entsprechende Vorschläge sind ersatzlos zu streichen oder auf ein supranationales Mass zurückzunehmen.

2.2 Keine Doppelspurigkeiten bei der Aufsicht

Da viele Schweizer Unternehmen eine Tätigkeit in der Europäischen Union ausüben, werden diese auf der Grundlage von Art. 3 DSGVO i.V.m. Art. 55 Abs. 1 DSGVO auch der Aufsicht der nationalen Datenschutzbehörden unterstehen. Diese Doppelaufsicht bringt einerseits zahlreiche Rechtsunsicherheiten mit sich und andererseits verursacht sie eine massive administrative Zusatzbelastung der Schweizer Unternehmen. Es ist mit der Europäischen Union eine Gleichbehandlung auszuhandeln, damit die Schweizer Datenschutzaufsicht gegenseitig in das Konzept des „One-Stop-

Shop" nach Art. 56 DSGVO einbezogen werden kann. Heute steht diese für Unternehmen ausserhalb der EU nicht zur Verfügung.

3. Fehlende verfassungskonforme Regulierungskosten Folgeabschätzung (RFA)

Die Bundesverfassung verpflichtet in Art. 170 die Bundesversammlung, die Massnahmen des Bundes auf ihre Wirksamkeit zu prüfen („Die Bundesversammlung sorgt dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden."). Nach Art. 141 Abs. 2 Bst. f) ParlG müssen in der Botschaft an das Parlament eine Kosten-Nutzen Abschätzung sowie nach Bst. g) die Folgen für die Wirtschaft und die Gesellschaft erläutert werden.

Auf Seite 23 des Erläuterungsberichts zum VE-DSG werden die Regulierungskosten als unbedeutend eingestuft. **Diese Einschätzung ist falsch**. Alle Unternehmen bearbeiten heute in zunehmendem und komplexem Mass Personendaten bzw. Rohdaten für Persönlichkeitsprofile und sind damit von den Bestimmungen direkt betroffen. **Die Regulierungskosten sind für alle Unternehmen massiv höher als beschrieben!**

3.1 Mangelhafte Durchführung der Regulierungsfolgeabschätzung

Wir stellen die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG grundsätzlich in Frage. Die Unternehmensbefragung basiert auf einer völlig ungenügenden Nettostichprobe von lediglich 95 (!) Fragebogen, wovon keines der Unternehmen den Fragebogen vollständig beantwortet hat. Insbesondere wurden die spezifischen Daten zu den Folgen nur von wenigen Unternehmen beantwortet. Keines der angefragten Unternehmen machte bei einer Interviewerhebung mit.[1] Die Studienverfasser – immerhin eine renommierte Revisionsgesellschaft – erklären dazu ohne jeden Interpretationsspielraum selbst:

> „Die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten waren sowohl in Bezug auf Quantität als auch Qualität unzureichend; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands."[2]

> „Die Quantität und die Qualität des Rücklaufs aus der Unternehmensbefragung ermöglichte es nicht, in repräsentativer Weise eine Hochrechnung zur Schätzung der finanziellen Auswirkungen zu erstellen."[3]

Eine korrekte Aussage ist daher aufgrund dieser Angaben nicht möglich und es ist erstaunlich, dass das EJPD in ihrem Erläuterungsbericht zum Ergebnis kommt, die zu erwartenden Regulierungskostenfolgen seien unbedeutend. Im Bericht wird lediglich angegeben, dass die fehlenden statistischen Erhebungen durch Gespräche mit Fachpersonen ausgeglichen worden sind. Auch das ist falsch: Die angeblichen Gespräche sind ein dreistündiges Gespräch vom 4. Mai 2016 mit neun Fachpersonen, wo auch der Geschäftsführer von SUISSEDIGITAL anwesend war. Die anwesenden Vertreter haben bei der mündlichen Erörterung der Fragen wiederholt darauf hingewiesen, dass eine verbindliche Beurteilung der „statistischen" Ergebnisse aufgrund der unzureichen-

---

1 Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

2 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 8.

3 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

den Quantität und Qualität der Umfrageergebnisse absolut unmöglich sei. Wir finden die sehr kritischen Aussagen der angeblich befragten Fachpersonen im Bericht heute mit keinem Wort erwähnt. In der Studie wird lediglich vermerkt, dass diese Aussagen nicht repräsentativ sind.[4] Über den Verlauf der Sitzung vom 4. Mai 2016 wurde durch den Geschäftsführer von SUISSEDIGITAL ein internes Protokoll erstellt; dort ist auch die – für die desaströse Datenqualität – von einem Berater des Bundes vorgebrachte Begründung vermerkt, für die Untersuchung wären halt lediglich CHF 80'000.- Budget zur Verfügung gestellt worden.

Wir sind der Meinung, dass damit die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt wurde. Das ist für einen Vorentwurf von derartiger wirtschaftlicher Tragweite nicht akzeptabel und wir behalten uns diesbezüglich alle rechtlichen Massnahmen ausdrücklich vor, sollte dieser Umstand im Zuge der Abwicklung des weiteren Gesetzesprojekts keine Beachtung finden.

3.2 Methodisch fehlerhafte Durchführung der Regulierungsfolgeabschätzung

Die Einteilung der Unternehmen in drei Kategorien scheint völlig willkürlich und basiert nicht auf der tatsächlichen Betroffenheit. So werden zum Beispiel die Mehrheit der gewerblichen KMU-Betriebe (wie Metzgerei, Schreinerei, Papeterie, Spenglerei, Elektriker, lokale Transporteure, Baubetriebe, Bauernbetriebe, Velomechaniker, Coiffeur etc.) in das Segment A als Unternehmen mit geringer datenschutzrechtlicher Exponierung und keinem oder geringem Einsatz von Web-IT-Technologien eingeteilt.

Dabei wird verkannt, dass heute – und vor allem in Zukunft – jedes Unternehmen moderne Informatikmittel einsetzt, eine Internetseite und Social Media-Profile betreibt und damit Personendaten bearbeitet. Gerade kleine Unternehmen nutzen überdurchschnittlich viel cloudbasierte Internetapplikationen oder beziehen ihre gesamte Geschäftssoftware aus der Cloud. Als Beispiel deinen Cloud-Angebote wie „Microsoft 365" für kleinere und mittlere Unternehmen mit einer Datenspeicherung im Ausland, u.a. auch in den USA. Damit müssen diese 335'000 (55.1%) Unternehmen korrekterweise dem Segment B als Unternehmen mit mittlerer bis grosser datenschutzrechtlicher Exponierung (innerhalb der Schweiz und weltweit tätige Unternehmen und/oder Einsatz von Web-IT-Technologien wie Webseiten für Marketing oder Nutzung von Cloud Services) zugeordnet werden.[5]

3.3 Falsche Angaben zur Regulierungsfolgeabschätzung im VE-DSG

Die Folgekosten für die Wirtschaft werden überhaupt nicht quantifiziert. Vielmehr wird behauptet:

> „Die Analyseergebnisse zeigen, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen generell nur geringfügig betroffen sind. Die Auswirkungen der Revision auf dieses Segment sind somit verhältnismässig gering. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im VE vorgesehenen Massnahmen stärker betroffen als Grossunternehmen, da

[4] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 25.

[5] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 5.

> sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei."[6]

Nur schon durch das Zusammenziehen der in der Studie vorhandenen – ungenügenden – Schätzungen, wird der massive Umsetzungsaufwand sichtbar, entsprechend unerklärlich es ist, dass dies im Erläuterungsbericht mit keinem Wort erwähnt wird:[7]

Handlungspflichten nach VE-DSG	**Einmalig**	**Wiederkehrend**	**Kosten CHF**
Informationspflichten			
Pflicht zur Information der betroffenen Person	60 – 100 Stunden	30 Stunden	3000 – 40'000
Auskunft über Aufbau der Datenbearbeitung	4- 12 Stunden	1.6 h – 3 Tage pro Fall	Keine Angabe
Informationspflicht Automatisierte Entscheidungen	30 – 50 Stunden	3 Stunden pro Fall	10'000
Meldung Data Breach	5 – 20 Stunden	2 – 5 Stunden pro Fall	5'000 – 10'000
Datenherrschaft			
Mitteilung, Löschung, Beschränkung	14 – 20 Stunden	3 Stunden pro Fall	100 – 5'000
Pflichten auf Datenübertragbarkeit	12 Stunden	2 Stunden pro Fall	7'500
Unternehmensinterne Datenschutzorganisation			
Datenschutz-Folgeabschätzung[8]		20 – 160 h pro Fall	5'000 – 30'000
Privacy by Default	1 – 40 Stunden		500 – 5'000
Betriebliche Datenschutzbeauftragter		500 – 2'000 h pro Jahr	
Grenzüberschreitender Datenverkehr			
Genehmigung Standard Datentransfervereinbarung	50 Stunden		5'000

Auch wenn man nur die Aufgaben einbezieht, die alle Unternehmen beachten müssen, und als Basis Minimalschätzungen als Grundlage für eine Hochrechnung annimmt, ergeben sich Umsetzungskosten für die Schweizer Wirtschaft von über CHF 1'532'160'000, resp. im Durchschnitt von CHF 2'520 pro Unternehmen.[9] In der Praxis dürften diese noch wesentlich höher liegen.

Es muss heute nämlich davon ausgegangen werden, dass alle Unternehmen von diesen vorgeschlagenen Bestimmungen betroffen sind, insbesondere da auch alle ohne jede *de minimis*-Schwelle den exzessiven Strafbestimmungen unterliegen. Selbst die Studienverfasser gehen von einer vergleichsweise hohen Belastung der Unternehmen aus:

> „Gleichsam haben mehrere Fachpersonen im Rahmen der Fachgespräche vorgebracht, dass bei gleicher Datenbearbeitungstätigkeit KMU stärker von der Revision oder generell von den datenschutz-rechtlichen Verpflichtungen betroffen sind als grosse Unternehmen, da ihnen die notwendige Compliance-Infrastruktur fehle resp. sie im Verhältnis teurer sei. In Bezug auf die

---

6 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetze und Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 23.

7 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 27 ff.

8 In einer Studie der Europäischen Union zur Datenschutz-Folgeabschätzung (Privat Impact Analysis) wurden die Kosten pro Durchführung auf € 14'000 – 149'000 geschätzt. Quelle: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, Seite 70.

9 608'000 Unternehmen mit einem Aufwand von 84 Stunden zu einem Stundenkostensatz von CHF 30.

> Unternehmen der Segmente B und C ist demgegenüber von einer vergleichsweise hohen Belastung durch die Revision des Datenschutzgesetzes auszugehen."[10]

Aufgrund der methodischen Fehlbeurteilung wird in Verbindung mit der ungenügenden Datenerhebung bei den Unternehmen sichtbar, dass einerseits die Regulierungsfolgenabschätzung nicht korrekt durchgeführt wurde und andererseits die Regulierung für die gesamte Wirtschaft massiv höhere Kosten zur Folge hat.

Bislang wurde die korrekte Durchführung eines Vernehmlassungsverfahrens oder sogar die Vorlage einer Botschaft an das Parlament ohne solche Regulierungskostenfolgenabschätzung nie durch die Judikative überprüft. Wir und mit uns die gesamte Schweizer KMU-Wirtschaft müssen darauf vertrauen, dass dieses Manko vor einer Parlamentsvorlage unbedingt und professionell korrigiert wird. Andernfalls muss diese Korrektur spätestens vom Parlament bzw. den entsprechenden Rechtskommissionen vorgenommen werden. Sollte diese nicht gelingen, würden die neuen Regulierungen spätestens beim Vollzug einer auf den VE-DSG gestützten Verordnung über die akzessorische Normenkontrolle Fälle für Gerichte.

B. Forderungen

Wir stellen weiter folgende Forderungen grundsätzlicher Natur an das revidierte Datenschutzgesetz:

a) Eine klare Regelung der Einwilligung und eine gesetzliche Vermutung der Einwilligung bei definierten Vorgängen, wie zum Beispiel einem Vertragsverhältnis würden den Unternehmen wesentlich mehr Rechtssicherheit und weniger administrativen Aufwand bringen. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten.

b) Auf die unüberschaubare Menge von Informations- und Dokumentationspflichten der Unternehmen sowie der rein administrativen Meldungen an den Beauftragten ist grundsätzlich zu verzichten. Hingegen sollten Unternehmen vom Beauftragten innerhalb von 30 Tagen eine verbindliche Beurteilung einer Datenbearbeitung verlangen können (Negativattest, *Comfort Letter* oder dergleichen).

c) Auf eine Ausweitung des Strafenkatalogs ist zu verzichten. Insbesondere sind nur materielle Datenschutzverletzungen zu sanktionieren und keinesfalls Verletzungen von Dokumentations- oder Meldepflichten an den Beauftragten. Es bestehen heute genügend Möglichkeiten bei tatsächlichen Verstössen, Sanktionen gegen fehlbare Unternehmen zu verhängen. Der Verweis auf das Persönlichkeitsrecht für Ansprüche von betroffenen Personen hat sich ebenfalls bewährt und muss nicht geändert werden.

C. Stellungnahme zu den einzelnen Artikeln

Im Übrigen finden Sie unsere Anträge und Bemerkungen zu den einzelnen Artikeln wie verlangt in der nachfolgenden tabellarischen Übersicht:

---

[10] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 53.

VE-DSG	Anträge und Bemerkungen
1. Abschnitt: Zweck, Geltungsbereich und Begriffe	
Art. 1 Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.	**Antrag zu Art. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. Wenn nicht im Gesetzestext (Art. 1 oder Art. 2 Abs. 1 VE-DSG) selbst, so ist diese Klarstellung spätestens in der Botschaft unmissverständlich anzubringen.
Art. 2 Geltungsbereich [1] Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen durch: a. private Personen; b. Bundesorgane. [2] Es ist nicht anwendbar auf: a. Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden; b. Personendaten, die durch die Eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden; c. Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden; d. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007, die in der Schweiz Immunität geniessen, wie das Internationale Komitee vom Roten Kreuz. [3] Dieses Gesetz ist nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Für die Bearbeitung der übrigen Daten sind sie von	**Antrag zu Art. 2 Abs. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. **Antrag zu Art. 2 Abs. 2 lit. c)**: Beibehaltung des geltenden Wortlauts. Der VE will neu nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung nicht mehr gelten. Das ist weder sachgerecht, noch nachvollziehbar, und führt zu schwerwiegenden Konsequenzen im Zusammenhang mit der Führung von Gerichtsverfahren (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).

VE-DSG	Anträge und Bemerkungen
der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ausgenommen. [4] Die Bundesversammlung und der Bundesrat sind von der Aufsicht durch den Beauftragten ausgenommen.	**Antrag zu Art. 2 Abs. 5 (neu)**: Der im Erläuterungsbericht erwähnte Allgemeincharakter des VE (*Lex Generalis*) ist in einem neuen Abs. 5 ausdrücklich vorzusehen. Es ist festzustellen, dass datenschutz- bzw. datenbearbeitungsrelevante Regelungen in kantonalen und anderen Erlassen des Bundes dem allgemeinen DSG vorgehen (*Lex Specialis*). Damit können entsprechende Einzelhinweise im VE gestrichen werden. Solche Einzelerwähnungen sind nicht sinnvoll und gefährlich, weil diese das im Erläuterungsbericht erwähnte, selbstverständliche Wirkungsprinzip „*Lex Specialis derogat Lex Generalis*" grundsätzlich in Frage stellen. Diese generelle Klarstellung ist aber vor allem deshalb wichtig, weil das Prinzip beim Anspruch auf Information über bearbeitet Personendaten schon nach geltendem Recht immer wieder in Frage gestellt worden (Beispiel: Ein Teil der allgemeinen Datenschutz-Lehre meint unzutreffend, dass Art. 8 DSG auch im Bereich von fernmelderechtlich geschützten Personendaten anwendbar bleibt, ergo die spezifischen fernmelderechtlichen Datenschutzbestimmungen in Art. 43 bis 46 FMG und 9. Kapitel „Fernmeldegeheimnis und Datenschutz", Art. 80 ff. FDV, den Datenschutz bei der Datenherausgabe im Zusammenhang mit der Erbringung von Fernmeldediensten nicht als „Lex Specialis" abschliessend regelt.)
2. Abschnitt: Allgemeine Datenschutzbestimmungen	
Art. 3 Begriffe Die folgenden Ausdrücke bedeuten: a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; b. *betroffene Person:* natürliche Person, über die Daten bearbeitet werden; c. *besonders schützenswerte Personendaten:* 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,	**Antrag zu Art. 3 lit. c Ziff. 4**: Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Der im Erläuterungsbericht enthaltene Hinweis, wann auch Fotos als biometrische Personendaten gelten, ist unverständlich. Es ist klarzustellen, wann Fotos als Personendaten gelten; dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biometrische Daten gelten.

VE-DSG	Anträge und Bemerkungen
5. Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe; d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten; e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten; f. *Profiling:* jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;	**Bemerkung zu Art. 3 lit. c Ziff. 5**: Die Bestimmung ist in dieser allgemeinen Form problematisch; etwa wenn Vermögensdelikte zur Diskussion stehen, von welchen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste. **Antrag zu Art. 3 lit. f)**: Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes „Daten". Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um „Personendaten". Andere Daten werden gemäss Erläuterungsbericht durch den Begriff „Personendaten" konsumiert. Der Begriff des „Profiling" ist zu unbestimmt und gefährdet damit die Rechtssicherheit mit nicht ermittelbaren Kostenfolgen für die gesamtschweizerische Wirtschaft. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem „Persönlichkeitsprofil" des geltenden Rechts abzulehnen. **Generelle Bemerkung zu Art. 3 lit. f)**: Die nicht reflektierte Übernahme von Begriffen des ausländischen Rechts führt dazu, dass sich die Anwendung und Auslegung von Schweizer Recht zukünftig primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und hier vor allem deshalb nicht sachgerecht. weil der Begriff des „Profiling" gegenüber dem EU-Recht sogar nicht mit einem „Swiss Finish" versehen und inhaltlich ausgeweitet wird. Die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich schädlich, die Bearbeitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als „Voraussage" eines späteren Verhaltens interpretiert werden könnten. Die Revision schiesst hier

VE-DSG	Anträge und Bemerkungen
	weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen, ohne alle erheblichen Verpflichtungen einzuhalten, die der VE mit dem „Profiling" verknüpft. Es gäbe zahlreiche Beispiele von sicherlich nicht beabsichtigten und unbedachten Konsequenzen in längst etablierten und von Konsumenten akzeptierten digitalisierten Wirtschaftsprozessen: Man denke nur an die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind. So etwas Selbstverständliches würde plötzlich problematisch.
g. *Bundesorgan:* Behörde und Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist; h. *Verantwortlicher*: Bundesorgan oder private Person, das oder die – alleine oder zusammen mit anderen – über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet;	**Antrag zu Art. 3 lit. h und i**: Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), *eventualiter* zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu einer unklaren – teilweise unsinnigen – Aufteilung der Verantwortung und zu Doppelspurigkeiten. Zudem wird übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen *kann*. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für wen?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den Verantwortlichen?) geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den Verantwortlichen?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht, ergo auch hier nicht einmal das Generalargumente der Bundesverwaltung zieht, man müsse etwas so regeln, weil es ausländisches Recht so vorgebe und man andernfalls auf eine „Blacklist" gesetzt werde. Dass „Arbeitnehmer mit einem Arbeitsvertrag" (gibt es auch Arbeitnehmer ohne Arbeitsvertrag?) nicht unter den Begriff des "Auftragsbearbeiters" fallen, steht zwar im Erläuterungsbericht. In Anbetracht der merkwürdigen Formulierung „Arbeitnehmer mit Arbeitsvertrag" wäre es aber dringend nötig, dies klar und deutlich im Gesetzestext zu normieren (Simpler Vorschlag: „Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter").
i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	

VE-DSG	Anträge und Bemerkungen
Art. 4 Grundsätze [1] Personendaten müssen rechtmässig bearbeitet werden. [2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.	**Antrag zu Art. 4 Abs. 2**: In Absatz 2 ist zu ergänzen, dass nicht nur die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und verhältnismässig zu sein hat, sondern auch die Ausübung anderer Rechte und Pflichten gemäss diesem Gesetz.
[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.	**Antrag I zu Art. 4 Abs. 3**: Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Der Erläuterungsbericht argumentiert, es sei mit der redaktionellen keine materielle Änderung beabsichtigt (das steht im Übrigen – beschwichtigend – an zahlreichen anderen Stellen des Erläuterungsberichts). Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann in der Praxis eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. **Antrag II zu Art. 4 Abs. 3**: Im Erläuterungsbericht wird beim Beispielkatalog von nicht erkennbaren Datenbearbeitungen die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch Privatunternehmen erwähnt. Es wird dazu auf den sog. Logistep-Entscheid (BGE 136 II 508 E.4) verwiesen. Dieser Verweis und dieses Beispiel ist deplatziert, zumal das Bundesgericht in diesem Entscheid ausdrücklich festgehalten hat, seine Begründung beziehe sich auf geltendes Recht, welches durch den Gesetzgeber im Lichte der mit der Sammlung solcher IP-Adressen zusammenhängenden vertretbaren Absicht allenfalls zu korrigieren sei. Es ist unverständlich, weshalb nun gerade dieses Beispiel als „Nicht-Erkennbarkeit einer Bearbeitung von Personendaten" aufgeführt ist. Vielmehr wäre gerade vorzusehen, dass die Beschaffung von IP-Adressen zum Zwecke der Strafverfolgung von diesem Grundsatz ausdrücklich nicht erfasst wird.
[4] Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.	**Antrag zu Art. 4 Abs. 4**: Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.
[5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten.	**Antrag zu Art. 4 Abs. 5**: Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Erläuterungsberichts sind auch hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten. *Eventualiter* ist Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind" zu beschränken (Streichung des Rests). Bekanntlich fängt die "Bearbeitung" schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE).
[6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von	

VE-DSG	Anträge und Bemerkungen
besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.	Eine fortdauernde Verpflichtung zur Nachführung ist nicht erfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Selbst wenn so etwas möglich wäre, ist dieses Konzept nicht finanzierbar. **Antrag zu Art. 4 Abs. 6**: Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f) vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (vgl. dazu auch die Bemerkungen zu Art. 3 lit. f VE). Die im Erläuterungsbericht vertretene Ansicht, mit der vorgeschlagenen Redaktion von Abs. 6 möge die in der Lehre ausgetragene Kontroverse über die „Ausdrücklichkeit" einer Einwilligung beendet sein, ist die blosse Äusserung einer Hoffnung. Das Gegenteil wird der Fall sein und die Kontroverse verstärkt werden: Es lassen sich über die Begriffe „freiwillig", „freiwillig und eindeutig", „ausdrücklich" und die Abgrenzung zur blossen „Einwilligung" (vgl. z.B. Art. 6 Abs. 1 lit. a VE) vorzügliche juristische Publikationen schreiben.
Art. 5 Bekanntgabe ins Ausland [1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. [2] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz gewährleistet. [3] Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch: a. einen völkerrechtlichen Vertrag; b. spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde; c. standardisierte Garantien, insbesondere durch Vertrag: 1. welche der Beauftragte vorgängig genehmigt hat, oder 2. welche der Beauftragte ausgestellt oder anerkannt hat; d. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig genehmigt wurden: 1. durch den Beauftragten, oder 2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet. [4] Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 Buchstabe b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien informieren. [5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c	**Antrag zu Art. 5 Abs. 3 lit. d)**: Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG. **Antrag zu Art. 5 Abs. 4 bis 6**: Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt – wie aus dem Wort ersichtlich – nach den Weisungen des Verantwortlichen, dem – wiederum entsprechend seiner Bezeichnung – die Verantwortung für die Information des Beauftragten obliegt.

VE-DSG	Anträge und Bemerkungen
Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht. [6] Der Verantwortliche oder der Auftragsbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit. [7] Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.	**Antrag zu Art. 5 Abs. 7**: Es ist zu ergänzen, dass der Bundesrat die Liste quartalsweise aktualisieren muss und dazu ein ständiges Staaten-Monitoring etabliert. Heute ist die Liste von Staaten mit der Gewährleistung von angemessenem Schutz des EDÖB gut etabliert und ausreichend dynamisch. Wenn nun die Kompetenz zum Bundesrat hinaufgereicht wird, ist sicherzustellen, dass der Bundesrat diese sehr operative Rolle auch bedarfsgerecht wahrnehmen muss.
Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: a. die betroffene Person im Einzelfall eingewilligt hat; b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt; c. die Bekanntgabe im Einzelfall unerlässlich ist für: 1. die Wahrung eines überwiegenden öffentlichen Interesses, oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde; d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; e. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; f. die Daten aus einem gesetzlich vorgesehenen Register stammen, das zugänglich ist für die Öffentlichkeit oder für Personen mit einem schutzwürdigen Interesse, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. [2] Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.	**Antrag zu Art. 6 Abs. 1 lit. a)**: Es ist zu präzisieren, wie sich die hier ohne die Zusätze „freiwillig", „eindeutig" oder „ausdrücklich" auskommende Einwilligung gestalten lässt. **Antrag zu Art. 6 Abs. 2**: Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1 lit. b, c oder d ins Ausland bekanntgegeben wird. Das gilt erst recht, wenn neben dem Verantwortlichen auch noch der Auftragsbearbeiter verpflichtet werden soll. Es ist mit dieser Doppelnennung nicht klar, wer am Ende für die Erfüllung der Meldepflicht verantwortlich ist. Die Folge davon

VE-DSG	Anträge und Bemerkungen
	wird sein, dass sowohl der Verantwortliche, als auch der Auftragsbearbeiter Meldung erstatten müssen, um sich nicht einer Strafverfolgung auszusetzen. Die Bestimmung ist weiter auch deshalb heikel, weil solche Meldungen z.T. sensible Geschäftsinformationen betreffen (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetzen auch für Dritte einsehbar werden. Auch hier wurde offenbar in keiner Weise an den berechtigten Schutz von Geschäftsgeheimnissen gedacht.
Art. 7 Auftragsdatenbearbeitung [1] Die Bearbeitung von Personendaten kann durch Vereinbarung oder Gesetz einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. [2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters. [3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. [4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.	s **Antrag zu Art. 7 Abs. 2**: Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Die Pflichten des Auftragsbearbeiters ergeben sich aus den Pflichten des Verantwortlichen und des zwischen diesem und dem Auftragsbearbeiter abgeschlossenen Vertrags. **Antrag zu Art. 7 Abs. 3**: Schaffung der Möglichkeit einer generellen Einwilligung.
Art. 8 Empfehlungen der guten Praxis [1] Der Beauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen. [2] Der Verantwortliche sowie interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie. [3] Er veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.	**Antrag zu Art. 8**: Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der von diesem vordefinierten "interessierten Kreise" – erfahrungsgemäss ist die Zusammenstellung von solchen *Round Tables* „interessierter Kreise" völlig willkürlich und intransparent – ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. Es ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen *tel quel* als Ermessensindikator zugrunde legen werden. Der Beauftragte wird damit im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich faktisch gemäss seinen Eindrücken Recht setzen. Dies wiegt umso schwerer, als der Beauftragte nicht einmal Jurist oder Anwalt sein oder über Erfahrungen in der Unternehmensjurisprudenz verfügen muss.
Art. 9 Einhaltung der Empfehlungen der guten Praxis [1] Befolgt der Verantwortliche die Empfehlungen der guten Praxis, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren. [2] Die Datenschutzvorschriften können auch auf andere Weise eingehalten werden, als in Empfehlungen der guten Praxis vorgesehen.	**Antrag zu Art. 9**: Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zu Lasten des Datenbearbeiters führen.

VE-DSG	Anträge und Bemerkungen
Art. 10 Zertifizierung [1] Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen. [2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.	Keine Bemerkungen
Art. 11 Sicherheit von Personendaten [1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden. [2] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.	Keine Bemerkungen
Art. 12 Daten einer verstorbenen Person [1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und: a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder b. keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen. [2] Ein schutzwürdiges Interesse wird bei Personen vermutet, die mit der verstorbenen Person in gerader Linie verwandt sind oder mit ihr bis zum Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten. [3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.	**Antrag I zu Art. 12**: Die Bestimmung ist aus dem VE zu entfernen und die Thematik in die aktuell laufende Revision des Erbrechts zu integrieren. Derart weitreichende, thematisch in einem allgemeinen Datenschutzgesetz nicht zu erwartende Regularien als Folge des Todes gehören dorthin, wo der Tod und dessen Folgen abgewickelt werden. Das ist das allgemeine Erbrecht. Die dort zu erlassenden datenschutzrechtlichen Bestimmungen sind *lex specialis* zum DSG. Weiter ist die gesamte Bestimmung voll von schwerwiegenden Unklarheiten: Wer urteilt über das Vorliegen überwiegender Interessen der verstorbenen Person? Wer über die überwiegenden Interessen Dritter? Wie verhält sich das schutzwürdige Interesse zum überwiegenden Interesse Dritter? Weiter ist die Verknüpfung des schutzwürdigen Interesses mit Verwandtschaftsgraden unbegründet und willkürlich. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären. Es gäbe unzählige weitere Beispiele. Art. 4 Abs. 1 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen. **Antrag II zu Art. 12 Abs. 3**: Die Bestimmung ist gerade umzukehren. Sie ist abzuändern, dass im Zusammenhang mit dem Vollzug dieser Bestimmung Amts- und Berufsgeheimnisse von Geheimnisträgern jederzeit geltend gemacht werden können. Alles andere wäre absurd: Es gäbe zahlreiche Beispiele, die dramatische Konsequenzen zur Folge hätten. Man denke nur an den Fall, in

VE-DSG	Anträge und Bemerkungen
	welchem ein Mitglied einer zerstrittenen Erbengemeinschaft den Vertrauensanwalt des Verstorbenen nötigen würde, ihm Einsicht in die Personendaten zu geben, die er dann auch noch auf Geheiss vernichten müsste.
[4] Jeder Erbe kann verlangen, dass der Verantwortliche Personendaten des Erblassers kostenlos löscht oder vernichtet, ausser: a. der Erblasser hat dies zu Lebzeiten ausdrücklich untersagt; oder b. der Löschung oder Vernichtung stehen überwiegende Interessen des Erblassers oder von Dritten entgegen.	**Antrag zu Art. 12 Abs. 4**: Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und Löschungsrecht völlig ausreichen.
[5] Vorbehalten bleiben spezielle Bestimmungen anderer Bundesgesetze.	**Bemerkung zu Art. 12 Abs. 5**: Es ist bezeichnend, dass genau bei dieser Bestimmung noch einmal explizit betont wird, was gemäss Art. 2 VE ohnehin generell gilt. Diese Bestimmung steht mit zahlreichen spezialgesetzlichen Regelungen komplett im Widerspruch. Insofern ist der Sinn einer solchen allgemeinen Datenschutzklausel im Zusammenhang mit Verstorbenen nicht ersichtlich.
3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters	**Vorbemerkungen**: - Es fehlt an Übergangsbestimmungen, welche regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar und führt über Jahre hinweg zu grossen Unsicherheiten in der Praxis. - Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention – und nicht die DSGVO – den Massstab für die Angemessenheit des Datenschutzes zu liefern haben.
Art. 13 Informationspflicht bei der Beschaffung von Personendaten [1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. [2] Er teilt der betroffenen Person spätestens bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten; c. den Zweck der Bearbeitung.	**Antrag zu Art. 13 Abs. 1 und 2:** Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird zwar festgehalten, es genüge eine solche "allgemeine Information". Das ist allerdings im Wortlaut der Bestimmung nicht ersichtlich. In der vorliegenden Form ist die Bestimmung nicht praktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle informieren, deren Daten sie bearbeiten. In der Telekommunikationsbranche ist dies selbst mit solchen Massenschreiben nicht möglich, weil regelmässig Personendaten bearbeitet werden, mit welchen ein Dienstanbieter nie in einem direkten Kontakt

VE-DSG	Anträge und Bemerkungen
	steht. Die Bestimmung ist schlicht nicht umsetzbar und schiesst über das Ziel hinaus: Selbst die insgesamt absolut ungenügende Analyse der Regulierungskostenfolgeabschätzung von PWC hält dies so fest.
[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.	**Antrag zu Art. 13 Abs. 3** Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist nicht akzeptierbar. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, in welchen persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger jeder Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen.
[4] Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die er bearbeitet, mit.	**Antrag zu Art. 13 Abs. 4**: Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
[5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden; werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.	**Antrag zu Art. 13 Abs. 5**: Ersatzlos streichen. *Eventualiter* ist die aktive Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten zu beschränken. Die vorgesehene uferlose Informationspflicht ist schlicht nicht umsetzbar und – selbst wenn diese umsetzbar wäre – völlig unverhältnismässig. Hinzu kommt, dass die Bestimmung sogar noch weiter geht als die DSGVO, die immerhin noch einen Monat Frist gewährt. Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird. Weiter muss man sich bei diesem Konzept auch die Auswirkungen auf Konsumentenseite vor Augen führen: Da in Zukunft praktisch kein Wirtschaftszweig mehr ohne die Beschaffung und Bearbeitung von Personendaten auskommen wird, wird der Konsument mit solchen Informationen regelrecht zugespamt werden. Die einzelne Information versinkt im Informationsmeer. Der Adressat wird abgestumpft und negiert die diesem Informationswahn zu Grunde gelegten Absichten, den Adressaten vor „bösen" Datenbearbeitern zu schützen.
Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen [1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt.	**Bemerkung**: Wurde unnötigerweise enger als die SEV 108 gefasst. **Antrag zu Art. 14 Abs. 1:** Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung),

VE-DSG	Anträge und Bemerkungen
[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn: a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.	in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist. **Antrag zu Art. 14 Abs. 2**: 1. Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der VE für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
[3] Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn: a. ein Gesetz im formellen Sinn dies vorsieht; oder b. dies aufgrund überwiegender Interessen Dritter erforderlich ist.	
[4] Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten: a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt; b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls eine der folgenden Voraussetzungen erfüllt ist: 1. es ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich; oder 2. die Übermittlung der Information stellt den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage.	**Antrag zu Art. 14 Abs. 4 lit. a**: Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns (der als Dritter gilt) unnötig erschwert.
II. [5] Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	
Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung [1] Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.	**Antrag zu Art. 15 Abs. 1**: Streichen. *Eventualiter* ist die Bestimmung um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a DSGVO EU (2016/679) zu ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als untauglicher Versuch, Konsumenten vor jeder Art automatisiert getroffener Entscheidungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche" Auswirkung ist, dürfte letztlich von der Sensibilität des Be-

VE-DSG	Anträge und Bemerkungen
	troffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte. Die saloppe Begründung im Erläuterungsbericht „denn solche Entscheidungen sind in allen Wirtschaftsbereichen immer häufiger und werden teilweise auf der Grundlage falscher Daten getroffen" reicht jedenfalls nicht aus, einer solchen weitreichenden Bestimmung ein öffentliches Interesse mitzugeben. Art. 22 DSGVO nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor. Eine von der DSGVO abweichende Regelung wäre demnach zweifellos auch für die Schweiz zulässig. Es ist nicht nachvollziehbar, weshalb hier ein „Swiss Finish" erfolgt. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung seit der Gründung des Bundesstaates frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Das hat nichts damit zu tun, ob die Grundlage für einen solchen Entscheid aus Papier, aus Menschen oder aus Algorithmen stammt.
[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.	**Antrag zu Art. 15 Abs. 2**: Streichen. Wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand für die gesamte Schweizer Wirtschaft. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens.
[3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.	**Antrag zu Art. 15 Abs. 3**: Streichen. Es ist nicht nachvollziehbar, weshalb gerade der Staat automatisierte Entscheidungen ohne Informations- und Anhörungspflicht durchführen darf. Das Handeln des Staates ist an die Einhaltung von Grundrechten geknüpft. Diese Bestimmung zeugt von einem sehr gefährlichen Grundverständnis der Gesetzesredaktoren: Hier der gute Staat, dort die böse Wirtschaft. Es ist daran zu erinnern, dass solche Ausnahmen für staatliches Handeln vor allem Mittel totalitärer Staaten sind, sich für nichts rechtfertigen zu müssen.
Art. 16 Datenschutz-Folgenabschätzung [1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen. [2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern.	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschätzungen bei jeder beliebigen Datenbearbeitung vornehmen zu müssen; abgesehen davon muss die Abschätzung ohnehin durchgeführt werden, um herauszufinden, ob die Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit führt. Die Kosten sind angefallen, selbst wenn man zum Schluss käme, dass gar keine Risiken bestehen. Hier wird ein bürokratisches Monstrum freigesetzt,

VE-DSG	Anträge und Bemerkungen
[3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen. [4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit.	das in der Privatwirtschaft im Ergebnis nichts ausser gigantischen Kosten bringen wird. Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier, Zeit und Geld dafür aufwenden müssen. Denn anders als der Bund, der – wie im vorliegenden Fall – meint, mit wenig Geld eine verfassungskonforme Regulierungskostenfolgenabschätzung machen zu können, hat der private Datenbearbeiter mit seiner Existenz gerade zu stehen, wenn er einer solchen Verpflichtung nicht im Sinne des Gesetzes nachkommen sollte. **Antrag zu Art. 16 Abs. 3 und 4**: Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist ist weiter viel zu lang und zeugt nicht von einem Verständnis wirtschaftlicher Prozesse. Wenn es bei solchen Folgeabschätzungen Beanstandungen gibt, dann hat der Beauftragte Einwände innert 7 Tagen zu adressieren, ansonsten Geschäftsprozesse während Monaten blockiert bleiben müssen. Wir weisen dazu auch darauf hin, dass allein die Überprüfung der zu erwartenden Schwemme solcher Meldungen, ein Herr von neuen Beamten erforderlich machen wird, die nichts anderes tun, als solche Folgeabschätzungen zu prüfen.
Art. 17 Meldung von Verletzungen des Datenschutzes [1] Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.	**Antrag zu Art. 17**: Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien unseres Rechtsstaates. Es ist nicht zu rechtfertigen, dass diese Garantie gerade im Datenschutzrecht nicht mehr gewährleistet werden soll; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer Flut von Selbstanzeigen zu rechnen, die erneut nur den Apparat des Beauftragten übermässig aufblähen würde. Diese aus den USA bekannten Regulierungsmechanismen sollten in der Schweiz nicht angefasst werden. Der Druck auf die Verantwortlichen wäre enorm und würde ein pragmatisches und/oder vernunftgetriebenes Handeln von vornherein ausschliessen. Die Selbstanzeige ist in einem solchen System immer die sicherste Art, sich prophylaktisch „compliant" zu verhalten.

VE-DSG	Anträge und Bemerkungen
[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. [3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. [4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung.	**Antrag zu Art. 17 Abs. 2**: Streichung; In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen. **Bemerkung zu Art. 17 Abs. 4**: Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen [1] Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. [2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.	**Antrag zu Art. 18**: Streichung. Die Bestimmung ist redundant. Der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Art. 19 Weitere Pflichten Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie dokumentieren ihre Datenbearbeitung; b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.	**Antrag zu Art. 19**: Streichung; Die Bestimmung ist nicht nur überflüssig, sondern teilweise nicht umsetzbar. Die stipulierte Dokumentationspflicht würde insbesondere für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b ist von vornherein nicht umsetzbar. Teilweise lassen sich dagegen auch absurde Beispiele vorbringen: Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine allfällige Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gemäss Art. 25 machen zu müssen. Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Auch hier gilt es, sich auch in die Situation der Informationsadressaten zu versetzen. Dass Millionen unnützer Mitteilungen versandt werden ist das eine; dass aber jeder Einzelne tausende solcher Informationen von allen Datenbearbeitern erhält, das andere. Diese Informationen sind die neuen „Spam Waves" und werden bei den Adressaten keinerlei Wirkung erzielen, geschweige denn, diese in ihren Persönlichkeiten schützen.
4. Abschnitt: Rechte der betroffenen Person	
Art. 20 Auskunftsrecht	

VE-DSG	Anträge und Bemerkungen
[1] Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. [2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten; c. der Zweck der Bearbeitung; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; e. das Vorliegen einer automatisierten Einzelentscheidung;	**Antrag zu Art. 20 Abs. 2 lit e)**: Streichen; in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich(vgl. auch den Antrag zu Art. 15).
f. die verfügbaren Angaben über die Herkunft der Personendaten;	**Antrag zu Art. 20 Abs. 2 lit. f)**: Streichen; die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntgeben zu müssen, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen.
g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4.	
[3] Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.	**Antrag zu Art. 20 Abs. 3**: Streichen; *eventualiter* ist Abs. 3 auf die Pflicht zu beschränken, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt: Entweder wird ein Vertrag geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, eine Begründungspflicht für den Nicht-Abschluss von Verträgen über das Datenschutzrecht einzuführen. Das kann nicht das Ziel des Datenschutzes sein. Die Verweigerung von Geschäftsbeziehungen ist ausschliesslich ein wettbewerbs- und lauterkeitsrechtlicher Tatbestand. Es ist lebensfremd, wenn man heute meint, allein durch eine modernere Datenbearbeitung würden Fehler bei der Einschätzung von geschäftlichen Tätigkeiten verursacht. Die Frage, ob zwei Personen miteinander kontrahieren, basierte seit jeher auf der Einschätzung von „Personendaten“ und „Persönlichkeitsprofilen“. Es kam bislang niemand auf die Idee, im allgemeinen oder im besonderen Teil des OR eine Begründungspflicht für den Nicht-Abschluss eines Vertrages zu fordern. Vielfach wird gerade deshalb kein Vertrag geschlossen, weil die persönliche Chemie nicht stimmt. In den seltenen Fällen wird dies der anderen Seite so direkt mitgeteilt. Wieso es weiter für den Schutz der Persönlichkeit erforderlich sein soll, dem Betroffenen die Auswirkungen eines Nicht-Entscheids zu erläutern, ist völlig unerfindlich, wenn

VE-DSG	Anträge und Bemerkungen
[4] Personendaten über die Gesundheit können der betroffenen Person durch einen von ihr bezeichneten Arzt mitgeteilt werden. [5] Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat. [6] Niemand kann im Voraus auf das Auskunftsrecht verzichten.	nicht gleichzeitig eine Rechtsmittelmöglichkeit besteht, die am Ende in einen Vertragszwang münden könnte. Beides wird zum Glück und konsequenterweise (jedoch im Kontext aller anderen Ideen fast schon überraschend) nicht gefordert.
Art. 21 Einschränkung des Auskunftsrechts [1] Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. [2] Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.	Keine Bemerkungen
Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende [1] Werden Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben: a. Die Daten geben Aufschluss über die Informationsquellen; b. Es müsste dafür Einsicht in Entwürfe für Publikationen gewährt werden; c. Die freie Meinungsbildung des Publikums würde gefährdet. [2] Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.	Keine Bemerkungen
5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen	
Art. 23 Persönlichkeitsverletzungen [1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. [2] Eine Persönlichkeitsverletzung liegt insbesondere vor: a. wenn Personendaten entgegen den Grundsätzen nach den Artikeln 4-6 und 11 bearbeitet werden; b. wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden; c. wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden; d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.	**Antrag zu Art. 23 Abs. 2 lit d)**: Streichung; zum Profiling vgl. Bemerkungen zu Art. 3 lit. f VE.

VE-DSG	Anträge und Bemerkungen
[3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	**Bemerkung zu Art. 23 Abs. 3**: Streichung des zweiten Teils „und eine Bearbeitung nicht ausdrücklich untersagt hat". Was einmal allgemein zugänglich gemacht worden ist, kann später nicht mehr widerrufen werden.
Art. 24 Rechtfertigungsgründe [1] Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. [2] Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere: a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet; b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben; c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn: 1. es sich dabei nicht um besonders schützenswerte Personendaten handelt, 2. Dritten nur Daten bekanntgegeben werden, welche diese für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen, 3. die betroffene Person volljährig ist; d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet; e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet, soweit: 1. die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt, 2. Dritten besonders schützenswerte Personendaten so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind, 3. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind; f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.	**Antrag I zu Art. 24 Abs. 2, erster Satz**: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit. **Antrag II zu Art. 24 Abs. 2. lit a)**: Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft Abgrenzungsfragen auf, für welche der VE keine Antworten liefert. **Antrag zu Art. 24 Abs. 2 lit. c) Ziff. 3**: Streichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar (Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft). Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit Sicherheit bestimmbar.
Art. 25 Rechtsansprüche [1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs. Die klagende Partei kann insbesondere verlangen, dass:	

VE-DSG	Anträge und Bemerkungen
a. die Datenbearbeitung verboten wird; b. die Bekanntgabe von Personendaten an Dritte untersagt wird; c. Personendaten berichtigt, gelöscht oder vernichtet werden. 2 Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die klagende Partei verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird. Sie kann darüber hinaus verlangen, dass die Bearbeitung der bestrittenen Daten eingeschränkt wird. 3 Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.	**Antrag Art. 25 lit. a) bis c)**: Es müsste klargestellt werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. Ansonsten kann die Bestimmung nicht umgesetzt werden. **Antrag Art. 25 Ziff. 2**: Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", *eventualiter* Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis schiefe Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat. **Antrag Art. 25 Ziff. 3**: Ziff. 3. streichen. Lit. a) bis c) reichen völlig, um die Interessen der Betroffenen zu wahren. Auch die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor.
6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane	
Art. 26 Verantwortliches Organ und Kontrolle 1 Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt. 2 Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.	Keine Bemerkungen
Art. 27 Rechtsgrundlagen 1 Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. 2 Für die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Eine Grundlage in einem Gesetz im materiellen Sinn ist ausreichend, wenn die folgenden Voraussetzungen erfüllt sind: a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn klar festgelegte Aufgabe unentbehrlich; und b. Die Bearbeitung birgt für die Persönlichkeit und die Grundrechte der betroffenen Person keine besonderen Risiken. 3 In Abweichung von den Absätzen 1 und 2 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Der Bundesrat bewilligt die Bearbeitung, sofern die Rechte der betroffenen Person nicht gefährdet sind; b. Die betroffene Person hat in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt;	**Antrag zu Art. 15 Abs. 2**: Streichen „oder den Erlass einer automatisierten Einzelfallentscheidungen nach Artikel Art. 15 Absatz 1" (vgl. dazu den Kommentar zu Art. 15 Abs. 2): Damit würde jede Prozessautomatisierung und -optimierung in der Verwaltung massiv erschwert. Es stellt sich grundsätzlich auch die Frage, ob als Grundlage für die Datenbearbeitung nicht auch Regelungen auf Verordnungsstufe ausreichen sollten.

VE-DSG	Anträge und Bemerkungen
c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.	
Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen [1] Der Bundesrat kann vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling bewilligen, wenn: a. die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz im formellen Sinn geregelt sind; b. ausreichende Massnahmen getroffen werden, um eine Verletzung der Grundrechte der betroffenen Person zu verhindern; und c. eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, zwingend erforderlich ist. [2] Er holt vorgängig die Stellungnahme des Beauftragten ein. [3] Das zuständige Bundesorgan legt dem Bundesrat spätestens innerhalb von zwei Jahren nach Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor. [4] Die automatisierte Datenbearbeitung oder das Profiling müssen in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage umfasst.	**Antrag zu Art. 28 Abs. 1 und 2**: Die Bestimmung ist entweder zu streichen, oder die entsprechenden Möglichkeiten ist auch Privaten zu eröffnen.
Art. 29 Bekanntgabe von Personendaten [1] Bundesorgane dürfen Personendaten bekannt geben, wenn eine Rechtsgrundlage im Sinne von Artikel 27 Absätze 1 und 2 dies vorsieht. [2] In Abweichung von Absatz 1 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten bekannt geben, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich; b. Die betroffene Person hat in die Bekanntgabe eingewilligt; c. Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; d. Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt; e. Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben, wenn: a. die betreffenden Daten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen; und b. an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. [4] Name, Vorname, Adresse und Geburtsdatum einer Person dürfen Bundesorgane auf Anfrage auch bekannt geben, wenn die Voraussetzungen von Absatz 1 oder 2 nicht erfüllt sind. [5] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 3 bekannt geben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst gelöscht. [6] Sie lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn: a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.	
Art. 30 Widerspruch gegen die Bekanntgabe von Personendaten [1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen. [2] Das Bundesorgan weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist: a. es besteht eine Rechtspflicht zur Bekanntgabe; b. die Erfüllung seiner Aufgabe wäre sonst gefährdet. [3] Artikel 29 Absatz 3 bleibt vorbehalten.	Keine Bemerkungen
Art. 31 Angebot von Unterlagen an das Bundesarchiv [1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998 bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen. [2] Sie vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese: a. anonymisiert sind; b. zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.	Keine Bemerkungen
Art. 32 Datenbearbeitung für Forschung, Planung und Statistik [1] Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn: a. die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt;	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
b. das Bundesorgan privaten Personen besonders schützenswerte Personendaten so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind; c. die Empfängerin oder der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und d. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. [2] Die Artikel 4 Absatz 3, 27 Absätze 1 und 2 sowie Artikel 29 Absatz 1 sind nicht anwendbar.	
Art. 33 Privatrechtliche Tätigkeit von Bundesorganen [1] Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen. [2] Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.	Keine Bemerkungen
Art. 34 Ansprüche und Verfahren [1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es: a. die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt; b. die Folgen einer widerrechtlichen Bearbeitung beseitigt; c. die Widerrechtlichkeit der Bearbeitung feststellt. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so muss das Bundesorgan bei den Daten einen Bestreitungsvermerk anbringen und deren Bearbeitung einschränken. [3] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan: a. die betreffenden Personendaten berichtigt, löscht oder vernichtet; b. seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, das Verbot der Bearbeitung, den Widerspruch gegen die Bekanntgabe nach Artikel 30 oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht. [4] Die Berichtigung, Löschung oder Vernichtung von Personendaten kann nicht verlangt werden in Bezug auf die Bestände öffentlich zugänglicher Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderer öffentlicher Gedächtnisinstitutionen. Wenn die Gesuchstellerin oder der Gesuchsteller ein überwiegendes Interesse nachweisen kann, kann sie oder er jedoch verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt. [5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.	Keine Bemerkungen
Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Öffentlichkeitsgesetzes hängig, so kann die betroffene Person im Rahmen dieses Verfahrens diejenigen Rechte geltend machen, die ihr nach Artikel 34 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.	Keine Bemerkungen
Art. 36 Register [1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [2] Der Beauftragte führt ein Register der Datenbearbeitungstätigkeiten. Das Register ist öffentlich.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.	
7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte	
Art. 37 Ernennung und Stellung [1] Die oder der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen.	**Antrag zu Art. 37 Abs. 1**: Dem Bundesrat soll ein Vorschlagsrecht zukommen und die Wahl soll durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Amtsdauer von 4 Jahren gewählt". Was die blosse Genehmigung einer Wahl bringen soll, ist nicht ersichtlich. Die Person des Beauftragten soll über grosse Kompetenzen und einen Wirkungsgrad mit erheblichen finanziellen Auswirkungen auf die Schweizer Wirtschaft verfügen. In Anbetracht des zukünftigen, angedachten Gewichts dieses Posten, ist eine Wahl durch das Parlament gerechtfertigt.
[2] Das Arbeitsverhältnis der oder des Beauftragten richtet sich, soweit dieses Gesetz nichts anderes vorsieht, nach dem Bundespersonalgesetz vom 24. März 2000 (BPG). [3] Die oder der Beauftragte übt ihre bzw. seine Funktion unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder zu erhalten. Sie oder er ist administrativ der Bundeskanzlei zugeordnet. [4] Sie oder er verfügt über ein ständiges Sekretariat und ein eigenes Budget. Sie oder er stellt sein Personal an. [5] Die oder der Beauftragte unterstehen nicht dem Beurteilungssystem nach Artikel 4 Absatz 3 BPG.	**Antrag zu Art. 37 Abs. 4**: Das Budget wird durch das Parlament genehmigt.
Art. 38 Wiederwahl und Beendigung der Amtsdauer [1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden. [2] Verfügt der Bundesrat nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl, so ist der oder die Beauftragte für eine neue Amtsdauer wiedergewählt. [3] Die oder der Beauftragte kann den Bundesrat unter Einhaltung einer Frist von sechs Monaten um Entlassung auf ein Monatsende ersuchen. [4] Der Bundesrat kann die Beauftragte oder den Beauftragten vor Ablauf der Amtsdauer des Amtes entheben, wenn diese oder dieser: a. vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder b. die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.	**Antrag zu Art. 38 Abs. 2**: Der oder die Beauftragte ist für jede Amtsperiode neu zu wählen. Das Verfahren über eine Verfügung kommt einem Kündigungsverfahren gleich, das in der Praxis nur aus wichtigen Gründen möglich ist. Das Wahlorgan soll in seiner Wahl wirklich frei sein.
Art. 39 Nebenbeschäftigung [1] Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, der Verwaltung, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein. [2] Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1 auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.	**Antrag zu Art. 39 Abs. 2**: Solche Bewilligungen von Nebenbeschäftigung sind offenzulegen. Für die Vermeidung von Interessenkonflikten ist absolute Transparenz unabdingbar.
Art. 40 Aufsicht	Keine Bemerkungen.

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte überwacht die Einhaltung der Datenschutzvorschriften des Bundes. [2] Bundesverwaltungsbehörden, die nach einem anderen Bundesgesetz Private oder Organisationen ausserhalb der Bundesverwaltung beaufsichtigen, laden den Beauftragten zur Stellungnahme ein, bevor sie eine Verfügung treffen, die Fragen des Datenschutzes berührt. [3] Führt der Beauftragte gegen die gleiche Partei ein eigenes Verfahren, so haben die beiden Behörden ihre Verfahren zu koordinieren.	
Art. 41 Untersuchung [1] Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.	
[2] Das Bundesorgan oder die private Person erteilt dem Beauftragten die von ihm verlangten Auskünfte und stellen ihm alle für die Untersuchung notwendigen Unterlagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes.	**Antrag zu Art. 41 Abs. 2**: Hier ist zu ergänzen, dass bei Untersuchungen gegen Private alle Untersuchungsakten nicht dem Öffentlichkeitsgesetz unterliegen, da ansonsten über diesen Umweg Betriebsgeheimnisse an Dritte gelangen könnten. Wenn Unternehmen verpflichtet sind, dem Beauftragten alle notwendigen Unterlagen zur Verfügung zu stellen, muss es die Garantie haben, dass diese nicht veröffentlicht werden. Der Beauftragte veröffentlicht bei Untersuchungen gegen private Personen nur die Empfehlung.
[3] Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte vergeblich versucht, Auskünfte und Unterlagen einzuholen, so kann der Beauftragte im Rahmen einer Untersuchung: a. ohne Vorankündigung Räumlichkeiten inspizieren; b. Zugang zu allen notwendigen Daten und Informationen verlangen.	**Antrag zur Art. 41 Abs. 3**: Diese Bestimmung ist nur akzeptabel, wenn das Unternehmen Rechtsmittel gegen die Auskunftsverfügung hat. Eine unbestimmte Verletzung von Mitwirkungspflichten darf nicht zu Strafsanktionen oder publizitätswirksamen Aktionen des Beauftragten gegen Unternehmen führen. Bevor solche Massnahmen ergriffen werden, muss eine Editionsverfügung des Beauftragten einer gerichtlichen Überprüfung zugänglich sein.
[4] Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten.	**Antrag zu Art. 41 Abs. 4**: Streichen „private Personen". Ein Tätigwerden des Beauftragten gegenüber Privaten ohne Anzeige einer Datenschutzverletzung ist strikt abzulehnen. Wenn Anhaltspunkte vorliegen, kann der Beauftragte nach Art. 41 Abs. 1 formell vorgehen. Es dürfen hier keine mehrgleisigen Verfahren ohne Rechtsschutz für die betroffenen Parteien eingefügt werden. Im Gegenteil, es müsste für Unternehmen möglich sein, Sachverhalte rechtsverbindlich durch den Beauftragten überprüfen und mittels Attest der Datenrechtskonformität genehmigen zu lassen.
[5] Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung.	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Parteistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte Abs. 5 auch gestrichen werden.
Art. 42 Vorsorgliche Massnahmen	

VE-DSG	Anträge und Bemerkungen
[1] Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern. [2] Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.	**Antrag zu Art. 42 Abs. 1**: Ändern: Der Beauftragte kann beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen. Vorsorgliche Massnahmen sind – auch im Persönlichkeitsschutz – immer Sache der Gerichte. Hier ist die bisherige Regelung mit dem Antrag beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts beizubehalten. Es sollte hier nicht von den bewährten rechtsstaatlichen Prozessen abgewichen werden. Jedenfalls gibt es dazu keine ausreichenden Rechtfertigungsgründe.
Art. 43 Verwaltungsmassnahmen [1] Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden. [2] Der Beauftragte kann zudem die Bekanntgabe ins Ausland aufschieben oder untersagen, wenn sie gegen die Voraussetzungen nach Artikel 5 oder 6 oder gegen spezifische Bestimmungen betreffend die Bekanntgabe von Personendaten ins Ausland in anderen Bundesgesetzen, verstösst.	**Antrag zu Art 43 Abs. 1**: Ändern: Anstelle der Empfehlung und des nachfolgenden Gerichtswegs wie im heutigen Recht wird hier auch die Klage- und Beweislast umgekehrt. Das ist abzulehnen. Der Beauftragte hat in der Verfügung die Rechtsverletzung nachzuweisen. Eine Verfügung sollte nur nach der Durchführung einer Untersuchung zulässig sein, in welchem dem betroffenen Datenbearbeiter selbstverständlich auch das rechtliche Gehör gewährt wurde. Eine Datenvernichtung darf nicht durch den Beauftragten angeordnet werden können, da dies nicht wieder gutzumachende Folgen hat (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 41 reicht zum Schutz Betroffener völlig aus.
Art. 44 Verfahren [1] Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz. [2] Partei sind lediglich das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wurde. [3] Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt keine aufschiebende Wirkung zu.	**Antrag zu Art. 44 Abs. 2**: Drittpersonen haben keine Parteistellung und kein Akteneinsichtsrecht, was zu begrüssen ist. Zu ergänzen ist weiter, dass Untersuchungsunterlagen nicht dem Öffentlichkeitsgesetz unterliegen dürfen. **Antrag zu Art. 44 Abs. 3**: Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Vielmehr wäre vorzusehen, dass die aufschiebende

VE-DSG	Anträge und Bemerkungen
[4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.	Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt nicht praktikable Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Art. 45 Anzeigepflicht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.	**Antrag zu Art. 45**: Streichen. Ein Recht zur Anzeige würde völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE).
Art. 46 Amtshilfe zwischen schweizerischen Behörden [1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses Gesetzes erforderlich sind. [2] Der Beauftragte gibt den folgenden Behörden die Informationen und Personendaten bekannt, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind: a. den für den Datenschutz zuständigen kantonalen Behörden; b. den zuständigen Strafverfolgungsbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 45 geht; c. den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss Artikel 41 Absatz 3, 42 und 43.	**Antrag zu Art. 46 Abs. 2**: Hier ist zu ergänzen, dass Informationen die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen.
Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden [1] Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen: a. die Identität des Verantwortlichen, des Auftragsbearbeiters oder anderer beteiligter Dritter; b. Kategorien von betroffenen Personen; c. die Identität der betroffenen Personen, falls: 1. die betroffenen Personen eingewilligt haben, oder 2. die Mitteilung der Identität der betroffenen Personen unumgänglich ist, um die gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde zu erfüllen; d. bearbeitete Personendaten oder Kategorien von bearbeiteten Personendaten; e. den Zweck der Datenbearbeitung; f. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern; g. technische und organisatorische Massnahmen. [2] Der Beauftragte kann der ausländischen Behörde Amtshilfe gewähren und ihr die Informationen gemäss Absatz 1 zur Verfügung stellen, wenn sie folgende Voraussetzungen erfüllt: a. Sie verpflichtet sich, die zur Verfügung gestellten Informationen und Personendaten, nicht für andere Zwecke zu verwenden, als im Amtshilfegesuch angegeben; b. Sie verpflichtet sich, ähnlichen Amtshilfegesuchen der Schweiz Folge zu leisten;	**Antrag zu Art. 47 Abs. 1**: Auch hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen, insbesondere auch für Informationen, die in der Schweiz dem Berufsgeheimnis unterliegen. Die Herausgabe vertraulicher Unternehmensdaten darf nicht im Ermessen des Beauftragten liegen, sondern – wenn überhaupt – nur mit Zustimmung des betroffenen Unternehmens zulässig sein.

VE-DSG	Anträge und Bemerkungen
c. Sie verpflichtet sich zur Wahrung des Amts- und Berufsgeheimnisses; d. Sie verpflichtet sich, die erhaltenen Informationen und Personendaten nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln; e. Sie verpflichtet sich, die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten.	
Art. 48 Information [1] Der Beauftragte erstattet der Bundesversammlung periodisch sowie bei Bedarf Bericht. Er übermittelt den Bericht gleichzeitig dem Bundesrat. Die periodischen Berichte werden veröffentlicht. [2] In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über seine Feststellungen und Verfügungen.	**Antrag zu Art. 48 Abs. 2**: Streichen des Begriffs „seine Feststellungen und Verfügungen" und ersetzen mit „seine Untersuchungen". Damit der Beauftragte die Persönlichkeitsrechte wahrt, soll er nur über die Tatsache einer Untersuchung informieren. Es ist nicht ersichtlich, weshalb der Beauftragte zur Profilierung von Amt und Person ein öffentliches Prangerrecht haben soll.
Art. 49 Weitere Aufgaben Der Beauftragte nimmt darüber hinaus insbesondere folgende Aufgaben wahr: a. Er informiert und berät die Organe des Bundes und der Kantone sowie private Personen bei Fragen des Datenschutzes. b. Er arbeitet mit schweizerischen und ausländischen Behörden, die für den Datenschutz zuständig sind, zusammen. c. Er sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz. d. Er erteilt der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann. e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen. f. Er nimmt die ihm durch das Öffentlichkeitsgesetz übertragenen Aufgaben wahr.	**Antrag zu Art. 49 lit. d**: Streichen. Wenn der Datenschutzbeauftragte eine Aufsichtsfunktion hat, kann er nicht gleichzeitig auch eine Konsumentenschutzaufgabe erfüllen dürfen.
8. Abschnitt: Strafbestimmungen	**Antrag zum 8. Abschnitt (Art. 50ff)**: Das gesamte Sanktionssystem ist zu überarbeiten. Es führt zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden und Unternehmen. Unverständlich ist zudem, dass gerade die Verwaltung von den Strafsanktionen ausgenommen werden soll. Es wird komplett vergessen und ausgeblendet, dass vor noch nicht langer Zeit, die Gefahr im Umgang mit Daten nicht von Privaten und nicht von Unternehmen, sondern vom Staat selbst ausgegangen ist (Stichwort: Fichen-Affäre). Es wäre naiv zu glauben, dass sich diese Bedrohung in den letzten 20 Jahren komplett verflüchtigt hätte. Mit einer zunehmend

VE-DSG	Anträge und Bemerkungen
	hohen Verwaltungsquote von gegen 40% wäre ein sehr hoher Anteil der Berufstätigen vom Sanktionssystem ausgenommen. Das ist höchst zweifelhaft und politisch nicht zu rechtfertigen. Alternative: Der Beauftragte soll als Aufsichtsbehörde untersuchen und verfügen können. Unternehmen sollen sich in diesem verwaltungsrechtlichen Verfahren wehren können. Erst wenn rechtskräftige Entscheide nicht umgesetzt worden sind, sollten Strafsanktionen greifen. Es besteht kein Rechtfertigungsgrund, von diesem in anderen Belangen des Bundesrechts verankerten Prinzip abzuweichen.
Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten [1] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft: a. die ihre Pflichten nach den Artikeln 13, 15 und 20 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;	**Antrag zu Art. 50**: Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen. Der Bussenrahmen ist auf eine maximale Höhe von CHF 5'000.- bzw. – im Wiederholungsfall – auf maximal CHF 10'000.- zu begrenzen. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen anzusetzen, sicher nicht Beträge bis CHF 500'000.-. Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.- für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Grössenordnungen. Bussenbeträge über CHF 100'000.- sind bislang in der Schweiz nicht bekannt. Die Erhöhung des Strafrahmens auf CHF 500'000.- ist daher völlig überrissen und nicht nachvollziehbar.
b. die es vorsätzlich unterlassen: 1. die betroffene Person nach Artikel 13 Absätze 1 und 5, 15 und 17 Absatz 2 die betroffene Person zu informieren; oder 2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2, 3 und 4 zu liefern.	**Antrag zu Art. 50 Abs. 1 lit. b)**: Ändern. Art 13 ist vollständig von der Sanktionierung auszunehmen.
c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3).	**Antrag zu Art. 50 Abs. 1 lit. c)**: Streichen. Ist vollständig von der Sanktionierung auszunehmen.
[2] Mit Busse bis zu 500 000 Franken werden private Personen bestraft, wer vorsätzlich: a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b und Absatz 6 zu informieren; b. die es unterlassen, dem Beauftragten die standardisierten Garantien oder die verbindlichen unternehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d Ziff. 1);	**Antrag zu Art. 50 Abs. 2, lit. a) und b)**: Streichen. Da die Meldepflicht sowieso massiv reduziert werden müssen, ist auch diese Bestimmung zu streichen.

VE-DSG	Anträge und Bemerkungen
c. dem Beauftragten bei der Untersuchung (Art. 41 Abs. 2) falsche Auskünfte erteilen oder die Mitwirkung verweigern; e. es unterlassen, dem Beauftragten Verletzungen des Datenschutzes nach Artikel 17 Absatz 1 zu melden; f. einer Verfügung des Beauftragten nicht Folge leistet. [3] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft, die es vorsätzlich unterlassen: a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren; b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 zu informieren. [4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**Antrag zu Art. 50 Abs. 2, lit. e)**: Ändern. Diese Bestimmung ist auf Vorfälle zu beschränken, die schwerwiegend sind und mehr als 1'000 Personen betreffen. **Antrag zu Art. 50 Abs. 2, lit. f**: Streichen. Hier genügt die bestehende Strafbestimmung im StGB. **Antrag zu Art. 50 Abs. 3, lit. a)**: Streichen. Die dem Bst. a) zugrundeliegende Bestimmung ist Art. 19 Bst. b) ist in der Praxis gar nicht umsetzbar. Daher ist auch die Strafbestimmung zu streichen. **Antrag zu Art. 50 Abs. 4**: Streichen. Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen.
Art. 51 Verletzung der Sorgfaltspflichten [1] Mit Busse bis zu 500'000 Franken werden private Personen auf **Antrag** bestraft, die vorsätzlich: a. unter Verstoss gegen Artikel 5 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln; b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 7 Absätze 1 und 2 erfüllt sind; c. es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder Verlust zu schützen (Art. 11); d. es unterlassen, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16); e. es unterlassen, die Vorkehren nach Artikel 18 zu treffen; f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert.	**Antrag zu Art. 51 Abs. 1**: Bei Vorsatz sind Bussen bis CHF 10'000.- angemessen. **Antrag zu Art. 51 Abs. 1 lit. a)**: Die Meldepflicht von Art. 6 Abs. 2 ist von der Busse auszunehmen, da ansonsten tausende von KMU unwissentlich kriminalisiert werden. **Antrag zu Art. 51 Abs. 1 lit. d)**: Streichen; erst die Folgeabschätzung kann ja zeigen, ob eine Folgeabschätzung notwendig wäre. Die Strafdrohung führt dazu, dass dieses Verfahren für jede Datenbearbeitung durchgeführt werden muss. In der Rechtsfolgeabschätzung werden Kosten von CHF 5'000 – 30'000.- pro Durchführung veranschlagt, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU führen würde. **Antrag zu Art. 51 Abs. 1 lit. e)**: Streichen; Hier handelt es sich um eine unbestimmte Handlungsdefinition, die dadurch kaum eine Strafbarkeit auslösen kann. **Antrag zu Art. 51 Abs. 1 lit. f)**: Streichen; die Strafdrohung führt dazu, dass alle Prozesse für die Datenbearbeitung vorsorglich dokumentiert werden müs-

VE-DSG	Anträge und Bemerkungen
[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	sen, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU, führen würde. In der RFA wurden diese Kosten nicht erhoben. **Antrag zu Art. 51 Abs. 2**: Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen.
Art. 52 Verletzung der beruflichen Schweigepflicht [1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf **Antrag** bestraft, wer vorsätzlich geheime Personendaten bekannt gibt: a. von denen er im Rahmen seiner beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat; b. welche er selbst zu kommerziellen Zwecken bearbeitet hat. [2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er bei der Tätigkeit für einen Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat. [3] Das Bekanntgeben geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.	**Antrag zu Art. 52**: Streichen; der bisherige Art. 35 DSG hat die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten geregelt. Die Ausweitung auf den unbestimmten Begriff „geheime Personendaten" wird abgelehnt. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Damit würde jeder Bearbeiter von Personendaten einer strafbewehrten Schweigepflicht unterworfen. Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist völlig unverhältnismässig. *Eventualiter* wäre es sinnvoller, die Strafbarkeit in dieser Bestimmung auf Auftragsbearbeiter und Beauftragte zu beschränken.
Art. 53 Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.	**Antrag zu Art. 53**: Streichen; die bestehenden Regelungen im Verwaltungsstrafrecht und im Strafrecht sind ausreichend.
Art. 54 Anwendbares Recht und Verfahren Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.	**Antrag zu Art. 54**: Streichen; die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet werden und ist somit vom Bund zu führen.
Art. 55 Verfolgungsverjährung für Übertretungen Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.	**Antrag zu Art 55**: Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109) und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
9. Abschnitt: Abschluss von Staatsverträgen	
Art. 56 Der Bundesrat kann Staatsverträge abschliessen betreffend: a. die internationale Zusammenarbeit zwischen Datenschutzbehörden; b. die gegenseitige Anerkennung eines angemessenen Schutzes für die Bekanntgabe von Personendaten ins Ausland.	Titel fehlt zum Artikel fehlt.
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unterstehen den Artikeln 1-22, 26, 27, 29 bis 32, 34 Absätze 1-3 und 36 dieses Gesetzes, soweit sie nicht kantonalen Datenschutzvorschriften unterstehen, die einen angemessenen Schutz der Daten gewährleisten. [2] Die Kantone bestimmen ein Organ, das die Einhaltung der Datenschutzvorschriften überwacht. Die Artikel 41-43, 48 und 49 gelten sinngemäss.	
Art. 58 Aufhebung und Änderung anderer Erlasse Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.	Keine Bemerkungen
Art. 59 Übergangsbestimmung Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die für Verantwortlichen sowie der Auftragsbearbeiter in der Lage sein: a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen; b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.	**Antrag zu Art. 59**: Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, die nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken ist.
Art. 60 Referendum und Inkrafttreten [1] Dieses Gesetz untersteht dem fakultativen Referendum. [2] Der Bundesrat bestimmt das Inkrafttreten.	Keine Bemerkungen

Sammlung Änderungsvorschläge: Aufhebung und Änderung anderer Erlasse

VE-DSG	Anträge und Bemerkungen
11. Zivilprozessordnung *Art. 20 Bst. d* Für die folgenden Klagen und Begehren ist das Gericht am Wohnsitz oder Sitz einer der Parteien zuständig: d. Klagen und Begehren nach dem Datenschutzgesetz vom ... *Art. 99 Abs. 3 Bst. d* [3] Keine Sicherheit ist zu leisten: d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom.... *Art. 113 Abs. 2 Bst. g* [2] Keine Gerichtskosten werden gesprochen in Streitigkeiten:	**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Da in Datenschutzfragen der Beauftragte eine Aufsichtsfunktion ausübt, kann er bei Verstössen aktiv werden. Es braucht hier keine weitere soziale Gerichtsbarkeit. Für zivilrechtliche Verfahren genügen die bestehenden Regeln. Das kostenlose Prozessieren könnte hier eine Flut – auch von mutwilligen – Klagen auslösen. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll – wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist – seine Kostenrisiken abwägen müssen, ehe Gerichte bemüht werden.

VE-DSG	Anträge und Bemerkungen
g. nach dem Datenschutzgesetz vom …… *Art. 114 Bst. f* Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom …… *Art. 243 Abs. 2 Bst. d* [2] Es gilt ohne Rücksicht auf den Streitwert für Streitigkeiten: d. zur Durchsetzung der Ansprüche nach den Artikeln 12 und 20 des Datenschutzgesetzes vom …	

VE-DSG	Anträge und Bemerkungen
13. Strafgesetzbuch *Art. 179novies* Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. *Art. 179decies* Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.	**Antrag zu Art. 179novies**: Die Strafbarkeit der Beschaffung ist zu beschränken auf Daten die einem Berufsgeheimnis unterliegen sowie auf besonders schützenswerte Personendaten. Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe zu bestrafen ist unverhältnismässig. Hier reicht eine Geldstrafe.
37. Fernmeldegesetz vom 30. April 1997 *Art. 13a Abs. 1 erster Satz* 1 Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, bearbeiten, sofern dies für die Erfüllung der ihnen durch die Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. ... *Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz* 1 ... Zu diesen Daten gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten. 2 Unter Vorbehalt anders lautender internationaler Vereinbarungen dürfen die Kommission und das Bundesamt ausländischen Aufsichtsbehörden im Fernmeldebereich Daten, einschliesslich in Verwaltungs- oder Verwaltungsstrafverfahren beschaffter besonders schützenswerter Personendaten, nur übermitteln, sofern diese Behörden: 4 Schweizerische Behörden geben der Kommission und dem Bundesamt kostenlos diejenigen Daten weiter, die für die Durchsetzung der Fernmeldegesetzgebung von Bedeutung sein können, einschliesslich besonders schützenswerter Personendaten. ...	**Bemerkung zu datenschutzrechtlichen Regulierungen im Fernmeldegesetz**: Es ist klarzustellen, dass datenschutzrechtliche Regulierungen im Fernmeldegesetz und in dessen Ausführungsbestimmungen als *lex specialis* den allgemeinen Datenschutzbestimmungen des DSG und dessen Ausführungsbestimmungen vorgehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
WWZ Telekom AG

Thomas Reber
Leiter Telekom

René Bühler
Leiter Informatikdienste

wynet
Kommunikationsnetz Wynau

Wynet, Kommunikationsnetz Wynau
Flurweg 24, 4923 Wynau
Telefon 062 929 20 41
wynet@besonet.ch

www.wynet.ch

CHE-102.251.766 MwSt.

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

4923 Wynau 02.04.2017 / uhu

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DDSG)

Sehr geehrte Frau Bundesrätin

Sie haben am 21. Dezember 2016 interessierte Kreise eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nimmt die Genossenschaft Wynet Kommunikationsnetz Wynau gerne wahr.

Die Wynet Genossenschaft Wynau ist ein Anbieter von Telekommunikationsnetzinfrastrukturen und -dienstleistungen.Wir leisten damit einen grossen Beitrag an die digitale Vernetzung der Schweiz und deren Bevölkerung. Unser Kerngeschäft ist die Datenverarbeitung. Diese Daten erfüllen zunehmend und überwiegend die Voraussetzungen von Personendaten bzw. Daten, die zu einer Identifikation einer Person führen könnten. Datenschutz und Datensicherheit, sowie die entsprechenden Regulierungen sind daher für uns eine der wichtigsten Geschäftsgrundlagen. Entsprechend besteht eine hohe Betroffenheit, wenn diesbezüglich neue Regulierungen zur Diskussion stehen.

Gerne nehmen wir wie folgt Stellung, wobei wir zunächst auf einige grundsätzliche Punkte eingehen, ehe wir – wie verlangt – zu den einzelnen Bestimmungen des VE-DSG Stellung beziehen und Anträge stellen:

A. Grundsätzliche Bemerkungen

1. Chancen der Digitalisierung und damit auch Chancen der Datenbearbeitung

Die Digitalisierung bietet für die Zukunft ein enormes Entwicklungspotential und sollte durch unterstützende Rahmenbedingungen – gerade im Bereich Datenbearbeitung – gefördert werden. Die Schweiz sollte ein Wirtschaftsstandort für digitale Geschäftsmodelle sein und grösstmögliche Freiräume für die Datenbearbeitung zulassen. Grundsätzlich sollte jede Form von Datenbearbei-

tung zulässig sein und die informelle Selbstbestimmung sollte über Auskunfts- und Kontrollrechte realisiert werden. Ein Regulierungskonzept darf nicht der Vorstellung folgen, eine „Datenbearbeitung" durch Unternehmen sei *per se* anrüchig. Ein modernes Datenschutzgesetz ist weiter auch kein spezielles Konsumentenschutzrecht.

Die im Vorentwurf vorherrschende „Verbots- und Bestrafungskultur" sollte deshalb so nicht umgesetzt werden. Die Datenschutzgesetzgebung ist bisher – und gemäss VE-DSG noch mehr – als Konsumentenschutzgesetzgebung stark von gesetzlichen Einschränkungenfür Unternehmen geprägt, die jedoch in der Praxis durch Einwilligungserklärungen der Datensubjekte übersteuert werden können. Dies führt heute gesamthaft nicht zu mehr Datenschutz, sondern nur zu aufwendigeren Einwilligungsverfahren und damit höheren Transaktionskosten bei der Geschäftsabwicklung.

Wir begrüssen eine Stärkung des Rechts auf informelle Selbstbestimmung, lehnen jedoch die Stossrichtung ab, dass zukünftig einzelfallbezogene Zustimmungserklärungen eingeholt werden müssen. Für eine wirtschaftliche Geschäftsabwicklung muss es möglich sein, in einem Vertragsverhältnis eine pauschale Einwilligung über allgemeine Geschäftsbedingungen abzuschliessen. Die Grundlagen dazu genügen im UWG.

2. Gleichwertigkeit des Datenschutzes in der CH und in der EU

Datenschutzregulierung ist heute kein nationales Thema mehr. Die modernen Kommunikationsnetze und die technologischen Entwicklungen machen den Datenverkehr zu einem globalen Thema. Ein freier Datenverkehr ist aus unserer Sicht unbedingt zu erreichen, insbesondere durch eine gegenseitige institutionelle Anerkennung eines gleichwertigen Datenschutzes mit möglichst vielen Ländern. Allen voran natürlich mit der Europäischen Union und den USA. Damit können für Unternehmen hohe administrative Hürden und Kosten vermieden werden. Dabei sind die notwendigen Bestimmungen für eine Gleichwertigkeit im Datenschutz umzusetzen.

2.1 Unnötiger „Swiss Finish"

Ein Grund für die Revision des DSG ist gemäss Erläuterungsbericht des EJPD/BJ die Entwicklung des Datenschutzes im europäischen Raum. Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) EuDSGVO in Kraft. Zudem gilt die EU-Richtlinie 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen.Die DSG-Revision soll die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Die Annäherung würde zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür bilden, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht (obschon unserer Ansicht nach dies auch das bestehende DSG weiterhin tun würde). Die Revision des Schweizer DSG geht aber in mehreren Fällen über das Schutzniveau der EU hinaus, was nicht nachvollziehbar ist. Beispiele für diesen Swiss Finish sind:

a) Art. 13 Abs. 3 und 4 VE-DSG sehen eine Pflicht zur detaillierten Information betroffener Personen über die Datenweitergabe an externe Auftragsbearbeiter (z.B. ein

Versanddienstleister) sowie bei der Weitergabe von jeglichen Personendaten vor. Für den Adressaten solcher Informationen führt dies in einer zunehmend über digitale Geschäftsprozesse gesteuerten Gesellschaft zu einer Informationsflut. Nicht einmal die EU-Richtlinie 680/2016 vom 27. April 2016 sieht diesen Detaillierungsgrad vor.

b) Art. 16 Abs. 3 VE-DSG sieht eine Informationspflicht des Datenschutzbeauftragten über die Datenschutz-Folgeabschätzungen in jedem Fall vor. Die EU-Richtlinie 680/2016 hingegen fordert dies in Art. 27 und 28 nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen.

c) Gemäss Art. 19 lit. a VE-DSG soll in der Schweiz eine Dokumentationspflicht für sämtliche Datenverarbeitungsvorgänge gelten. Auch diese Bestimmung geht weiter als die in der EU-Richtlinie vorgesehene Protokollierung (Art. 25). Diese besagt lediglich, dass gewisse Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden sollen.

d) Art. 20 Abs. 3 VE-DSG sieht vor, dass die betroffene Person bei jeder, aufgrund einer Datenbearbeitung getroffenen Entscheidung Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung erhält. Sowohl die EU-Richtlinie 2016/680 als auch die EuDSGVO sehen eine solche Information nur bei der automatisierten Einzelentscheidung vor und nicht bei Entscheidungen basierend auf einer Datenbearbeitung generell.

e) Auch der Ansatz des VE-DSG betreffend Profiling geht über die Bestimmungen der EuDSGVO und der Konvention 108 des Europarates hinaus. Die vorgeschlagene zusätzliche Schutzkategorie ist weder im Sinne der EuDSGVO noch der Konvention. Schutzrelevant soll ein Verarbeitungsvorgang sein, bei welchem es mittels technischer Hilfsmittel zu einer automatisierten, systematischen Verarbeitung von Personendaten kommt, sofern dieser Prozess dazu bestimmt ist, wesentliche, auf eine bestimmte Person bezogene persönliche Merkmale zu analysieren, zu bewerten oder diesbezügliche Entwicklungen zu antizipieren. Die Bedingung einer vorgängigen ausdrücklichen Einwilligung bei jeder Art von Profiling schiesst über das Ziel hinaus. Profiling soll nicht bereits bei dessen Erstellung schutzrelevant werden.

f) Überschiessende Informationspflichten (z.B. Art. 6 Abs. 2 oder Art. 13 Abs. 5 VE-DSG), die Geschäftsgeheimnisse betreffen können (gemäss Art. 6 Abs. 2 VE-DSG informiert der EDÖB über heikle Verfahren und Geschäftsgeheimnisse, ohne dass ein datenschutzrechtlicher Tatbestand dazu vorliegen müsste). Diese Pflicht ist dem EU Recht (inkl. E-SEV 108) fremd.

Wir lehnen Bestimmungen ab, die über das Mass der europäischen Regelungen hinausgehen. Es besteht keine Notwendigkeit für einen «Swiss Finish». Entsprechende Vorschläge sind ersatzlos zu streichen oder auf ein supranationales Mass zurückzunehmen.

2.2 Keine Doppelspurigkeiten bei der Aufsicht

Da viele Schweizer Unternehmen eine Tätigkeit in der Europäischen Union ausüben, werden diese auf der Grundlage von Art. 3 DSGVO i.V.m. Art. 55 Abs. 1 DSGVO auch der Aufsicht der nationalen Datenschutzbehörden unterstehen. Diese Doppelaufsicht bringt einerseits zahlreiche Rechtsunsicherheiten mit sich und andererseits verursacht sie eine massive administrative Zusatzbelastung der Schweizer Unternehmen. Es ist mit der Europäischen Union eine Gleichbehandlung auszuhandeln, damit die Schweizer Datenschutzaufsicht gegenseitig in das Konzept des „One-Stop-Shop" nach Art. 56 DSGVO einbezogen werden kann. Heute steht diese für Unternehmen ausserhalb der EU nicht zur Verfügung.

3. Fehlende verfassungskonforme Regulierungskosten Folgeabschätzung (RFA)

Die Bundesverfassung verpflichtet in Art. 170 die Bundesversammlung, die Massnahmen des Bundes auf ihre Wirksamkeit zu prüfen („Die Bundesversammlung sorgt dafür, dass die Massnahmen des Bundes auf ihre Wirksamkeit überprüft werden."). Nach Art. 141 Abs. 2 Bst. f) ParlG müssen in der Botschaft an das Parlament eine Kosten-Nutzen Abschätzung sowie nach Bst. g) die Folgen für die Wirtschaft und die Gesellschaft erläutert werden.

Auf Seite 23 desErläuterungsberichts zum VE-DSG werden die Regulierungskosten als unbedeutend eingestuft. **Diese Einschätzung ist falsch**. Alle Unternehmen bearbeiten heute in zunehmendem und komplexem Mass Personendaten bzw. Rohdaten für Persönlichkeitsprofile und sind damit von den Bestimmungen direkt betroffen. **Die Regulierungskosten sind für alle Unternehmen massiv höher als beschrieben!**

3.1 Mangelhafte Durchführung der Regulierungsfolgeabschätzung

Wir stellen die Durchführung der RFA und vor allem das Ergebnis in Bezug auf den VE-DSG grundsätzlich in Frage. Die Unternehmensbefragung basiert auf einer völlig ungenügenden Nettostichprobe von lediglich 95 (!) Fragebogen, wovon keines der Unternehmen den Fragebogen vollständig beantwortet hat. Insbesondere wurden die spezifischen Daten zu den Folgen nur von wenigen Unternehmen beantwortet. Keines der angefragten Unternehmen machte bei einer Interviewerhebung mit.[1] Die Studienverfasser – immerhin eine renommierte Revisionsgesellschaft – erklären dazu ohne jeden Interpretationsspielraum selbst:

> „Die im Rahmen der Durchführung der Unternehmensbefragung erfassten Daten waren sowohl in Bezug auf Quantität als auch Qualität unzureichend; auf eine gesamtwirtschaftliche Hochrechnung der Auswirkungen musste daher verzichtet werden. Die Gründe des unzureichenden Datenrücklaufs liegen zunächst in der Komplexität des Untersuchungsgegenstands."[2]

> „Die Quantität und die Qualität des Rücklaufs aus der Unternehmensbefragung ermöglichte es nicht, in repräsentativer Weise eine Hochrechnung zur Schätzung der finanziellen Auswirkungen zu erstellen."[3]

---

1 Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

2 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 8.

3 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 24.

Eine korrekte Aussage ist daher aufgrund dieser Angaben nicht möglich und es ist erstaunlich, dass das EJPD in ihrem Erläuterungsbericht zum Ergebnis kommt, die zu erwartenden Regulierungskostenfolgen seien unbedeutend. Im Bericht wird lediglich angegeben, dass die fehlenden statistischen Erhebungen durch Gespräche mit Fachpersonen ausgeglichen worden sind. Auch das ist falsch: Die angeblichen Gespräche sind ein dreistündiges Gespräch vom 4. Mai 2016 mit neun Fachpersonen, wo auch der Geschäftsführer von SUISSEDIGITAL anwesend war. Die anwesenden Vertreter haben bei der mündlichen Erörterung der Fragen wiederholt darauf hingewiesen, dass eine verbindliche Beurteilung der „statistischen" Ergebnisse aufgrund der unzureichenden Quantität und Qualität der Umfrageergebnisse absolut unmöglich sei. Wir finden die sehr kritischen Aussagen der angeblich befragten Fachpersonen im Bericht heute mit keinem Wort erwähnt. In der Studie wird lediglich vermerkt, dass diese Aussagen nicht repräsentativ sind.[4] Über den Verlauf der Sitzung vom 4. Mai 2016 wurde durch den Geschäftsführer von SUISSEDIGITAL ein internes Protokoll erstellt; dort ist auch die – für die desaströse Datenqualität – von einem Berater des Bundes vorgebrachte Begründung vermerkt, für die Untersuchung wären halt lediglich CHF 80'000.- Budget zur Verfügung gestellt worden.

Wir sind der Meinung, dass damit die gesetzlich vorgeschriebene Regulierungsfolgeabschätzung nicht korrekt durchgeführt wurde. Das ist für einen Vorentwurf von derartiger wirtschaftlicher Tragweite nicht akzeptabel und wir behalten uns diesbezüglich alle rechtlichen Massnahmen ausdrücklich vor, sollte dieser Umstand im Zuge der Abwicklung des weiteren Gesetzesprojekts keine Beachtung finden.

3.2 Methodisch fehlerhafte Durchführung der Regulierungsfolgeabschätzung

Die Einteilung der Unternehmen in drei Kategorien scheint völlig willkürlich und basiert nicht auf der tatsächlichen Betroffenheit. So werden zum Beispiel die Mehrheit der gewerblichen KMU-Betriebe (wie Metzgerei, Schreinerei, Papeterie, Spenglerei, Elektriker, lokale Transporteure, Baubetriebe, Bauernbetriebe, Velomechaniker, Coiffeur etc.) in das Segment A als Unternehmen mit geringer datenschutzrechtlicher Exponierung und keinem oder geringem Einsatz von Web-IT-Technologien eingeteilt.

Dabei wird verkannt, dass heute – und vor allem in Zukunft – jedes Unternehmen moderne Informatikmitteleinsetzt, eine Internetseite und Social Media-Profile betreibt und damit Personendaten bearbeitet. Gerade kleine Unternehmen nutzen überdurchschnittlich viel cloudbasierte Internetapplikationen oder beziehen ihre gesamte Geschäftssoftware aus der Cloud. Als Beispiel deinen Cloud-Angebote wie„Microsoft365" für kleinere und mittlere Unternehmen mit einer Datenspeicherung im Ausland, u.a. auch in den USA. Damit müssen diese 335'000 (55.1%) Unternehmen korrekterweise dem Segment B als Unternehmen mit mittlerer bis grosser datenschutzrechtlicher Exponierung (innerhalb der Schweiz und weltweit tätige Unternehmen und/oder Einsatz von Web-IT-Technologien wie Webseiten für Marketing oder Nutzung von Cloud Services) zugeordnet werden.[5]

---

[4] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 25.

[5] Vgl. RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 5.

3.3 Falsche Angaben zur Regulierungsfolgeabschätzung im VE-DSG

Die Folgekosten für die Wirtschaft werden überhaupt nicht quantifiziert. Vielmehr wird behauptet:

> „Die Analyseergebnisse zeigen, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen generell nur geringfügig betroffen sind. Die Auswirkungen der Revision auf dieses Segment sind somit verhältnismässig gering. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im VE vorgesehenen Massnahmen stärker betroffen als Grossunternehmen, da sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei."[6]

Nur schon durch das Zusammenziehen der in der Studie vorhandenen – ungenügenden – Schätzungen, wird der massive Umsetzungsaufwand sichtbar, entsprechend unerklärlich es ist, dass dies im Erläuterungsbericht mit keinem Wort erwähnt wird:[7]

Handlungspflichten nach VE-DSG	Einmalig	Wiederkehrend	Kosten CHF
Informationspflichten			
Pflicht zur Information der betroffenen Person	60 – 100 Stunden	30 Stunden	3000 – 40'000
Auskunft über Aufbau der Datenbearbeitung	4- 12 Stunden	1.6 h – 3 Tage pro Fall	Keine Angabe
Informationspflicht Automatisierte Entscheidungen	30 – 50 Stunden	3 Stunden pro Fall	10'000
Meldung Data Breach	5 – 20 Stunden	2 – 5 Stunden pro Fall	5'000 – 10'000
Datenherrschaft			
Mitteilung, Löschung, Beschränkung	14 – 20 Stunden	3 Stunden pro Fall	100 – 5'000
Pflichten auf Datenübertragbarkeit	12 Stunden	2 Stunden pro Fall	7'500
Unternehmensinterne Datenschutzorganisation			
Datenschutz-Folgeabschätzung[8]		20 – 160 h pro Fall	5'000 – 30'000
Privacy by Default	1 – 40 Stunden		500 – 5'000
Betriebliche Datenschutzbeauftragter		500 – 2'000 h pro Jahr	
Grenzüberschreitender Datenverkehr			
Genehmigung Standard Datentransfervereinbarung	50 Stunden		5'000

Auch wenn man nur die Aufgaben einbezieht, die alle Unternehmen beachten müssen, und als Basis Minimalschätzungen als Grundlage für eine Hochrechnung annimmt, ergeben sich Umsetzungskosten für die Schweizer Wirtschaft von über CHF 1'532'160'000, resp. im Durchschnitt von CHF 2'520 pro Unternehmen.[9] In der Praxis dürften diese noch wesentlich höher liegen.

---

6 Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetze und Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 23.

7 RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 27 ff.

8 In einer Studie der Europäischen Union zur Datenschutz-Folgeabschätzung (Privat Impact Analysis) wurden die Kosten pro Durchführung auf € 14'000 – 149'000 geschätzt. Quelle: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, Seite 70.

9 608'000 Unternehmen mit einem Aufwand von 84 Stunden zu einem Stundenkostensatz von CHF 30.

Es muss heute nämlich davon ausgegangen werden, dass alle Unternehmen von diesen vorgeschlagenen Bestimmungen betroffen sind, insbesondere da auch alle ohne jede *de minimis*-Schwelle den exzessiven Strafbestimmungen unterliegen. Selbst die Studienverfasser gehen von einer vergleichsweise hohen Belastung der Unternehmen aus:

> „Gleichsam haben mehrere Fachpersonen im Rahmen der Fachgespräche vorgebracht, dass bei gleicher Datenbearbeitungstätigkeit KMU stärker von der Revision oder generell von den datenschutz-rechtlichen Verpflichtungen betroffen sind als grosse Unternehmen, da ihnen die notwendige Compliance-Infrastruktur fehle resp. sie im Verhältnis teurer sei. In Bezug auf die Unternehmen der Segmente B und C ist demgegenüber von einer vergleichsweise hohen Belastung durch die Revision des Datenschutzgesetzes auszugehen."[10]

Aufgrund der methodischen Fehlbeurteilung wird in Verbindung mit der ungenügenden Datenerhebung bei den Unternehmen sichtbar, dass einerseits die Regulierungsfolgenabschätzung nicht korrekt durchgeführt wurde und andererseits die Regulierung für die gesamte Wirtschaft massiv höhere Kosten zur Folge hat.

Bislang wurde die korrekte Durchführung eines Vernehmlassungsverfahrensodersogar die Vorlage einer Botschaft an das Parlament ohne solche Regulierungskostenfolgenabschätzung nie durch die Judikative überprüft. Wir und mit uns die gesamte Schweizer KMU-Wirtschaft müssen darauf vertrauen, dass dieses Manko vor einer Parlamentsvorlage unbedingt und professionell korrigiert wird. Andernfalls muss diese Korrektur spätestens vom Parlament bzw. den entsprechenden Rechtskommissionen vorgenommen werden. Sollte diese nicht gelingen, würden die neuen Regulierungen spätestens beim Vollzug einer auf den VE-DSG gestützten Verordnung über die akzessorische Normenkontrolle Fälle für Gerichte.

B. Forderungen

Wir stellenweiter folgende Forderungengrundsätzlicher Natur an das revidierte Datenschutzgesetz:

a) Eine klare Regelung der Einwilligung und eine gesetzliche Vermutung der Einwilligung bei definierten Vorgängen, wie zum Beispiel einem Vertragsverhältnis würden den Unternehmen wesentlich mehr Rechtssicherheit und weniger administrativen Aufwand bringen. Auf eine Ausweitung der Einwilligung auf jeden Einzelfall oder die Zustimmung zur Datenbearbeitung ist zu verzichten.

b) Auf die unüberschaubare Menge von Informations- und Dokumentationspflichten der Unternehmen sowie der rein administrativen Meldungen an den Beauftragten ist grundsätzlich zu verzichten. Hingegen sollten Unternehmen vom Beauftragten innerhalb von 30 Tagen eine verbindliche Beurteilung einer Datenbearbeitung verlangen können (Negativattest, *Comfort Letter* oder dergleichen).

c) Auf eine Ausweitung des Strafenkatalogs ist zu verzichten. Insbesondere sind nur materielle Datenschutzverletzungen zu sanktionieren und keinesfalls Verletzungen von Dokumentations- oder Meldepflichten an den Beauftragten. Es bestehen heute genügend Möglichkeiten bei tatsächlichen Verstössen, Sanktionen gegen fehlbare

---

[10] RFA DSG, Regulierungsfolgeabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), PWC, Schlussbericht vom 11. Juli 2016, S. 53.

Unternehmen zu verhängen. Der Verweis auf das Persönlichkeitsrecht für Ansprüche von betroffenen Personen hat sich ebenfalls bewährt und muss nicht geändert werden.

C. Stellungnahme zu den einzelnen Artikeln

Im Übrigen finden Sie unsere Anträge und Bemerkungen zu den einzelnen Artikeln wie verlangt in der nachfolgenden tabellarischen Übersicht:

VE-DSG	Anträge und Bemerkungen
1. Abschnitt: Zweck, Geltungsbereich und Begriffe	
Art. 1 Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.	**Antrag zu Art. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. Wenn nicht im Gesetzestext (Art. 1 oder Art. 2 Abs. 1 VE-DSG) selbst, so ist diese Klarstellung spätestens in der Botschaft unmissverständlich anzubringen.
Art. 2 Geltungsbereich 1 Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen durch: a. private Personen; b. Bundesorgane. 2 Es ist nicht anwendbar auf: a. Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden; b. Personendaten, die durch die Eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden; c. Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden; d. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007, die in der Schweiz Immunität geniessen, wie das Internationale Komitee vom Roten Kreuz. 3 Dieses Gesetz ist nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im	**Antrag zu Art. 2 Abs. 1**: Der Kreis der geschützten Personen ist nicht klar. Ausgeschlossen wird der Schutz der Persönlichkeit von juristischen Personen, nicht aber der Schutz von im Handelsregister eingetragenen Einzelunternehmen und von Mitgliedern der Personengesellschaften. Beide Kategorien sind vom Schutz auszunehmen. Weiter ist der Schutz der Persönlichkeit und der Grundrechte natürlicher Personen mit deren privaten Tätigkeiten zu verknüpfen. **Antragzu Art. 2 Abs. 2 lit. c)**: Beibehaltung des geltenden Wortlauts. Der VE will neu nur noch Daten vom DSG ausnehmen, welche die Justizbehörden des Bundes im Rahmen eines Verfahrens bearbeiten. Für die von den Prozessparteien bearbeiteten Personendaten und für die Bearbeitung durch erstinstanzliche Gerichte soll die bisherige Einschränkung nicht mehr gelten. Das ist weder sachgerecht, noch nachvollziehbar, und führt zu schwerwiegenden Konsequenzen im Zusammenhang mit der Führung von Gerichtsverfahren (Missbrauch des Auskunftsrechts zur Beschaffung von Beweismaterial, welches im Rahmen eines prozessualen Editionsbegehrens nicht herausgegeben werden müsste, etc.).

VE-DSG	Anträge und Bemerkungen
Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Für die Bearbeitung der übrigen Daten sind sie von der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ausgenommen. [4] Die Bundesversammlung und der Bundesrat sind von der Aufsicht durch den Beauftragten ausgenommen.	**Antrag zu Art. 2 Abs. 5 (neu)**: Der im Erläuterungsbericht erwähnte Allgemeincharakter des VE (*Lex Generalis*) ist in einem neuen Abs. 5 ausdrücklich vorzusehen. Es ist festzustellen, dass datenschutz- bzw. datenbearbeitungsrelevante Regelungen in kantonalen und anderen Erlassen des Bundes dem allgemeinen DSG vorgehen (*Lex Specialis*). Damit können entsprechendeEinzelhinweise im VE gestrichen werden. Solche Einzelerwähnungen sind nicht sinnvoll und gefährlich, weil diese das im Erläuterungsbericht erwähnte, selbstverständliche Wirkungsprinzip „*Lex Specialis derogat Lex Generalis*" grundsätzlich in Frage stellen. Diese generelle Klarstellung ist aber vor allem deshalb wichtig, weil das Prinzip beim Anspruch auf Information über bearbeitet Personendaten schon nach geltendem Recht immer wieder in Frage gestellt worden (Beispiel: Ein Teil der allgemeinen Datenschutz-Lehre meint unzutreffend, dass Art. 8 DSG auch im Bereich von fernmelderechtlich geschützten Personendaten anwendbar bleibt, ergo die spezifischen fernmelderechtlichen Datenschutzbestimmungen in Art. 43 bis 46 FMG und 9. Kapitel „Fernmeldegeheimnis und Datenschutz", Art. 80 ff. FDV, den Datenschutz bei der Datenherausgabe im Zusammenhang mit der Erbringung von Fernmeldediensten nicht als „Lex Specialis" abschliessend regelt.)
2. Abschnitt: Allgemeine Datenschutzbestimmungen	
Art. 3 Begriffe Die folgenden Ausdrücke bedeuten: a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; b. *betroffene Person:* natürliche Person, über die Daten bearbeitet werden; c. *besonders schützenswerte Personendaten:* 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,	**Antrag zu Art. 3 lit. c Ziff. 4**: Präzisierung des Begriffs der biometrischen Daten: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Der im Erläuterungsbericht enthaltene Hinweis, wann auch Fotos als biometrische Personendaten gelten, ist unverständlich. Es ist klarzustellen, wann Fotos als Personendaten gelten; dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biomet-

VE-DSG	Anträge und Bemerkungen
5. Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe; d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten; e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten; f. *Profiling:* jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;	rische Daten gelten. **Bemerkung zu Art. 3 lit. c Ziff. 5**: Die Bestimmung ist in dieser allgemeinen Form problematisch; etwa wenn Vermögensdelikte zur Diskussion stehen, von welchen ein künftiger Vertragspartner (z.B. Arbeitgeber) in Kenntnis gesetzt werden müsste. **Antrag zu Art. 3 lit. f)**: Beibehaltung des gegenwärtigen Begriffs des Persönlichkeitsprofils und Streichung des Wortes „Daten". Letzteres ist überflüssig und irreführend; es geht im DSG immer nur um „Personendaten". Andere Daten werden gemäss Erläuterungsbericht durch den Begriff „Personendaten" konsumiert. Der Begriff des „Profiling" ist zu unbestimmt und gefährdet damit die Rechtssicherheit mit nicht ermittelbaren Kostenfolgen für die gesamtschweizerische Wirtschaft. Angesichts der unverhältnismässigen Erschwernisse und Strafdrohungen, die der Vorentwurf mit einem allenfalls unerlaubten Profiling verknüpfen will, ist die jetzt vorgenommene Erweiterung des Begriffs gegenüber dem „Persönlichkeitsprofil" des geltenden Rechts abzulehnen. **Generelle Bemerkung zu Art. 3 lit. f)**: Die nicht reflektierte Übernahme von Begriffen des ausländischen Rechts führt dazu, dass sich die Anwendung und Auslegung von Schweizer Recht zukünftig primär an der ausländischen Rechtsprechung orientieren wird. Dies ist politisch unerwünscht und hier vor allem deshalb nicht sachgerecht, weil der Begriff des „Profiling" gegenüber dem EU-Recht sogar nicht mit einem „Swiss Finish" versehen und inhaltlich ausgeweitet wird. Die DSGVO 216/679 wendet den Begriff nur auf die automatisierte Verarbeitung von Personendaten an, der VE auf jede Bearbeitungsweise. Mit dem Begriff des "Profiling" wird der Katalog der nur unter verschärften Strafdrohungen zu bearbeitenden Daten übermässig ausgeweitet, indem offenbar jede Art von Voraussage pönalisiert werden soll. Im Ergebnis droht die Bearbeitung auch hinsichtlich von Merkmalen eingeschränkt zu werden, die unter dem geltenden DSG zu Recht weder als besonders schützenswert noch als "Persönlichkeitsprofil" qualifiziert worden sind (z.B. die wirtschaftlichen Verhältnisse und damit allenfalls auch das Zahlungsverhalten oder die Solvenz; entsprechende Daten sind vor der Inkraftsetzung des DSG ausdrücklich als nicht zur Intimsphäre gehörig bezeichnet worden, vgl. die Botschaft vom 23. März 1988, S. 446). Es wäre volkswirtschaftlich schädlich, die Bear-

VE-DSG	Anträge und Bemerkungen
	beitung solcher Informationen nur deswegen zu erschweren, weil sie theoretisch als „Voraussage" eines späteren Verhaltens interpretiert werden könnten. Die Revision schiesst hier weit über das Ziel hinaus. Beispielsweise dürfte dann auch kein Arbeitgeber mehr Prognosen über das berufliche Potential eines Arbeitnehmers erstellen, ohne alle erheblichen Verpflichtungen einzuhalten, die der VE mit dem „Profiling" verknüpft. Es gäbe zahlreiche Beispiele von sicherlich nicht beabsichtigten und unbedachten Konsequenzen in längst etablierten und von Konsumenten akzeptierten digitalisierten Wirtschaftsprozessen: Man denke nur an die Ausfertigung von Versicherungspolicen, in denen Berechnungen über das dannzumal anfallende Alterskapital enthalten sind. So etwas Selbstverständliches würde plötzlich problematisch.
g. *Bundesorgan:* Behörde und Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist;	
h. *Verantwortlicher:* Bundesorgan oder private Person, das oder die – alleine oder zusammen mit anderen – über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet;	**Antrag zu Art. 3 lit. h und i**: Beibehaltung der bisherigen Terminologie (einschliesslich der "Datensammlung"), *eventualiter* zumindest Entlassung des "Auftragsbearbeiters" aus bestimmten Pflichten. Die Abgrenzung zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" ist verschwommen und führt zu einer unklaren – teilweise unsinnigen – Aufteilung der Verantwortung und zu Doppelspurigkeiten. Zudem wird übersehen, dass der Auftragsbearbeiter die Pflichten des Verantwortlichen gar nicht in jedem Fall erfüllen *kann*. Laut Art. 16, 18 und 19 VE wäre er z.B. zur Erstellung einer Datenschutz-Folgeabschätzung (für wen?) verpflichtet, er hat für "datenschutzfreundliche Voreinstellungen" (durch den Verantwortlichen?) geradezustehen und muss Betroffene über Änderungen oder Löschungen (durch den Verantwortlichen?) informieren. Die DSGVO nimmt die Auftragsbearbeiter nicht derart in die Pflicht, ergo auch hier nicht einmal das Generalargumente der Bundesverwaltung zieht, man müsse etwas so regeln, weil es ausländisches Recht so vorgebe und man andernfalls auf eine „Blacklist" gesetzt werde. Dass „Arbeitnehmer mit einem Arbeitsvertrag" (gibt es auch Arbeitnehmer ohne Arbeitsvertrag?) nicht unter den Begriff des "Auftragsbearbeiters" fallen, steht zwar im Erläuterungsbericht. In Anbetracht der merkwürdigen Formulierung „Arbeitnehmer mit Arbeitsvertrag" wäre es aber dringend nötig, dies klar und deutlich im Gesetzestext zu normieren (Simpler Vorschlag: „Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter").
i. *Auftragsbearbeiter:* Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	

VE-DSG	Anträge und Bemerkungen
Art. 4 Grundsätze [1] Personendaten müssen rechtmässig bearbeitet werden. [2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.	**Antrag zu Art. 4 Abs. 2**: In Absatz 2 ist zu ergänzen, dass nicht nur die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und verhältnismässig zu sein hat, sondern auch die Ausübung anderer Rechte und Pflichten gemäss diesem Gesetz.
[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.	**Antrag I zu Art. 4 Abs. 3**: Streichung des Wortes "klar". Die Umformulierung ist überflüssig und schafft Rechtsunsicherheiten. So stellt sich z.B. die Frage, unter welchen Voraussetzungen der Zweck nicht nur erkennbar, sondern "klar erkennbar" ist. Der Erläuterungsbericht argumentiert, es sei mit der redaktionellen keine materielle Änderung beabsichtigt (das steht im Übrigen – beschwichtigend – an zahlreichen anderen Stellen des Erläuterungsberichts). Ein geänderter Wortlaut trägt aber immer das Risiko in sich, dass er dann in der Praxis eben auch anders ausgelegt wird. Der gleiche Vorbehalt gilt für Abs. 4 und 5. **Antrag II zu Art. 4 Abs. 3**: Im Erläuterungsbericht wird beim Beispielkatalog von nicht erkennbaren Datenbearbeitungen die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch Privatunternehmen erwähnt. Es wird dazu auf den sog. Logistep-Entscheid (BGE 136 II 508 E.4) verwiesen. Dieser Verweis und dieses Beispiel ist deplatziert, zumal das Bundesgericht in diesem Entscheid ausdrücklich festgehalten hat, seine Begründung beziehe sich auf geltendes Recht, welches durch den Gesetzgeber im Lichte der mit der Sammlung solcher IP-Adressen zusammenhängenden vertretbaren Absicht allenfalls zu korrigieren sei. Es ist unverständlich, weshalb nun gerade dieses Beispiel als „Nicht-Erkennbarkeit einer Bearbeitung von Personendaten" aufgeführt ist. Vielmehr wäre gerade vorzusehen, dass die Beschaffung von IP-Adressen zum Zwecke der Strafverfolgung von diesem Grundsatz ausdrücklich nicht erfasst wird.
[4] Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.	**Antrag zu Art. 4 Abs. 4**: Streichen, da der Grundsatz der Verhältnismässigkeit auch die Dauer der Bearbeitung/Aufbewahrung bestimmt.
[5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten.	**Antrag zu Art. 4 Abs. 5**: Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Erläuterungsberichts sind auch hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten. *Eventualiter* ist Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind" zu beschränken (Streichung des Rests).
[6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von	

VE-DSG	Anträge und Bemerkungen
besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.	Bekanntlich fängt die "Bearbeitung" schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE). Eine fortdauernde Verpflichtung zur Nachführung ist nicht erfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Selbst wenn so etwas möglich wäre, ist dieses Konzept nicht finanzierbar. **Antrag zu Art. 4 Abs. 6**: Streichung des "Profiling" und Beschränkung des Erfordernisses der "ausdrücklichen" Einwilligung auf besonders schützenswerte Personendaten. Dies insbesondere, falls die Art. 3 lit. f) vorgenommene Ausweitung des Begriffs des Persönlichkeitsprofils beibehalten werden sollte (vgl. dazu auch die Bemerkungen zu Art. 3 lit. f VE). Die im Erläuterungsbericht vertretene Ansicht, mit der vorgeschlagenen Redaktion von Abs. 6 möge die in der Lehre ausgetragene Kontroverse über die „Ausdrücklichkeit" einer Einwilligung beendet sein, ist die blosse Äusserung einer Hoffnung. Das Gegenteil wird der Fall sein und die Kontroverse verstärkt werden: Es lassen sich über die Begriffe „freiwillig", „freiwillig und eindeutig", „ausdrücklich" und die Abgrenzung zur blossen „Einwilligung" (vgl. z.B. Art. 6 Abs. 1 lit. a VE) vorzügliche juristische Publikationen schreiben.
Art. 5 Bekanntgabe ins Ausland [1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. [2] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz gewährleistet. [3] Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch: a. einen völkerrechtlichen Vertrag; b. spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde; c. standardisierte Garantien, insbesondere durch Vertrag: 1. welche der Beauftragte vorgängig genehmigt hat, oder 2. welche der Beauftragte ausgestellt oder anerkannt hat; d. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig genehmigt wurden: 1. durch den Beauftragten, oder 2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet. [4] Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 Buchstabe b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien informieren.	**Antrag zu Art. 5 Abs. 3 lit. d)**: Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG. **Antrag zu Art. 5 Abs. 4 bis 6**: Streichung der Genehmigungspflicht sowie des Auftragsbearbeiters; letzterer handelt – wie aus dem Wort ersichtlich – nach den Weisungen des Verantwortlichen, dem – wiederum entsprechend seiner

VE-DSG	Anträge und Bemerkungen
[5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht. [6] Der Verantwortliche oder der Auftragsbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit. [7] Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.	Bezeichnung – die Verantwortung für die Information des Beauftragten obliegt. **Antrag zu Art. 5 Abs. 7**: Es ist zu ergänzen, dass der Bundesrat die Liste quartalsweise aktualisieren muss und dazu ein ständiges Staaten-Monitoring etabliert. Heute ist die Liste von Staaten mit der Gewährleistung von angemessenem Schutz des EDÖB gut etabliert und ausreichend dynamisch. Wenn nun die Kompetenz zum Bundesrat hinaufgereicht wird, ist sicherzustellen, dass der Bundesrat diese sehr operative Rolle auch bedarfsgerecht wahrnehmen muss.
Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen [1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn: a. die betroffene Person im Einzelfall eingewilligt hat; b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt; c. die Bekanntgabe im Einzelfall unerlässlich ist für: 1. die Wahrung eines überwiegenden öffentlichen Interesses, oder 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde; d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; e. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; f. die Daten aus einem gesetzlich vorgesehenen Register stammen, das zugänglich ist für die Öffentlichkeit oder für Personen mit einem schutzwürdigen Interesse, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind. [2] Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.	**Antrag zu Art. 6 Abs. 1 lit. a)**: Es ist zu präzisieren, wie sich die hier ohne die Zusätze „freiwillig", „eindeutig" oder „ausdrücklich" auskommende Einwilligung gestalten lässt. **Antrag zu Art. 6 Abs. 2**: Ersatzlose Streichung der Meldepflicht, mindestens jedoch Streichung des Auftragsbearbeiters. Es ist völlig unverhältnismässig, jedes Mal eine Mitteilung an den Beauftragten senden zu müssen, wenn ein Personendatum nach Abs. 1 lit. b, c oder d ins Ausland bekanntgegeben wird. Das gilt erst recht, wenn neben dem Verantwortlichen auch noch der Auf-

VE-DSG	Anträge und Bemerkungen
	tragsbearbeiter verpflichtet werden soll. Es ist mit dieser Doppelnennung nicht klar, wer am Ende für die Erfüllung der Meldepflicht verantwortlich ist. Die Folge davon wird sein, dass sowohl der Verantwortliche, als auch der Auftragsbearbeiter Meldung erstatten müssen, um sich nicht einer Strafverfolgung auszusetzen. Die Bestimmung ist weiter auch deshalb heikel, weil solche Meldungen z.T. sensible Geschäftsinformationen betreffen (etwa Gerichtsverfahren im Ausland), die dann kraft Öffentlichkeitsgesetzen auch für Dritte einsehbar werden. Auch hier wurde offenbar in keiner Weise an den berechtigten Schutz von Geschäftsgeheimnissen gedacht.
Art. 7 Auftragsdatenbearbeitung [1] Die Bearbeitung von Personendaten kann durch Vereinbarung oder Gesetz einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. [2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters. [3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen. [4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.	s **Antrag zu Art. 7 Abs. 2**: Streichung der Kompetenz des Bundesrates, die "weiteren Pflichten" des Auftragsbearbeiters zu präzisieren. Die Pflichten des Auftragsbearbeiters ergeben sich aus den Pflichten des Verantwortlichen und des zwischen diesem und dem Auftragsbearbeiter abgeschlossenen Vertrags. **Antrag zu Art. 7 Abs. 3**: Schaffung der Möglichkeit einer generellen Einwilligung.
Art. 8 Empfehlungen der guten Praxis [1] Der Beauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen. [2] Der Verantwortliche sowie interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie. [3] Er veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.	**Antrag zu Art. 8**: Ersatzlos streichen. Im Ergebnis werden Datenbearbeiter damit völlig der Willkür des zukünftigen Beauftragten und der von diesem vordefinierten "interessierten Kreise" – erfahrungsgemäss ist die Zusammenstellung von solchen *Round Tables* „interessierter Kreise" völlig willkürlich und intransparent – ausgeliefert. Gegen die Empfehlungen des Beauftragten wird ja kein Rechtsmittel zur Verfügung stehen, diese dürften aber absehbar erhebliche Auswirkungen auf die Rechtslage haben. Es ist damit zu rechnen, dass die Gerichte die Empfehlungen des Beauftragten ihren Urteilen *tel quel* als Ermessensindikator zugrunde legen werden. Der Beauftragte wird damit im Ergebnis genau das tun, was eigentlich nicht vorgesehen ist, nämlich faktisch gemäss seinen Eindrücken Recht setzen. Dies wiegt umso schwerer, als der Beauftragte nicht einmal Jurist oder Anwalt sein oder über Erfahrungen in der Unternehmensjurisprudenz verfügen muss.
Art. 9 Einhaltung der Empfehlungen der guten Praxis [1] Befolgt der Verantwortliche die Empfehlungen der guten Praxis, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren.	**Antrag zu Art. 9**: Streichen. Dieser wird trotz Abs. 2 im Ergebnis zu einer Beweislastumkehr zu Lasten des Datenbearbeiters führen.

VE-DSG	Anträge und Bemerkungen
[2] Die Datenschutzvorschriften können auch auf andere Weise eingehalten werden, als in Empfehlungen der guten Praxis vorgesehen.	
Art. 10 Zertifizierung [1] Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen. [2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.	Keine Bemerkungen
Art. 11 Sicherheit von Personendaten [1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden. [2] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.	Keine Bemerkungen
Art. 12 Daten einer verstorbenen Person [1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und: a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder b. keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen. [2] Ein schutzwürdiges Interesse wird bei Personen vermutet, die mit der verstorbenen Person in gerader Linie verwandt sind oder mit ihr bis zum Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten.	**Antrag I zu Art. 12**: Die Bestimmung ist aus dem VE zu entfernen und die Thematik in die aktuell laufende Revision des Erbrechts zu integrieren. Derart weitreichende, thematisch in einem allgemeinen Datenschutzgesetz nicht zu erwartende Regularien als Folge des Todes gehören dorthin, wo der Tod und dessen Folgen abgewickelt werden. Das ist das allgemeine Erbrecht.Die dort zu erlassenden datenschutzrechtlichen Bestimmungen sind *lex specialis* zum DSG. Weiter ist die gesamte Bestimmung voll von schwerwiegenden Unklarheiten: Wer urteilt über das Vorliegen überwiegender Interessen der verstorbenen Person? Wer über die überwiegenden Interessen Dritter? Wie verhält sich das schutzwürdige Interesse zum überwiegenden Interesse Dritter? Weiter ist die Verknüpfung des schutzwürdigen Interesses mit Verwandtschaftsgraden unbegründet und willkürlich. Mit der Regelung von Art. 12 VE würde dem Rechtsmissbrauch Tür und Tor geöffnet. Erben wären damit z.B. in der Lage, ein Unternehmen zur Vernichtung haftpflichtrechtlich entlastender Daten zu zwingen, um danach Ansprüche geltend zu machen, zu deren Abwehr eben jene Daten erforderlich gewesen wären. Es gäbe unzählige weitere Beispiele. Art. 4 Abs. 1 lit. b) wäre mindestens zu ergänzen um einen Passus, der auch eigene Interessen des datenbearbeitenden Unternehmens vorbehält, nicht nur die des Erblassers und allfälliger Dritter. Im Übrigen wird die obligationenrechtliche Aktenaufbewahrungspflicht dem stipulierten Löschungsrecht in der Praxis häufig entgegenstehen.
[3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.	**Antrag II zu Art. 12 Abs. 3**: Die Bestimmung ist gerade umzukehren. Sie ist abzuändern, dass im Zusammenhang mit dem Vollzug dieser Bestimmung Amts- und Berufsgeheimnisse von Geheimnisträgern jederzeit geltend ge-

VE-DSG	Anträge und Bemerkungen
[4] Jeder Erbe kann verlangen, dass der Verantwortliche Personendaten des Erblassers kostenlos löscht oder vernichtet, ausser: a. der Erblasser hat dies zu Lebzeiten ausdrücklich untersagt; oder b. der Löschung oder Vernichtung stehen überwiegende Interessen des Erblassers oder von Dritten entgegen. [5] Vorbehalten bleiben spezielle Bestimmungen anderer Bundesgesetze.	macht werden können. Alles andere wäre absurd: Es gäbe zahlreiche Beispiele, die dramatische Konsequenzen zur Folge hätten. Man denke nur an den Fall, in welchem ein Mitglied einer zerstrittenen Erbengemeinschaft den Vertrauensanwalt des Verstorbenen nötigen würde, ihm Einsicht in die Personendaten zu geben, die er dann auch noch auf Geheiss vernichten müsste. **Antrag zu Art. 12 Abs. 4**: Ersatzlos streichen. Weder die DSGVO noch die Konvention 108 regeln die Bearbeitung von Daten Verstorbener. Laut Art 31 ZGB endet die Persönlichkeit mit dem Tode. Unter dem geltenden Recht muss auch der Persönlichkeitsschutz mit dem Tod enden. Sofern den Erben ein eigener Anspruch gegeben werden soll, würde das allgemeine Berichtigungs- und Löschungsrecht völlig ausreichen. **Bemerkung zu Art. 12 Abs. 5**: Es ist bezeichnend, dass genau bei dieser Bestimmung noch einmal explizit betont wird, was gemäss Art. 2 VE ohnehin generell gilt. Diese Bestimmung steht mit zahlreichen spezialgesetzlichen Regelungen komplett im Widerspruch. Insofern ist der Sinn einer solchen allgemeinen Datenschutzklausel im Zusammenhang mit Verstorbenen nicht ersichtlich.
3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters	**Vorbemerkungen**: - Es fehlt an Übergangsbestimmungen, welche regeln, wann die Beschaffung erfolgt sein muss, um die Informationspflicht gemäss Art. 13 VE auszulösen. Die Behandlung "altrechtlicher" Datenbestände ist unklar und führt über Jahre hinweg zu grossen Unsicherheiten in der Praxis. - Die Pflicht zur aktiven Information geht deutlich über das von der Konvention 108 Geforderte hinaus; diese sieht lediglich eine Auskunftspflicht vor. Letztlich wird diese Konvention – und nicht die DSGVO – den Massstab für die Angemessenheit des Datenschutzes zu liefern haben.
Art. 13 Informationspflicht bei der Beschaffung von Personendaten [1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. [2] Er teilt der betroffenen Person spätestens bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten; c. den Zweck der Bearbeitung.	**Antrag zu Art. 13 Abs. 1 und 2:** Es ist ausdrücklich vorzusehen, dass der Informationspflicht auch in genereller Weise Genüge getan werden kann, z.B. durch Publikation auf einer Webseite oder in den AGB. Im Erläuterungsbericht wird zwar festgehalten, es genüge eine solche "allgemeine Information". Das ist allerdings im Wortlaut der Bestimmung nicht ersichtlich. In der vorliegenden Form ist die Bestimmung nicht praktikabel. Datenverarbeitende Unternehmen, die keinen direkten (z.B. vertraglichen) Kontakt mit den Personen haben, deren Daten sie verarbeiten, könnten unter Berufung auf Art. 13 gezwungen werden, hunderttausende von Schreiben zu versenden, mit denen sie alle

VE-DSG	Anträge und Bemerkungen
	informieren, deren Daten sie bearbeiten. In der Telekommunikationsbranche ist dies selbst mit solchen Massenschreiben nicht möglich, weil regelmässig Personendaten bearbeitet werden, mit welchen ein Dienstanbieter nie in einem direkten Kontakt steht. Die Bestimmung ist schlicht nicht umsetzbar und schiesst über das Ziel hinaus: Selbst die insgesamt absolut ungenügende Analyse der Regulierungskostenfolgeabschätzung von PWC hält dies so fest.
[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.	**Antrag zu Art. 13 Abs. 3** Die voraussetzungslose Erweiterung des Auskunftsrechts auf alle "Empfängerinnen und Empfänger" (die Bedeutung des Wortes "oder" ist völlig unklar) ist nicht akzeptierbar. "Kategorien" muss wie bis anhin genügen. Eine detailliertere Offenlegungspflicht wäre in jedem Fall auf solche Fälle zu beschränken, in welchen persönlichkeitsverletzende Angaben (z.B. unrichtige Informationen mit schwerwiegenden Auswirkungen auf den Betroffenen) weitergegeben worden sind. Ein voraussetzungsloser Anspruch, jeden einzelnen Empfänger jeder Information zu kennen, ist abzulehnen. Ein solcher würde datenbearbeitende Unternehmen im Ergebnis ohne jede Not zur Offenlegung ihres Kundenkreises und damit ihrer Geschäftsgeheimnisse zwingen.
[4] Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die er bearbeitet, mit.	**Antrag zu Art. 13 Abs. 4**: Auch hier muss es bei den "Kategorien der Daten" bleiben. Die Kontaktdaten des Auftragsbearbeiters sind zu streichen; die Bekanntgabe kann allenfalls im Rahmen des Auskunftsrechts Sinn machen, aber nicht im Zusammenhang mit den Informationspflichten von Art. 13. VE DSG.
[5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden; werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.	**Antrag zu Art. 13 Abs. 5**: Ersatzlos streichen. *Eventualiter* ist die aktive Informationspflicht auf die Bearbeitung besonders schützenswerter Personendaten zu beschränken. Die vorgesehene uferlose Informationspflicht ist schlicht nicht umsetzbar und – selbst wenn diese umsetzbar wäre – völlig unverhältnismässig. Hinzu kommt, dass die Bestimmung sogar noch weiter geht als die DSGVO, die immerhin noch einen Monat Frist gewährt. Die Transparenzpflicht gemäss Art. 4 VE bzw. Art. 4 DSG würde völlig ausreichen. Es muss genügen, dass die Art der Datenbearbeitung auf der Homepage des Datenbearbeiters erklärt wird. Weiter muss man sich bei diesem Konzept auch die Auswirkungen auf Konsumentenseite vor Augen führen: Da in Zukunft praktisch kein Wirtschaftszweig mehr ohne die Beschaffung und Bearbeitung von Personendaten auskommen wird, wird der Konsument mit solchen Informationen regelrecht zugespamt werden. Die einzelne Information versinkt im Informationsmeer. Der Adressat wird abgestumpft und negiert die diesem Informationswahn zu Grunde gelegten Absichten, den Adressaten vor „bösen" Datenbearbeitern zu schützen.

VE-DSG	Anträge und Bemerkungen
Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen [1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt.	**Bemerkung**: Wurde unnötigerweise enger als die SEV 108 gefasst. **Antrag zu Art. 14 Abs. 1:** Ergänzung um den Fall, dass eine Datenbearbeitung zur Rechtsdurchsetzung erforderlich ist (z.B. im Rahmen der Prozessvorbereitung), in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist.
[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn: a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.	**Antrag zu Art. 14 Abs. 2**: 1. Erweiterung des Ausnahmenkatalogs um den Fall, dass keine besonders schützenswerte Personendaten bearbeitet werden. Die Bestimmung des VE entspricht weitgehend Art. 9 des bestehenden Rechts (Ausnahmen von der Auskunftspflicht). Dort geht es jedoch um Abwägungen im Einzelfall, also um eine völlig andere Ausgangslage als bei der (generellen) Informationspflicht. Die Ausnahmen von dieser Informationspflicht müssten schon angesichts der drakonischen Strafen, die der VE für bezügliche Verstösse vorsieht, deutlich weiter gefasst und klarer formuliert werden.
[3] Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn: a. ein Gesetz im formellen Sinn dies vorsieht; oder b. dies aufgrund überwiegender Interessen Dritter erforderlich ist.	
[4] Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten: a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt; b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls eine der folgenden Voraussetzungen erfüllt ist: 1. es ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich; oder 2. die Übermittlung der Information stellt den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage. **II.** [5]Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.	**Antrag zu Art. 14 Abs. 4 lit. a**: Streichung des Kriteriums der fehlenden Weitergabe von Personendaten an Dritte. Auch hier würde die Weitergabe von Daten innerhalb eines Konzerns (der als Dritter gilt) unnötig erschwert.
Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung [1] Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.	**Antrag zu Art. 15 Abs. 1**: Streichen. *Eventualiter* ist die Bestimmung um die Beschränkungen gemäss Art. 22 Abs. 2 lit. a DSGVO EU (2016/679) zu ergänzen; weiter wäre ausdrücklich zu vermerken, dass es sich um "negative" rechtliche Wirkungen handeln muss. Art. 15 erscheint insgesamt als untauglicher Versuch, Konsumenten vor jeder Art automatisiert getroffener Entschei-

VE-DSG	Anträge und Bemerkungen
	dungen zu "schützen", die sich irgendwie auf sie auswirken könnten (eine "rechtliche Wirkung" wird ja fast immer in irgend einer Weise argumentierbar sein, und was eine "erhebliche" Auswirkung ist, dürfte letztlich von der Sensibilität des Betroffenen abhängen). Es besteht kein Grund zur Annahme, dass solche Entscheidungen per se gravierender sein müssen als von Menschen mitgetroffene oder überwachte. Die saloppe Begründung im Erläuterungsbericht „denn solche Entscheidungen sind in allen Wirtschaftsbereichen immer häufiger und werden teilweise auf der Grundlage falscher Daten getroffen" reicht jedenfalls nicht aus, einer solchen weitreichenden Bestimmung ein öffentliches Interesse mitzugeben. Art. 22 DSGVO nimmt im Gegensatz zum VE den Vertragsschluss und die Vertragserfüllung ausdrücklich von der Informationspflicht aus und behält erst noch abweichendes Recht von Mitgliedstaaten vor. Eine von der DSGVO abweichende Regelung wäre demnach zweifellos auch für die Schweiz zulässig. Es ist nicht nachvollziehbar, weshalb hier ein „Swiss Finish" erfolgt. Der Entscheid über einen Vertragsschluss ist unter der geltenden Rechtsordnung seit der Gründung des Bundesstaates frei und muss dies auch bleiben. Es gibt in keinem anderen Gebiet des Privatrechts eine generelle Begründungspflicht für den Nichtabschluss eines Vertrages. Das hat nichts damit zu tun, ob die Grundlage für einen solchen Entscheid aus Papier, aus Menschen oder aus Algorithmen stammt.
[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.	**Antrag zu Art. 15 Abs. 2**: Streichen. Wird trotz offensichtlich fehlender internationaler Verpflichtung an dieser Vorschrift festgehalten, droht im Ergebnis ein völlig unverhältnismässiger Aufwand für die gesamte Schweizer Wirtschaft. Dies ist nicht nur unverhältnismässig, sondern gefährdet auch in hohem Mass Geschäftsgeheimnisse des datenbearbeitenden Unternehmens.
[3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.	**Antrag zu Art. 15 Abs. 3**: Streichen. Es ist nicht nachvollziehbar, weshalb gerade der Staat automatisierte Entscheidungen ohne Informations- und Anhörungspflicht durchführen darf. Das Handeln des Staates ist an die Einhaltung von Grundrechten geknüpft. Diese Bestimmung zeugt von einem sehr gefährlichen Grundverständnis der Gesetzesredaktoren: Hier der gute Staat, dort die böse Wirtschaft. Es ist daran zu erinnern, dass solche Ausnahmen für staatliches Handeln vor allem Mittel totalitärer Staaten sind, sich für nichts rechtfertigen zu müssen.
Art. 16 Datenschutz-Folgenabschätzung [1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen.	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschätzungen bei jeder beliebigen Datenbearbeitung vornehmen zu müssen; abgesehen davon muss die Abschätzung ohnehin durchgeführt werden, um he-

VE-DSG	Anträge und Bemerkungen
[2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern. [3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen. [4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit.	rauszufinden, ob die Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit führt. Die Kosten sind angefallen, selbst wenn man zum Schluss käme, dass gar keine Risiken bestehen. Hier wird ein bürokratisches Monstrum freigesetzt, das in der Privatwirtschaft im Ergebnis nichts ausser gigantischen Kosten bringen wird. Mit dieser "Folgeabschätzung" wird kein einziger Missbrauch verhindert, die betroffenen Unternehmen werden aber ungeheuer viel Papier, Zeit und Geld dafür aufwenden müssen. Denn anders als der Bund, der – wie im vorliegenden Fall – meint, mit wenig Geld eine verfassungskonforme Regulierungskostenfolgenabschätzung machen zu können, hat der private Datenbearbeiter mit seiner Existenz gerade zu stehen, wenn er einer solchen Verpflichtung nicht im Sinne des Gesetzes nachkommen sollte. **Antrag zu Art. 16 Abs. 3 und 4**: Die Pflicht, diese Folgenabschätzung und die Massnahmen dem Beauftragten vorzulegen und das Vetorecht sind in jedem Fall zu streichen. Die 3 Monatsfrist ist weiter viel zu lang und zeugt nicht von einem Verständnis wirtschaftlicher Prozesse. Wenn es bei solchen Folgeabschätzungen Beanstandungen gibt, dann hat der Beauftragte Einwände innert 7 Tagen zu adressieren, ansonsten Geschäftsprozesse während Monaten blockiert bleiben müssen. Wir weisen dazu auch darauf hin, dass allein die Überprüfung der zu erwartenden Schwemme solcher Meldungen, ein Herr von neuen Beamten erforderlich machen wird, die nichts anderes tun, als solche Folgeabschätzungen zu prüfen.
Art. 17 Meldung von Verletzungen des Datenschutzes [1] Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.	**Antrag zu Art. 17**: Streichen. Die Schweiz will auch hier weit über die DSGVO hinausgehen. Dort wird die Selbstanzeige nur gefordert, falls Schutzmassnahmen versagt haben und daraus ein Sicherheitsrisiko entsteht (Art. 33 DSGVO i.V. mit Ziff. 85ff. der Erwägungen). Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien unseres Rechtsstaates. Es ist nicht zu rechtfertigen, dass diese Garantie gerade im Datenschutzrecht nicht mehr gewährleistet werden soll; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer Flut von Selbstanzeigen zu rechnen, die erneut nur den Apparat des Beauftragten übermässig aufblähen würde. Diese aus den USA bekannten Regulierungsmechanismen sollten in der Schweiz nicht angefasst werden. Der Druck auf die Verantwortlichen wäre enorm und

VE-DSG	Anträge und Bemerkungen
[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. [3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten. [4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung.	würde ein pragmatisches und/oder vernunftgetriebenes Handeln von vornherein ausschliessen. Die Selbstanzeige ist in einem solchen System immer die sicherste Art, sich prophylaktisch „compliant" zu verhalten. **Antrag zu Art. 17 Abs. 2**: Streichung; In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen. **Bemerkung zu Art. 17 Abs. 4**: Vgl. den Antrag zu Art. 14 Abs. 3 und 4
Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen [1] Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. [2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.	**Antrag zu Art. 18**: Streichung. Die Bestimmung ist redundant. Der Bearbeiter ist unter dem DSG schon durch die Grundsätze der Datenrichtigkeit, der Zweckbindung und der Verhältnismässigkeit verpflichtet, eine Lösung anzustreben, die die Rechtsstellung von Betroffenen möglichst wenig tangiert. Dasselbe gilt für die Pflicht, angemessene technische Sicherheitsmassnahmen zu treffen.
Art. 19 Weitere Pflichten Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie dokumentieren ihre Datenbearbeitung; b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.	**Antrag zu Art. 19**: Streichung; Die Bestimmung ist nicht nur überflüssig, sondern teilweise nicht umsetzbar. Die stipulierte Dokumentationspflicht würde insbesondere für KMU zu einem völlig unverhältnismässigen Aufwand führen und gegenüber der bereits bestehenden Pflicht zur Aktenaufbewahrung keinen Mehrwert bringen. Die Informationspflicht gemäss lit. b ist von vornherein nicht umsetzbar. Teilweise lassen sich dagegen auch absurde Beispiele vorbringen: Es kann ja z.B. nicht sein, dass Adresswechsel einer betroffenen Person zuerst aktiv recherchiert und dann allen mitgeteilt werden muss, die sich je nach der Adresse erkundigt haben! Schliesslich scheint es überzogen, sämtlichen Empfängern von Informationen Mitteilung über eine allfällige Verletzung von Datenschutzgrundsätzen oder über "Einschränkungen" der Datenbearbeitung gemäss Art. 25 machen zu müssen. Auch diese Bestimmung bewirkt nichts, ausser Rechtsunsicherheit zu schaffen und droht Jahr für Jahr allein in der Schweiz Millionen unnötiger Mitteilungen auszulösen. Auch hier gilt es, sich auch in die Situation der Informationsadressaten zu versetzen. Dass Millionen unnützer Mitteilungen versandt werden ist das eine; dass aber jeder Einzelne tausende solcher Informationen von allen Datenbearbeitern erhält, das andere. Diese Informationen sind die neuen „Spam Waves" und werden bei den Adressaten keinerlei Wirkung erzielen, geschweige denn, diese in ihren Persönlichkeiten schützen.

VE-DSG	Anträge und Bemerkungen
4. Abschnitt: Rechte der betroffenen Person	
Art. 20 Auskunftsrecht [1] Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. [2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt: a. die Identität und die Kontaktdaten des Verantwortlichen; b. die bearbeiteten Personendaten; c. der Zweck der Bearbeitung; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer; e. das Vorliegen einer automatisierten Einzelentscheidung; f. die verfügbaren Angaben über die Herkunft der Personendaten; g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4. [3] Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.	**Antrag zu Art. 20 Abs. 2 lit e)**: Streichen; in der Regel ist dies für den Betroffenen ohne weiteres ersichtlich(vgl. auch den Antrag zu Art. 15). **Antrag zu Art. 20 Abs. 2 lit. f)**: Streichen; die Pflicht zur Bekanntgabe der jeweiligen Datenherkunft führt in vielen Fällen zu einem Zwang, Geschäftsgeheimnisse bekanntgeben zu müssen, oder sie tangiert schützenswerte Interessen Dritter. Die Bekanntgabepflicht ist zumindest unter den Vorbehalt des Schutzes überwiegender Interessen Dritter und von Geschäftsgeheimnissen zu stellen. **Antrag zu Art. 20 Abs. 3**: Streichen; *eventualiter* ist Abs. 3 auf die Pflicht zu beschränken, den Betroffenen über den Entscheid zu informieren. In aller Regel wird dieser allerdings sowieso mitgeteilt: Entweder wird ein Vertrag geschlossen oder eben nicht. Eine Verpflichtung zur Offenlegung des "Zustandekommens" eines Entscheids würde wiederum darauf hinauslaufen, eine Begründungspflicht für den Nicht-Abschluss von Verträgen über das Datenschutzrecht einzuführen. Das kann nicht das Ziel des Datenschutzes sein. Die Verweigerung von Geschäftsbeziehungen ist ausschliesslich ein wettbewerbs- und lauterkeitsrechtlicher Tatbestand. Es ist lebensfremd, wenn man heute meint, allein durch eine modernere Datenbearbeitung würden Fehler bei der Einschätzung von geschäftlichen Tätigkeiten verursacht. Die Frage, ob zwei Personen miteinander kontrahieren, basierte seit jeher auf der Einschätzung von „Personendaten" und „Persönlichkeitsprofilen". Es kam bislang niemand auf die Idee, im allgemeinen oder im besonderen Teil des OR eine Begründungspflicht für den Nicht-Abschluss eines Vertrages zu fordern. Vielfach wird

VE-DSG	Anträge und Bemerkungen
[4] Personendaten über die Gesundheit können der betroffenen Person durch einen von ihr bezeichneten Arzt mitgeteilt werden. [5] Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat. [6] Niemand kann im Voraus auf das Auskunftsrecht verzichten.	gerade deshalb kein Vertrag geschlossen, weil die persönliche Chemie nicht stimmt. In den seltenen Fällen wird dies der anderen Seite so direkt mitgeteilt. Wieso es weiter für den Schutz der Persönlichkeit erforderlich sein soll, dem Betroffenen die Auswirkungen eines Nicht-Entscheids zu erläutern, ist völlig unerfindlich, wenn nicht gleichzeitig eine Rechtsmittelmöglichkeit besteht, die am Ende in einen Vertragszwang münden könnte. Beides wird zum Glück und konsequenterweise (jedoch im Kontext aller anderen Ideen fast schon überraschend) nicht gefordert.
Art. 21 Einschränkung des Auskunftsrechts [1] Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben. [2] Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.	Keine Bemerkungen
Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende [1] Werden Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben: a. Die Daten geben Aufschluss über die Informationsquellen; b. Es müsste dafür Einsicht in Entwürfe für Publikationen gewährt werden; c. Die freie Meinungsbildung des Publikums würde gefährdet. [2] Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.	Keine Bemerkungen
5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen	
Art. 23 Persönlichkeitsverletzungen [1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. [2] Eine Persönlichkeitsverletzung liegt insbesondere vor: a. wenn Personendaten entgegen den Grundsätzen nach den Artikeln 4-6 und 11 bearbeitet werden; b. wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden;	

VE-DSG	Anträge und Bemerkungen
c. wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden; d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person. [3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	**Antrag zu Art. 23 Abs. 2 lit d)**: Streichung; zum Profiling vgl. Bemerkungen zu Art. 3 lit. f VE. **Bemerkung zu Art. 23 Abs. 3**: Streichung des zweiten Teils „und eine Bearbeitung nicht ausdrücklich untersagt hat". Was einmal allgemein zugänglich gemacht worden ist, kann später nicht mehr widerrufen werden.
Art. 24 Rechtfertigungsgründe [1] Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. [2] Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere:	**Antrag I zu Art. 24 Abs. 2, erster Satz**: Beibehaltung des bisherigen Wortlauts. Im DSG lautet die Formulierung "wird vermutet". Der vorgeschlagene Text schafft nur eine zusätzliche Rechtunsicherheit.
a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet;	**Antrag II zu Art. 24 Abs. 2. lit a)**: Das Wort "unmittelbar" ist zu streichen. Der "unmittelbare" Zusammenhang stellt eine zu starke Einschränkung dar und wirft Abgrenzungsfragen auf, für welche der VE keine Antworten liefert.
b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben; c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn: 1. es sich dabei nicht um besonders schützenswerte Personendaten handelt, 2. Dritten nur Daten bekanntgegeben werden, welche diese für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen, 3. die betroffene Person volljährig ist;	**Antrag zu Art. 24 Abs. 2 lit. c) Ziff. 3**: Streichen. Die Volljährigkeit ist häufig weder bekannt noch eruierbar (Amtsstellen erteilen über das Geburtsdatum einer Person schon heute nicht oder nur zurückhaltend Auskunft). Solange selbst Identifikationsdaten von Behörden als geheim behandelt werden und es zudem an einem Personenidentifikator fehlt, ist häufig schon die Identität des von einer Datenbearbeitung Betroffenen nicht mit Sicherheit bestimmbar.
d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet; e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet, soweit: 1. die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt, 2. Dritten besonders schützenswerte Personendaten so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind, 3. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind; f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das	

VE-DSG	Anträge und Bemerkungen
Wirken dieser Person in der Öffentlichkeit beziehen.	
Art. 25 Rechtsansprüche [1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs. Die klagende Partei kann insbesondere verlangen, dass: a. die Datenbearbeitung verboten wird; b. die Bekanntgabe von Personendaten an Dritte untersagt wird; c. Personendaten berichtigt, gelöscht oder vernichtet werden. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die klagende Partei verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird. Sie kann darüber hinaus verlangen, dass die Bearbeitung der bestrittenen Daten eingeschränkt wird. [3] Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.	**Antrag Art. 25 lit. a) bis c)**: Es müsste klargestellt werden, dass eine "bestimmte" Datenverarbeitung verboten werden kann, und dass "bestimmte" Daten nicht mehr bearbeitet und/oder bekanntgegeben werden dürfen, etc. Ansonsten kann die Bestimmung nicht umgesetzt werden. **Antrag Art. 25 Ziff. 2**: Streichung der Pflicht zur Anbringung eines "Bestreitungsvermerks", *eventualiter* Aufnahme einer Verpflichtung zur Anbringung eines Hinweises, es handle sich bei einer bestimmten Behauptung um eine Einschätzung des Datenbearbeiters. Abs. 2 lässt in der Praxis schiefe Ergebnisse erwarten. Vor allem ist völlig unklar, was man sich unter einer "eingeschränkten" Datenbearbeitung vorzustellen hat. **Antrag Art. 25 Ziff. 3**: Ziff. 3. streichen. Lit. a) bis c) reichen völlig, um die Interessen der Betroffenen zu wahren. Auch die DGSVO sieht keine Mitteilung von Urteilen an Dritte vor.
6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane	
Art. 26 Verantwortliches Organ und Kontrolle [1] Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt. [2] Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.	Keine Bemerkungen
Art. 27 Rechtsgrundlagen [1] Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. [2] Für die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Eine Grundlage in einem Gesetz im materiellen Sinn ist ausreichend, wenn die folgenden Voraussetzungen erfüllt sind: a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn klar festgelegte Aufgabe unentbehrlich; und b. Die Bearbeitung birgt für die Persönlichkeit und die Grundrechte der betroffenen Person keine besonderen Risiken. [3] In Abweichung von den Absätzen 1 und 2 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Der Bundesrat bewilligt die Bearbeitung, sofern die Rechte der betroffenen Person nicht gefährdet	**Antrag zu Art. 15 Abs. 2**: Streichen „oder den Erlass einer automatisierten Einzelfallentscheidungen nach Artikel Art. 15 Absatz 1" (vgl. dazu den Kommentar zu Art. 15 Abs. 2): Damit würde jede Prozessautomatisierung und -optimierung in der Verwaltung massiv erschwert. Es stellt sich grundsätzlich auch die Frage, ob als Grundlage für die Datenbearbeitung nicht auch Regelungen auf Verordnungsstufe ausreichen sollten.

VE-DSG	Anträge und Bemerkungen
sind; b. Die betroffene Person hat in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt; c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.	
Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen [1] Der Bundesrat kann vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling bewilligen, wenn: a. die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz im formellen Sinn geregelt sind; b. ausreichende Massnahmen getroffen werden, um eine Verletzung der Grundrechte der betroffenen Person zu verhindern; und c. eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, zwingend erforderlich ist. [2] Er holt vorgängig die Stellungnahme des Beauftragten ein. [3] Das zuständige Bundesorgan legt dem Bundesrat spätestens innerhalb von zwei Jahren nach Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor. [4] Die automatisierte Datenbearbeitung oder das Profiling müssen in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage umfasst.	**Antrag zu Art. 28 Abs. 1 und 2**: Die Bestimmung ist entweder zu streichen, oder die entsprechenden Möglichkeiten ist auch Privaten zu eröffnen.
Art. 29 Bekanntgabe von Personendaten [1] Bundesorgane dürfen Personendaten bekannt geben, wenn eine Rechtsgrundlage im Sinne von Artikel 27 Absätze 1 und 2 dies vorsieht. [2] In Abweichung von Absatz 1 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten bekannt geben, wenn eine der folgenden Voraussetzungen erfüllt ist: a. Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich; b. Die betroffene Person hat in die Bekanntgabe eingewilligt; c. Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen; d. Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt; e. Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit ei-	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
nem unverhältnismässigen Aufwand zu erreichen. [3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004 auch Personendaten bekannt geben, wenn: a. die betreffenden Daten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen; und b. an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht. [4] Name, Vorname, Adresse und Geburtsdatum einer Person dürfen Bundesorgane auf Anfrage auch bekannt geben, wenn die Voraussetzungen von Absatz 1 oder 2 nicht erfüllt sind. [5] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 3 bekannt geben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst gelöscht. [6] Sie lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn: a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.	
Art. 30 Widerspruch gegen die Bekanntgabe von Personendaten [1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen. [2] Das Bundesorgan weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist: a. es besteht eine Rechtspflicht zur Bekanntgabe; b. die Erfüllung seiner Aufgabe wäre sonst gefährdet. [3] Artikel 29 Absatz 3 bleibt vorbehalten.	Keine Bemerkungen
Art. 31 Angebot von Unterlagen an das Bundesarchiv [1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen. [2] Sie vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese: a. anonymisiert sind; b. zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.	Keine Bemerkungen
Art. 32 Datenbearbeitung für Forschung, Planung und Statistik [1] Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn:	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
a. die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt; b. das Bundesorgan privaten Personen besonders schützenswerte Personendaten so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind; c. die Empfängerin oder der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und d. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind. [2] Die Artikel 4 Absatz 3, 27 Absätze 1 und 2 sowie Artikel 29 Absatz 1 sind nicht anwendbar.	
Art. 33 Privatrechtliche Tätigkeit von Bundesorganen [1] Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen. [2] Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.	Keine Bemerkungen
Art. 34 Ansprüche und Verfahren [1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es: a. die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt; b. die Folgen einer widerrechtlichen Bearbeitung beseitigt; c. die Widerrechtlichkeit der Bearbeitung feststellt. [2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so muss das Bundesorgan bei den Daten einen Bestreitungsvermerk anbringen und deren Bearbeitung einschränken. [3] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan: a. die betreffenden Personendaten berichtigt, löscht oder vernichtet; b. seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, das Verbot der Bearbeitung, den Widerspruch gegen die Bekanntgabe nach Artikel 30 oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht. [4] Die Berichtigung, Löschung oder Vernichtung von Personendaten kann nicht verlangt werden in Bezug auf die Bestände öffentlich zugänglicher Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderer öffentlicher Gedächtnisinstitutionen. Wenn die Gesuchstellerin oder der Gesuchsteller ein überwiegendes Interesse nachweisen kann, kann sie oder er jedoch verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt. [5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.	Keine Bemerkungen
Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Öffentlichkeitsgesetzes hängig, so kann die betroffene Person im Rahmen dieses Verfahrens diejenigen Rechte geltend machen, die ihr nach Artikel 34 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.	Keine Bemerkungen
Art. 36 Register [1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[2] Der Beauftragte führt ein Register der Datenbearbeitungstätigkeiten. Das Register ist öffentlich. [3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.	
7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte	
Art. 37 Ernennung und Stellung [1] Die oder der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen.	**Antrag zu Art. 37 Abs. 1**: Dem Bundesrat soll ein Vorschlagsrecht zukommen und die Wahl soll durch das Parlament erfolgen. Formulierungsvorschlag: "Die oder der Beauftragte wird vom Bundesrat zur Wahl vorgeschlagen und vom Parlament für eine Amtsdauer von 4 Jahren gewählt". Was die blosse Genehmigung einer Wahl bringen soll, ist nicht ersichtlich. Die Person des Beauftragten soll über grosse Kompetenzen und einen Wirkungsgrad mit erheblichen finanziellen Auswirkungen auf die Schweizer Wirtschaft verfügen. In Anbetracht des zukünftigen, angedachten Gewichts dieses Posten, ist eine Wahl durch das Parlament gerechtfertigt.
[2] Das Arbeitsverhältnis der oder des Beauftragten richtet sich, soweit dieses Gesetz nichts anderes vorsieht, nach dem Bundespersonalgesetz vom 24. März 2000 (BPG). [3] Die oder der Beauftragte übt ihre bzw. seine Funktion unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder zu erhalten. Sie oder er ist administrativ der Bundeskanzlei zugeordnet. [4] Sie oder er verfügt über ein ständiges Sekretariat und ein eigenes Budget. Sie oder er stellt sein Personal an. [5] Die oder der Beauftragte unterstehen nicht dem Beurteilungssystem nach Artikel 4 Absatz 3 BPG.	**Antrag zu Art. 37 Abs. 4**: Das Budget wird durch das Parlament genehmigt.
Art. 38 Wiederwahl und Beendigung der Amtsdauer [1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden. [2] Verfügt der Bundesrat nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl, so ist der oder die Beauftragte für eine neue Amtsdauer wiedergewählt. [3] Die oder der Beauftragte kann den Bundesrat unter Einhaltung einer Frist von sechs Monaten um Entlassung auf ein Monatsende ersuchen. [4] Der Bundesrat kann die Beauftragte oder den Beauftragten vor Ablauf der Amtsdauer des Amtes entheben, wenn diese oder dieser: a. vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder b. die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.	**Antrag zu Art. 38 Abs. 2**: Der oder die Beauftragte ist für jede Amtsperiode neu zu wählen. Das Verfahren über eine Verfügung kommt einem Kündigungsverfahren gleich, das in der Praxis nur aus wichtigen Gründen möglich ist. Das Wahlorgan soll in seiner Wahl wirklich frei sein.
Art. 39 Nebenbeschäftigung [1] Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, der Verwaltung, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein. [2] Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1	**Antrag zu Art. 39 Abs. 2**: Solche Bewilligungen von Nebenbeschäftigung sind

VE-DSG	Anträge und Bemerkungen
auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.	offenzulegen. Für die Vermeidung von Interessenkonflikten ist absolute Transparenz unabdingbar.
Art. 40 Aufsicht 1 Der Beauftragte überwacht die Einhaltung der Datenschutzvorschriften des Bundes. 2 Bundesverwaltungsbehörden, die nach einem anderen Bundesgesetz Private oder Organisationen ausserhalb der Bundesverwaltung beaufsichtigen, laden den Beauftragten zur Stellungnahme ein, bevor sie eine Verfügung treffen, die Fragen des Datenschutzes berührt. 3 Führt der Beauftragte gegen die gleiche Partei ein eigenes Verfahren, so haben die beiden Behörden ihre Verfahren zu koordinieren.	Keine Bemerkungen.
Art. 41 Untersuchung 1 Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. 2 Das Bundesorgan oder die private Person erteilt dem Beauftragten die von ihm verlangten Auskünfte und stellen ihm alle für die Untersuchung notwendigen Unterlagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes.	**Antrag zu Art. 41 Abs. 2**: Hier ist zu ergänzen, dass bei Untersuchungen gegen Private alle Untersuchungsakten nicht dem Öffentlichkeitsgesetz unterliegen, da ansonsten über diesen Umweg Betriebsgeheimnisse an Dritte gelangen könnten. Wenn Unternehmen verpflichtet sind, dem Beauftragten alle notwendigen Unterlagen zur Verfügung zu stellen, muss es die Garantie haben, dass diese nicht veröffentlicht werden. Der Beauftragte veröffentlicht bei Untersuchungen gegen private Personen nur die Empfehlung.
3 Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte vergeblich versucht, Auskünfte und Unterlagen einzuholen, so kann der Beauftragte im Rahmen einer Untersuchung: a. ohne Vorankündigung Räumlichkeiten inspizieren; b. Zugang zu allen notwendigen Daten und Informationen verlangen.	**Antrag zur Art. 41 Abs. 3**: Diese Bestimmung ist nur akzeptabel, wenn das Unternehmen Rechtsmittel gegen die Auskunftsverfügung hat. Eine unbestimmte Verletzung von Mitwirkungspflichten darf nicht zu Strafsanktionen oder publizitätswirksamen Aktionen des Beauftragten gegen Unternehmen führen. Bevor solche Massnahmen ergriffen werden, muss eine Editionsverfügung des Beauftragten einer gerichtlichen Überprüfung zugänglich sein.
4 Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten.	**Antrag zu Art. 41 Abs. 4**: Streichen „private Personen". Ein Tätigwerden des Beauftragten gegenüber Privaten ohne Anzeige einer Datenschutzverletzung ist strikt abzulehnen. Wenn Anhaltspunkte vorliegen, kann der Beauftragte nach Art. 41 Abs. 1 formell vorgehen. Es dürfen hier keine mehrgleisigen Verfahren ohne Rechtsschutz für die betroffenen Parteien eingefügt werden. Im Gegenteil, es müsste für Unternehmen möglich sein, Sachverhalte rechtsverbindlich durch den Beauftragten überprüfen und mittels Attest der Datenrechtskonformität genehmigen zu lassen.
5 Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung.	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Parteistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte

VE-DSG	Anträge und Bemerkungen
	Abs. 5 auch gestrichen werden.
Art. 42 Vorsorgliche Massnahmen [1] Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern. [2] Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.	**Antrag zu Art. 42 Abs. 1**: Ändern: Der Beauftragte kann beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen. Vorsorgliche Massnahmen sind – auch im Persönlichkeitsschutz –immer Sache der Gerichte. Hier ist die bisherige Regelung mit dem Antrag beim Präsidenten der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts beizubehalten. Es sollte hier nicht von den bewährten rechtsstaatlichen Prozessen abgewichen werden. Jedenfalls gibt es dazu keine ausreichenden Rechtfertigungsgründe.
Art. 43 Verwaltungsmassnahmen [1] Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden. [2] Der Beauftragte kann zudem die Bekanntgabe ins Ausland aufschieben oder untersagen, wenn sie gegen die Voraussetzungen nach Artikel 5 oder 6 oder gegen spezifische Bestimmungen betreffend die Bekanntgabe von Personendaten ins Ausland in anderen Bundesgesetzen, verstösst.	**Antrag zu Art 43 Abs. 1**: Ändern: Anstelle der Empfehlung und des nachfolgenden Gerichtswegs wie im heutigen Recht wird hier auch die Klage- und Beweislast umgekehrt. Das ist abzulehnen. Der Beauftragte hat in der Verfügung die Rechtsverletzung nachzuweisen. Eine Verfügung sollte nur nach der Durchführung einer Untersuchung zulässig sein, in welchem dem betroffenen Datenbearbeiter selbstverständlich auch das rechtliche Gehör gewährt wurde. Eine Datenvernichtung darf nicht durch den Beauftragten angeordnet werden können, da dies nicht wieder gutzumachende Folgen hat (Vernichtung von Daten ist endgültig, ausserdem sind Konflikte mit der Aktenaufbewahrungspflicht absehbar). Derartige Eingriffe in die Rechtsstellung der Datenbearbeiter müssen unabhängigen Gerichten überlassen werden. Art. 41 reicht zum Schutz Betroffener völlig aus.
Art. 44 Verfahren [1] Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz. [2] Partei sind lediglich das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wurde.	**Antrag zu Art. 44 Abs. 2**: Drittpersonen haben keine Parteistellung und kein Akteneinsichtsrecht, was zu begrüssen ist. Zu ergänzen ist weiter, dass Untersuchungsunterlagen nicht dem Öffentlichkeitsgesetz unterliegen dürfen.

VE-DSG	Anträge und Bemerkungen
[3] Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt keine aufschiebende Wirkung zu. [4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.	**Antrag zu Art. 44 Abs. 3**: Der generelle Entzug der aufschiebenden Wirkung ist unverhältnismässig. Vielmehr wäre vorzusehen, dass die aufschiebende Wirkung auf Antrag durch ein Gericht entzogen werden kann. Die Vorschrift zeitigt nicht praktikable Folgen, z.B. wenn der Beauftragte die Löschung von Daten verfügt, deren Bearbeitung durch ein Gericht dann als zulässig beurteilt wird, oder dgl.
Art. 45 Anzeigepflicht Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.	**Antrag zu Art. 45**: Streichen. Ein Recht zur Anzeige würde völlig genügen. Wir weisen erneut auf die untragbaren Folgen der Pflicht zur Selbstanzeige hin (Art. 17 VE).
Art. 46 Amtshilfe zwischen schweizerischen Behörden [1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses Gesetzes erforderlich sind. [2] Der Beauftragte gibt den folgenden Behörden die Informationen und Personendaten bekannt, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind: a. den für den Datenschutz zuständigen kantonalen Behörden; b. den zuständigen Strafverfolgungsbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 45 geht; c. den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss Artikel 41 Absatz 3, 42 und 43.	**Antrag zu Art. 46 Abs. 2**: Hier ist zu ergänzen, dass Informationen die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen.
Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden [1] Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen: a. die Identität des Verantwortlichen, des Auftragsbearbeiters oder anderer beteiligter Dritter; b. Kategorien von betroffenen Personen; c. die Identität der betroffenen Personen, falls: 1. die betroffenen Personen eingewilligt haben, oder 2. die Mitteilung der Identität der betroffenen Personen unumgänglich ist, um die gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde zu erfüllen; d. bearbeitete Personendaten oder Kategorien von bearbeiteten Personendaten; e. den Zweck der Datenbearbeitung; f. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern; g. technische und organisatorische Massnahmen. [2] Der Beauftragte kann der ausländischen Behörde Amtshilfe gewähren und ihr die Informationen ge-	**Antrag zu Art. 47 Abs. 1**: Auch hier ist zu ergänzen, dass Informationen, die in Untersuchungsverfahren als vertrauliche Unternehmensinformationen bezeichnet wurden, im Rahmen der Amtshilfe nicht weitergegeben werden dürfen. Eine solche Bestimmung ist notwendig, um die Geschäftsgeheimnisse der Unternehmen genügend zu schützen, insbesondere auch für Informationen, die in der Schweiz dem Berufsgeheimnis unterliegen. Die Herausgabe vertraulicher Unternehmensdaten darf nicht im Ermessen des Beauftragten liegen, sondern – wenn überhaupt – nur mit Zustimmung des betroffenen Unternehmens zulässig sein.

VE-DSG	Anträge und Bemerkungen
mäss Absatz 1 zur Verfügung stellen, wenn sie folgende Voraussetzungen erfüllt: a. Sie verpflichtet sich, die zur Verfügung gestellten Informationen und Personendaten, nicht für andere Zwecke zu verwenden, als im Amtshilfegesuch angegeben; b. Sie verpflichtet sich, ähnlichen Amtshilfegesuchen der Schweiz Folge zu leisten; c. Sie verpflichtet sich zur Wahrung des Amts- und Berufsgeheimnisses; d. Sie verpflichtet sich, die erhaltenen Informationen und Personendaten nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln; e. Sie verpflichtet sich, die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten.	
Art. 48 Information [1] Der Beauftragte erstattet der Bundesversammlung periodisch sowie bei Bedarf Bericht. Er übermittelt den Bericht gleichzeitig dem Bundesrat. Die periodischen Berichte werden veröffentlicht. [2] In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über seine Feststellungen und Verfügungen.	**Antrag zu Art. 48 Abs. 2**: Streichen des Begriffs „seine Feststellungen und Verfügungen" und ersetzen mit „seine Untersuchungen". Damit der Beauftragte die Persönlichkeitsrechte wahrt, soll er nur über die Tatsache einerUntersuchung informieren. Es ist nicht ersichtlich, weshalb der Beauftragte zur Profilierung von Amt und Person ein öffentliches Prangerrecht haben soll.
Art. 49 Weitere Aufgaben Der Beauftragte nimmt darüber hinaus insbesondere folgende Aufgaben wahr: a. Er informiert und berät die Organe des Bundes und der Kantone sowie private Personen bei Fragen des Datenschutzes. b. Er arbeitet mit schweizerischen und ausländischen Behörden, die für den Datenschutz zuständig sind, zusammen. c. Er sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz. d. Er erteilt der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann. e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen. f. Er nimmt die ihm durch das Öffentlichkeitsgesetz übertragenen Aufgaben wahr.	**Antrag zu Art. 49 lit. d**: Streichen. Wenn der Datenschutzbeauftragte eine Aufsichtsfunktion hat, kann er nicht gleichzeitig auch eine Konsumentenschutzaufgabe erfüllen dürfen.
8. Abschnitt: Strafbestimmungen	**Antrag zum 8. Abschnitt (Art. 50ff)**: Das gesamte Sanktionssystem ist zu überarbeiten. Es führt zu einer nicht sachgerechten Kriminalisierung der mit Datenschutz sich auseinandersetzenden Mitarbeitenden und Unternehmen. Unverständlich ist zudem, dass gerade die Verwaltung von den Strafsanktionen ausgenommen werden soll. Es wird komplett vergessen und ausgeblendet, dass vor noch nicht langer Zeit, die Gefahr im Umgang mit Daten nicht von Privaten und nicht von Unternehmen, sondern vom Staat selbst ausge-

VE-DSG	Anträge und Bemerkungen
	gangen ist (Stichwort: Fichen-Affäre). Es wäre naiv zu glauben, dass sich diese Bedrohung in den letzten 20 Jahren komplett verflüchtigt hätte. Mit einer zunehmend hohen Verwaltungsquote von gegen 40% wäre ein sehr hoher Anteil der Berufstätigen vom Sanktionssystem ausgenommen. Das ist höchst zweifelhaft und politisch nicht zu rechtfertigen. Alternative: Der Beauftragte soll als Aufsichtsbehörde untersuchen und verfügen können. Unternehmen sollen sich in diesem verwaltungsrechtlichen Verfahren wehren können. Erst wenn rechtskräftige Entscheide nicht umgesetzt worden sind, sollten Strafsanktionen greifen. Es besteht kein Rechtfertigungsgrund, von diesem in anderen Belangen des Bundesrechts verankerten Prinzip abzuweichen.
Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten [1] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft: a. die ihre Pflichten nach den Artikeln 13, 15 und 20 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;	**Antrag zu Art. 50**:Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen. Der Bussenrahmen ist auf eine maximale Höhe von CHF 5'000.- bzw. – im Wiederholungsfall –auf maximal CHF 10'000.- zu begrenzen. Bei Verletzung der Sorgfaltspflichten sind noch tiefere Bussen anzusetzen, sicher nicht Beträge bis CHF 500'000.-.Bei den Vorsatzbussen muss zwingend ein Zusammenhang mit den Umsatzzahlen oder dem steuerbaren Einkommen einer natürlichen Person bzw. eines Unternehmens hergestellt werden, wie dies in der DSVGO bei Unternehmen ausdrücklich vorgesehen ist (Art. 83 Abs. 2 geht von 2 % des weltweiten Umsatzes eines Unternehmens aus. Für Schweizer Verhältnisse wäre 1 % als Höchstgrenze wohl angemessen. Bisher betragen im Strafrecht die Bussen maximal CHF 10'000.- für eine Übertretung (Art. 106 Abs. 1 StGB). Das Verwaltungsstrafrecht kennt ähnliche Grössenordnungen. Bussenbeträge über CHF 100'000.- sind bislang in der Schweiz nicht bekannt. Die Erhöhung des Strafrahmens auf CHF 500'000.- ist daher völlig überrissen und nicht nachvollziehbar.
b. die es vorsätzlich unterlassen: 1. die betroffene Person nach Artikel 13 Absätze 1 und 5, 15 und 17 Absatz 2 die betroffene Person zu informieren; oder 2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2, 3 und 4 zu liefern.	**Antrag zu Art. 50 Abs. 1 lit. b)**:Ändern. Art 13 ist vollständig von der Sanktionierung auszunehmen.
c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3).	**Antrag zu Art. 50 Abs. 1 lit. c)**: Streichen. Ist vollständig von der Sanktionierung auszunehmen.
[2] Mit Busse bis zu 500 000 Franken werden private Personen bestraft, wer vorsätzlich: a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b und Absatz 6 zu informieren; b. die es unterlassen, dem Beauftragten die standardisierten Garantien oder die verbindlichen unternehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c	**Antrag zu Art. 50 Abs. 2, lit. a) und b)**:Streichen. Da die Meldepflicht sowieso massiv reduziert werden müssen, ist auch diese Bestimmung zu streichen.

VE-DSG	Anträge und Bemerkungen
Ziff. 1 und Bst. d Ziff. 1); c. dem Beauftragten bei der Untersuchung (Art. 41 Abs. 2) falsche Auskünfte erteilen oder die Mitwirkung verweigern; e. es unterlassen, dem Beauftragten Verletzungen des Datenschutzes nach Artikel 17 Absatz 1 zu melden; f. einer Verfügung des Beauftragten nicht Folge leistet. [3] Mit Busse bis zu 500 000 Franken werden private Personen auf **Antrag** bestraft, die es vorsätzlich unterlassen: a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren; b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 zu informieren. [4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**Antrag zu Art. 50 Abs. 2, lit. e)**: Ändern. Diese Bestimmung ist auf Vorfälle zu beschränken, die schwerwiegend sind und mehr als 1'000 Personen betreffen. **Antrag zu Art. 50 Abs. 2, lit. f**: Streichen. Hier genügt die bestehende Strafbestimmung im StGB. **Antrag zu Art. 50 Abs. 3, lit. a)**: Streichen. Die dem Bst. a) zugrundeliegende Bestimmung ist Art. 19 Bst. b) ist in der Praxis gar nicht umsetzbar. Daher ist auch die Strafbestimmung zu streichen. **Antrag zu Art. 50 Abs. 4**: Streichen. Die Fahrlässigkeit ist von der strafrechtlichen Sanktionierung generell auszunehmen.
Art. 51 Verletzung der Sorgfaltspflichten [1] Mit Busse bis zu 500'000 Franken werden private Personen auf **Antrag** bestraft, die vorsätzlich: a. unter Verstoss gegen Artikel 5 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln; b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 7 Absätze 1 und 2 erfüllt sind; c. es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder Verlust zu schützen (Art. 11); d. es unterlassen, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16); e. es unterlassen, die Vorkehren nach Artikel 18 zu treffen; f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert.	**Antrag zu Art. 51 Abs. 1**: Bei Vorsatz sind Bussen bis CHF 10'000.- angemessen. **Antrag zu Art. 51 Abs. 1 lit. a)**: Die Meldepflicht von Art. 6 Abs. 2 ist von der Busse auszunehmen, da ansonsten tausende von KMU unwissentlich kriminalisiert werden. **Antrag zu Art. 51 Abs. 1 lit. d)**: Streichen; erst die Folgeabschätzung kann ja zeigen, ob eine Folgeabschätzung notwendig wäre. Die Strafdrohung führt dazu, dass dieses Verfahren für jede Datenbearbeitung durchgeführt werden muss. In der Rechtsfolgeabschätzung werden Kosten von CHF 5'000 – 30'000.- pro Durchführung veranschlagt, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU führen würde. **Antrag zu Art. 51 Abs. 1 lit. e)**: Streichen; Hier handelt es sich um eine unbestimmte Handlungsdefinition, die dadurch kaum eine Strafbarkeit auslösen kann. **Antrag zu Art. 51 Abs. 1 lit. f)**: Streichen; die Strafdrohung führt dazu, dass

VE-DSG	Anträge und Bemerkungen
[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	alle Prozesse für die Datenbearbeitung vorsorglich dokumentiert werden müssen, was zu einer enormen administrativen Belastung der Unternehmen, insbesondere der KMU, führen würde. In der RFA wurden diese Kosten nicht erhoben. **Antrag zu Art. 51 Abs. 2**: Bei Fahrlässigkeit ist von einer strafrechtlichen Sanktionierung abzusehen.
Art. 52 Verletzung der beruflichen Schweigepflicht [1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf **Antrag** bestraft, wer vorsätzlich geheime Personendaten bekannt gibt: a. von denen er im Rahmen seiner beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat; b. welche er selbst zu kommerziellen Zwecken bearbeitet hat. [2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er bei der Tätigkeit für einen Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat. [3] Das Bekanntgeben geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.	**Antrag zu Art. 52**: Streichen; der bisherige Art. 35 DSG hat die Bekanntgabe von Persönlichkeitsprofilen und besonders schützenswerten Personendaten geregelt. Die Ausweitung auf den unbestimmten Begriff „geheime Personendaten" wird abgelehnt. Die strafrechtlichen Bestimmungen über die berufliche Schweigepflicht sind völlig ausreichend. Damit würde jeder Bearbeiter von Personendaten einer strafbewehrten Schweigepflicht unterworfen. Freiheitsstrafen bis 3 Jahren zu verhängen für die Verletzung von Schweigepflichten ist völlig unverhältnismässig. *Eventualiter* wäre es sinnvoller, die Strafbarkeit in dieser Bestimmung auf Auftragsbearbeiter und Beauftragte zu beschränken.
Art. 53 Übertretungen in Geschäftsbetrieben Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.	**Antrag zu Art. 53**: Streichen; die bestehenden Regelungen im Verwaltungsstrafrecht und im Strafrecht sind ausreichend.
Art. 54 Anwendbares Recht und Verfahren Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.	**Antrag zu Art. 54**: Streichen; die Verfolgung und Beurteilung strafbarer Handlungen im Zusammenhang mit dem Datenschutzgesetz soll als Verwaltungsverfahren ausgestaltet werden und ist somit vom Bund zu führen.
Art. 55 Verfolgungsverjährung für Übertretungen Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.	**Antrag zu Art 55**: Die Verjährungsfrist ist bei 3 statt 5 Jahren anzusetzen. Das entspricht auch vergleichbaren Regelungen (z.B. StGB 109) und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
9. Abschnitt: Abschluss von Staatsverträgen	
Art. 56 Der Bundesrat kann Staatsverträge abschliessen betreffend: a. die internationale Zusammenarbeit zwischen Datenschutzbehörden; b. die gegenseitige Anerkennung eines angemessenen Schutzes für die Bekanntgabe von Personendaten ins Ausland.	Titel fehlt zum Artikel fehlt.
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unterstehen den Artikeln 1-22, 26, 27, 29 bis 32, 34 Absätze 1-3 und 36 dieses Gesetzes, soweit sie nicht kantonalen Datenschutzvorschriften unterstehen, die einen angemessenen Schutz der Daten gewährleisten. [2] Die Kantone bestimmen ein Organ, das die Einhaltung der Datenschutzvorschriften überwacht. Die Artikel 41-43, 48 und 49 gelten sinngemäss.	
Art. 58 Aufhebung und Änderung anderer Erlasse Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.	Keine Bemerkungen
Art. 59 Übergangsbestimmung Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die für Verantwortlichen sowie der Auftragsbearbeiter in der Lage sein: a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen; b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.	**Antrag zu Art. 59**: Es ist eine generelle Übergangsfrist von zwei Jahren vorzusehen, die nicht nur auf die Datenschutz-Folgeabschätzung bzw. Datenbearbeitungen zu beschränken ist.
Art. 60 Referendum und Inkrafttreten [1] Dieses Gesetz untersteht dem fakultativen Referendum. [2] Der Bundesrat bestimmt das Inkrafttreten.	Keine Bemerkungen

Sammlung Änderungsvorschläge: Aufhebung und Änderung anderer Erlasse

VE-DSG	Anträge und Bemerkungen

VE-DSG	Anträge und Bemerkungen
11. Zivilprozessordnung *Art. 20 Bst. d* Für die folgenden Klagen und Begehren ist das Gericht am Wohnsitz oder Sitz einer der Parteien zuständig: d. Klagen und Begehren nach dem Datenschutzgesetz vom ... *Art. 99 Abs. 3 Bst. d* [3] Keine Sicherheit ist zu leisten: d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom.... *Art. 113 Abs. 2 Bst. g* [2] Keine Gerichtskosten werden gesprochen in Streitigkeiten: g. nach dem Datenschutzgesetz vom ..... *Art. 114 Bst. f* Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom ..... *Art. 243 Abs. 2 Bst. d* [2] Es gilt ohne Rücksicht auf den Streitwert für Streitigkeiten: d. zur Durchsetzung der Ansprüche nach den Artikeln 12 und 20 des Datenschutzgesetzes vom ...	**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht (weder kosten- noch verfahrensmässig). Da in Datenschutzfragen der Beauftragte eine Aufsichtsfunktion ausübt, kann er bei Verstössen aktiv werden. Es braucht hier keine weitere soziale Gerichtsbarkeit. Für zivilrechtliche Verfahren genügen die bestehenden Regeln. Das kostenlose Prozessieren könnte hier eine Flut – auch von mutwilligen – Klagen auslösen. Einem bedürftigen Kläger steht die unentgeltliche Prozessführung zur Verfügung, der solvente soll – wie dies bei zivilrechtlichen Streitigkeiten grundsätzlich der Fall ist – seine Kostenrisiken abwägen müssen, ehe Gerichte bemüht werden.

VE-DSG	Anträge und Bemerkungen
13. Strafgesetzbuch *Art. 179novies* Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. *Art. 179decies* Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.	**Antrag zu Art. 179novies**: Die Strafbarkeit der Beschaffung ist zu beschränken auf Daten die einem Berufsgeheimnis unterliegen sowie auf besonders schützenswerte Personendaten. Die unbefugte Beschaffung von Personendaten mit bis zu drei Jahren Freiheitsstrafe zu bestrafen ist unverhältnismässig. Hier reicht eine Geldstrafe.
37. Fernmeldegesetz vom 30. April 1997 *Art. 13a Abs. 1 erster Satz* 1 Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, bearbeiten, sofern dies für die Erfüllung der ihnen durch die Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. ... *Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz* 1 ... Zu diesen Daten gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten. 2 Unter Vorbehalt anders lautender internationaler Vereinbarungen dürfen die Kommission und das Bundesamt ausländischen Aufsichtsbehörden im Fernmeldebereich Daten, einschliesslich in Verwaltungs- oder Verwaltungsstrafverfahren beschaffter besonders schützenswerter Personendaten, nur übermitteln, sofern diese Behörden: 4 Schweizerische Behörden geben der Kommission und dem Bundesamt kostenlos diejenigen Daten weiter, die für die Durchsetzung der Fernmeldegesetzgebung von Bedeutung sein können, einschliesslich besonders schützenswerter Personendaten. ...	**Bemerkung zu datenschutzrechtlichen Regulierungen im Fernmeldegesetz**: Es ist klarzustellen, dass datenschutzrechtliche Regulierungen im Fernmeldegesetz und in dessen Ausführungsbestimmungen als *lex specialis* den allgemeinen Datenschutzbestimmungen des DSG und dessen Ausführungsbestimmungen vorgehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

Hunziker Urs
VRP

Hubacher Peter
Vize VRP