Amstutz Jonas BJ

Von:	Hermann Amstad <h.amstad@samw.ch>
Gesendet:	Montag, 3. April 2017 11:59
An:	Amstutz Jonas BJ
Cc:	Maurice Campagna; Claudia Appenzeller
Betreff:	Stellungnahme der Akademien der Wissenschaften Schweiz zum Vorentwurf für ein Bundesgesetz über die Totalrevision des Datenschutzgesetzes
Anlagen:	Stellungnahme_20170330_DSG-a+.doc

Sehr geehrter Herr Amstutz

Beiliegend finden Sie die Stellungnahme der Akademien der Wissenschaften Schweiz zum Vorentwurf für ein Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz.

Bei Rückfragen stehe ich Ihnen gerne zur verfügung.

Freundliche Grüsse
Hermann Amstad

Dr. med. Hermann Amstad, MPH
Generalsekretär
Schweizerische Akademie der Medizinischen Wissenschaften (SAMW)
Haus der Akademien
Laupenstrasse 7
CH-3001 Bern
Tel. +41 31 306 92 70 / 71 (direkt)
h.amstad@samw.ch

Die SAMW ist Mitglied der Akademien der Wissenschaften Schweiz
---

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 : Akademien der Wissenschaften Schweiz

Abkürzung der Firma / Organisation : a+

Adresse : Haus der Akademien, Laupenstrasse 1, 3001 Bern

Kontaktperson : Hermann Amstad

Telefon : 031 306 92 70

E-Mail : h.amstad@samw.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!

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 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 4

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.	Die Akademien der Wissenschaften Schweiz begrüssen die geplante Revision des Datenschutzgesetzes (DSG); im Kontext von «Big Data» und angesichts der zunehmenden Digitalisierung der Gesellschaft ist diese unumgänglich. Die Revision bringt den BürgerInnen eine grössere Transparenz und Autonomie in Bezug auf die Verwaltung ihrer Daten; zudem passt sie die schweizerische Gesetzgebung den europäischen Anforderungen an und erleichtert so den internationalen Datenaustausch.
Fehler! Verweisquelle konnte nicht gefunden werden.	Trotz der notwendigen Anpassungen bleibt das Gesetz erfreulich schlank, dies namentlich auch im Vergleich zu ähnlichen Gesetzen im Ausland. Allerdings enthält der Revisionsentwurf teilweise auch strengere Bestimmungen, als dies auf europäischer Ebene vorgesehen ist (z.B. in Art. 13 und Art. 17); auf diese ist zu verzichten.
Fehler! Verweisquelle konnte nicht gefunden werden.	Genetische Daten werden zu Recht neu namentlich im DSG erwähnt; damit werden sie in Zukunft in drei verschiedenen Gesetzen (GUMG, HFG und DSG) geregelt. Entsprechend wäre es wichtig, den jeweiligen Anwendungsbereich dieser Gesetze zu präzisieren.
Fehler! Verweisquelle konnte nicht gefunden werden.	An mehreren Stellen im Gesetz werden sowohl die notwendige Zustimmung der betroffenen Personen als auch die Informationspflicht zuhanden dieser Personen erwähnt; wie dies in der medizinischen Praxis umgesetzt werden soll, ist offen. Noch weniger umsetzbar in der medizinischen Praxis ist die Regelung, wonach im Falle einer jeder Berichtigung, Löschung oder Vernichtung von Daten der Verantwortliche den Dritten, denen er zuvor diese Daten zugänglich gemacht hat, diese Änderungen mitteilen muss. Auch wenn bei diesem und ähnlichen Artikeln jeweils vermerkt ist, dass die betreffende Bestimmung nicht gilt, falls sie nicht oder nur mit unverhältnismässigem Aufwand umsetzbar ist, wäre es zu begrüssen, wenn das DSG die medizinisch erhobenen Daten als Spezialfall erwähnen würde.
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
a+	DSG	2	1		Als Bearbeiter von Daten werden private Personen und Bundesorgane genannt; es ist unklar, inwiefern private oder öffentliche Institutionen (nicht) betroffen sind.
a+	DSG	3			Die Begriffe Identifizieren, Pseudonymisieren und Anonymisieren sind ebenfalls und harmonisiert mit dem Humanforschungsgesetz zu definieren
a+	DSG	4	4		Diese Bestimmung ist zu einschränkend für medizinische oder Gesundheitsdaten; diese sollten (auch im Interesse der betroffenen Person) über den für den ursprünglichen Zweck notwendigen Zeitraum hinaus aufbewahrt werden können (vgl. allgemeine Bemerkungen).
a+	DSG	4	5		Diese Bestimmung ist zu einschränkend für medizinische oder Gesundheitsdaten; diese sind unter Umständen auch von rechtsmedizinischem Interesse und sollten, selbst wenn sie falsch sind, aufbewahrt werden können, um gewisse Handlungen rechtfertigen zu können (vgl. allgemeine Bemerkungen).
a+	DSG	4	6		Es ist zu klären, was unter «eindeutiger» Einwilligung zu verstehen ist (z.B. Schriftlichkeit?).
a+	DSG	12	4		Diese Bestimmung ist zu einschränkend für medizinische oder Gesundheitsdaten; diese Daten können von sowohl von persönlichem Interesse sein für genetisch verwandte Nachkommen oder für Organempfänger, aber auch von öffentlichem Interesse (Forschung oder Public Health) oder von rechtsmedizinischem Interesse, um Handlungen zu Lebzeiten der betroffenen Person rechtfertigen zu können (vgl. allgemeine Bemerkungen).
a+	DSG	13			Anzupassen an die Vorgaben auf europäischer Ebene.
a+	DSG	13	4		In der Medizin ist es nicht möglich, im Moment der Datenbeschaffung jeden Auftragsbearbeiter zu kennen,

					namentlich was die diagnostischen Abklärungen betrifft (vgl. allgemeine Bemerkungen).
a+	DSG	16			In einem zusätzlichen Abschnitt sollte die Möglichkeit erwähnt werden, dass im Rahmen der Bearbeitung persönlicher (Gesundheits)Daten Zufallsbefunde erhoben werden können, die für die betroffenen Personen von grosser Tragweite sein können; diese Tatsache scheint durch Art. 20, Abs, 3 nicht abgedeckt zu sein.
a+	DSG	17	4		streichen
a+	DSG	19		b	Es ist offensichtlich, dass diese Bestimmung für die Medizin nicht oder nur mit unverhältnismässigem Aufwand möglich wäre (vgl. allgemeine Bemerkungen).
a+	DSG	20	4		«Arzt» ersetzen durch «Gesundheitsfachperson».
a+	DSG	50			Die Höhe der Busse für Privatpersonen ist unverhältnismässig.
a+	DSG	51			Die Höhe der Busse für Privatpersonen ist unverhältnismässig.
a+	DSG	52			Die Höhe der Busse für Privatpersonen ist unverhältnismässig.
a+	DSG	53			Die Höhe der Busse für Privatpersonen ist unverhältnismässig.

Am 27.3.2107

Amstutz Jonas BJ

Von: Acsi <acsi@acsi.ch>
Gesendet: Mittwoch, 5. April 2017 10:44
An: Amstutz Jonas BJ
Betreff: Loi protection des données
Anlagen: ACSI_Prise de position révision LPD.DOC

Cordiali saluti.

acsi
associazione consumatrici e consumatori della Svizzera italiana
Strada di Pregassona 33 – 6963 Pregassona
www.acsi.ch
Dove trovarci

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 : Associazione consumatrici e consumatori della Svizzera italiana

Abréviation de la société / de l'organisation : ACSI

Adresse : Strada di Pregassona 33, 6963 Pregassona

Personne de référence : Laura Regazzoni Meli – segretaria generale

Téléphone : 091 922 97 55

Courriel : l.regazzoni@acsi.ch

Date : 5 aprile 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

Remarques générales _____ 3

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 _____ 7

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 _____ Fehler! Textmarke nicht definiert.

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel _____ Fehler! Textmarke nicht definiert.

Rapport explicatif (excepté chap. 8 « Commentaire des dispositions»)_____ Fehler! Textmarke nicht definiert.

Rapport explicatif : chap. 8 « Commentaire des dispositions » _____ Fehler! Textmarke nicht definiert.

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.ACSI	L'ACSI soutient globalement le projet de loi proposé. Les avancées technologiques de ces dernières années nécessitent une révision de la Loi fédérale sur la protection des données, afin que le particulier dispose d'un niveau de sécurité suffisant sur ses propres données. Le responsable de fichier (ou de traitement selon la nouvelle terminologie) doit assurer transparence et proportionnalité lors du traitement de données.
Fehler! Verweisquelle konnte nicht gefunden werden.ACSI	Un exemple récent, qu'il faut mieux légiférer en Suisse sur la protection des données, est le suivant: Swisscom a informé ses clients, en février 2017, que leurs données allaient être transmises à des tiers. La communication qui a été faite aux clients Swisscom était peu transparente et n'expliquait pas les enjeux au niveau de la transmission des données, ni le destinataire de celles-ci. Les clients qui voulaient refuser devraient être pro-actifs pour s'opposer à l'utilisation de leurs données. Une simple opposition ne suffisait pas: il fallait passer par une procédure compliquée d'opt-out sur le site internet de Swisscom.. Pour les clients qui n'avaient pas le courage ou la possibilité de se lancer dans cette procédure, cela signifie que leurs données allaient être transmises à des tiers, certains étant aussi à l'étranger. Une procédure de ce type n'est pas acceptable du point de vue du client. La protection des données devrait être guidée par le principe du opt-in. Gage de confiance accrue entre entreprises et consommateurs, il faut pouvoir exiger des firmes un «opt-in actif»: ainsi, le consommateur donne ainsi son accord explicite à l'échange d'informations. L'opt-out passif, plus sournois, contraint le client à demander à être retiré d'un fichier où il a été enregistré d'office. L'ACSI considère que l'utilisation des données, sans contrepartie pour le consommateur, doit faire en tous les cas l'objet d'un opt-in.
Fehler! Verweisquelle konnte nicht gefunden werden.ACSI	Si certaines compétences du Préposé fédéral à la protection des données et à la transparence (PFPDT) sont élargies, il lui manquera toutefois toujours un pouvoir de sanctionner. Cela signifie qu'il faudra continuer à passer par le biais de procédures judiciaires pour voir reconnaître ses droits, ce qui est évidemment beaucoup plus lourd et compliqué pour un consommateur. S'il n'y a pas de sanction, il faudrait au moins donner la possibilité au PFPDT d'agir comme médiateur lorsqu'un consommateur a un litige, sur le même modèle que l'Ombudscom, par exemple. Cela serait très utile en particulier pour des procédures qui demandent de faire cesser l'atteinte, plutôt que d'agir en justice, ce qui est souvent compliqué et coûteux pour le consommateur.

Fehler! Verweisquelle konnte nicht gefunden werden.ACSI	S'agissant des amendes qui peuvent être infligées, il est regrettable que le projet prévoie que ce sont les personnes privées qui peuvent être sanctionnées et non les entreprises.
Fehler! Verweisquelle konnte nicht gefunden werden.ACSI	L'ACSI regrette que le projet de LPD, contrairement au droit européen, ne prévoit pas de droit à la portabilité qui permette de récupérer ses données dans un format standard pour se tourner vers un autre fournisseur. Cela aurait permis un meilleur contrôle sur ses données, favorisé leur réutilisation et le développement de nouveaux services.
Fehler! Verweisquelle konnte nicht gefunden werden.ACSI	L'avant-projet ne prévoit pas de renversement du fardeau de la preuve en faveur de la personne dont les données sont traitées. En cas de procédure judiciaire, c'est donc à celui qui allègue un fait de le prouver. Un renversement aurait obligé le responsable du traitement à démontrer qu'il traite les données de manière licite.
Fehler! Verweisquelle konnte nicht gefunden werden.ACSI	Aucune action collective n'est prévue, le Conseil fédéral préférant mettre cela en œuvre par le biais d'une modification générale du Code de procédure civile. Un regroupement des procédures devant le PFPDT aurait simplifié le travail aussi bien pour les responsables du traitement que pour les personnes concernées.
Fehler! Verweisquell	Plusieurs interventions parlementaires (Postulat Schwaab, 16.3682 ; Motion Savary, 12.3578 ; Question Comte, 12.1084) se sont penchées sur la problématique **des fichiers de solvabilité**. Ces fichiers tiennent des informations sur la solvabilité des personnes privées, donnent des

e konnte nicht gefunden werden.ACSI	renseignements commerciaux, voire même des notes sur des particuliers, sans que l'on sache d'où viennent les données et comment elles sont traitées. Moyennant finance, n'importe qui peut avoir accès à ces données. Souvent, les personnes fichées ne savent même pas qu'elles le sont. Et si elles le savent, elles peinent à savoir à quelles entreprises s'adresser. En résumé, il règne une immense opacité qui ne correspond pas aux principes de la loi sur la protection des données. En outre, se pose le problème de la véracité des données inscrites. Les renseignements sont souvent inexacts, les créances douteuses ou il y a confusion dans les noms (homonymie). De bons payeurs, des enfants parfois se retrouvent sur ces listes. Bref la population tout entière peut être victime d'un fichage abusif. Les conséquences de ces données disponibles dans les registres de solvabilité et à disposition de quiconque souhaite les consulter peuvent être graves. Le système de notation appliqué par les sociétés de recouvrement (la note A est la note maximale) peut être consulté par toute personne ou entreprise souhaitant se renseigner sur un citoyen. Cela a un impact quotidien sur la vie des gens (abonnement de téléphonie, bail, contrat de travail, petit crédit ou encore assurance refusés). Cela peut porter une grave atteinte à la vie privée des gens, inadmissible dans la plupart des cas. Aucune indication de durée n'est préconisée pour la conservation des données, aucune définition n'est arrêtée pour préciser qui est un bon ou un mauvais payeur. Il n'est pas rare d'avoir une mauvaise note sur la base d'un simple retard de paiement. La procédure pour demander l'effacement et la suppression des données n'est souvent pas claire, voire inexistante. Ces fichiers, à l'inverse du registre des poursuites et de l'IKO (fichier lié à la loi sur le crédit à la consommation), n'ont aucune base légale. Ils doivent être interdits dans la LPD. En 2012, une pétition de l'Alliance des organisations de consommateurs (ACSI, FRC et SKS), réunissant plus de 4000 signature, demandait au Conseil fédéral l'interdiction de ficher les personnes privées en matière de solvabilité dans des fichiers autres que le registre des poursuites et l'IKO, centre suisse de renseignements pour le crédit à la consommation. Pour sortir de ces fichiers, il faut souvent une longue procédure d'opt-out. Le Conseil fédéral avait répondu, notamment dans le cadre de la motion Savary et de la question Comte, qu'une législation complémentaire à ce sujet devrait être examinée dans le cadre de la révision de la LPD. Or, ce point n'a pas du tout été traité par la révision de la LPD. Il n'est même pas évoqué dans le rapport. Le problème se pose également avec les maisons de recouvrement qui transmettent les données récoltées à des sociétés de renseignements économiques, sans que l'on connaisse les critères de transmission. L'ACSI estime que la question doit être réglée dans le cadre de la révision de la LPD : le principe devrait être que ces fichiers, mis à part le Registre des poursuites et l'IKO, sont interdits.
ACSI	L'ACSI se réjouit que les données génétiques et les données biométriques qui identifient un individu de façon unique figurent explicitement dans cette révision de la LPD. 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. Lorsque la personne fait un don d'échantillon biologique à des fins de recherche, il est difficile de prévoir toutes les conséquences que pourrait avoir ce geste dans plusieurs années. Aussi, il nous semble primordial d'encadrer strictement le traitement de ces données. Le projet de révision de la LPD devrait mieux prendre en compte les risques liés à cette question. Il nous semble également utile de préciser que le concept d'anonymisation des données doit être appréhendé de manière très prudente. Avec le développement des techniques génétiques et physiologiques, il est actuellement aisé de relier un échantillon biologique à un individu. 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.
ACSI	L'ACSI considère que la LPD devrait aussi pouvoir s'appliquer à des entreprises n'ayant pas de siège en Suisse mais procédant à des traitements ayant des effets en Suisse. Celles-ci devraient avoir un répondant en Suisse.
ACSI	En résumé, l'ACSI, même si elle n'est pas entièrement satisfaite par la révision de la LPD telle que proposée, car trop légère, soutient cette révision. Elle demande par contre que soient ajoutés à la loi les points suivants : - Principe en matière de protection des données : Procédure d'opt-in - Droit à la portabilité - Renversement du fardeau de la preuve - Pouvoir de sanction administrative du PFPDT, ce qui impliquerait des moyens financiers supplémentaires pour le PFPDT - Action collective - Interdiction des fichiers de solvabilité, excepté les registres de poursuites et l'IKO, centre de renseignement suisse sur les crédits à la consommation - Amendes à l'égard des entreprises et non des personnes privées - Application de la LPD à des entreprises, n'ayant pas de siège en Suisse mais dont l'utilisation de données ont des effets en Suisse.

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 :
ACSI	LPD	2	1	a	Le rapport du Conseil fédéral ne définit pas clairement ce qu'il entend par « personne privée ». S'agit-il uniquement de personnes physiques ou s'agit-il des personnes physiques et morales ? L'acception pour nous doit être celle des personnes physiques et morales. Si tel n'est pas le cas, la portée de la révision de la LPD n'est pas suffisante.
ACSI	LPD	3		c	L'introduction spécifique des points 3. et 4. est saluée, soit les données génétiques, et les données biométriques qui identifient un individu de façon unique.
Fehler! Verweisquelle konnte nicht gefunden werden.ACS	LPD	4	2		L'exigence d'un traitement conforme au principe de la proportionnalité est essentielle et est saluée. Le principe de la minimisation des données doit conduire à un traitement approprié des seules données nécessaires au but recherché.

I					
Fehler! Verweisquelle konnte nicht gefunden werden.ACSI	LPD	4	3		La formulation de l'article 3 ne garantit aucune protection adéquate. Cela ne suffit pas, que le but du traitement soit clairement reconnaissable. Ce qui est déterminant, c'est que la personne concernée doit être informée explicitement au moment de la collecte des données. Il doit d'abord être informé de la collecte des données elle-même. D'autre part, le but du traitement des données doit être clairement expliqué. Le cas des données marketing transmises à des tiers est particulièrement criant, notamment celles transmises à des pseudo partenaires. Il ne devrait pas être possible de transmettre ces données sans accord exprès de la personne concernée. Proposition : Les données personnelles doivent être collectées pour des finalités déterminées et en informant du but recherché la personne concernée ;…. La deuxième partie de la phrase de l'article 4 dans la version française ne correspond pas à la version allemande, ce qui porte à confusion.
ACSI	LPD	4	6		Cet alinéa doit être complété par le principe du opt-in. En effet, l'ACSI estime que c'est un accord explicite qui doit guider les relations entre les parties pour que la confiance soit garantie entre les entreprises et les particuliers.
ACSI	LPD	5	1		Selon cet alinéa, aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée. Cette limitation à la gravité de la menace est en opposition avec les autres alinéas de l'art. 5 et doit être clairement refusée.
ACSI	LPD	5	2		Nous ne voyons pas très bien comment le Conseil fédéral pourra constater qu'un autre Etat dispose d'une législation assurant un niveau de protection suffisant, quels seront les critères pour déterminer cela.
ACSI	LPD	6	1	e	La lettre e de l'art. 6 al. 1 AP-LPD prévoit que des données peuvent exceptionnellement être communiquées à l'étranger lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement. La notion d'accessibilité n'est pas suffisante dans le monde numérique actuel. Il faudrait dès lors compléter cette

					notion par le terme publiquement. Par ailleurs, la collecte de données doit également être protégée par cette article. Nous proposons donc la formulation suivante pour la lettre e : La personne concernée a rendu les données personnelles accessibles publiquement à tout un chacun et n'est pas opposée expressément à la collecte.
ACSI	LPD	8			La publication de recommandations de bonnes pratiques par le PFPDT est à saluer. Néanmoins, le fait que celles-ci ne soient pas contraignantes restreint la portée de cette article et risque parfois de porter à confusion : s'agit-il d'un objectif idéal ou du minimum légal à atteindre ? Comme le montre l'exemple de Swisscom, le PFPDT a proposé une procédure d'opt-in, ce qui n'a pas été suivi par l'opérateur, qui a uniquement mis en place une procédure d'opt-out.
ACSI	LPD	10	1		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 certification « obligatoire ». Ceci permettrait 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 ;* *les organisations qui, de par la loi, sont amenées à traiter des données sur la santé.* »
Fehler! Verweisquelle konnte nicht gefunden werden.ACSI	LPD	12	3		Si l'on peut saluer le fait d'avoir voulu régler dans la LPD la question de la mort numérique, il apparaît en revanche que l'alinéa 3 de cet article est inacceptable. Les données médicales ou juridiques sont notamment protégées par les dispositions relatives au secret professionnel (art. 321 CP) et au secret de fonction (art. 320 CP). Le secret professionnel poursuit plusieurs intérêts, en particulier. - La protection de la sphère intime et privée du particulier, qui doit pouvoir se fier entièrement à la discrétion du professionnel en vue de lui livrer toutes les informations qui lui permettront de recevoir le traitement le plus adapté. - L'intérêt de l'Etat à ce que les professions protégées par le secret professionnel puissent être exercées correctement et sans entrave, dans la mesure où ces professions ne peuvent être exercées que si elles inspirent au public une confiance suffisante, moyennant de sérieuses garanties de discrétion. - L'intérêt du professionnel à ce qu'un rapport de confiance existe, de manière à pouvoir exercer son métier efficacement. - La protection des informations qui concernent des tiers et qui auraient été divulguées. Selon la jurisprudence, le secret médical continue de déployer ses effets après la mort du patient (ATF 87 IV 105). Même si la personnalité finit par la mort (art. 31 CC), il n'apparaît en effet pas dépourvu de sens de garantir aux justiciables qu'après leur décès, les renseignements figurant dans leur dossier médical demeureront couverts par le secret médical et ne seront divulgués *sans un contrôle sévère* (arrêt du Tribunal fédéral du 3 novembre 1989, RDAF 1990 p. 45, c. 4b). L'article 12 AP-LPD ouvre une brèche inacceptable au maintien du secret médical ou juridique après la mort du patient. Si le défunt n'a pas de son vivant interdit expressément la consultation de son dossier

					après sa mort, cette disposition permettrait en effet à tout tiers présentant un intérêt légitime de consulter son dossier si aucun intérêt prépondérant du défunt ou d'un tiers l'en empêche. Cette disposition est problématique à plusieurs titres : - L'article 12 AP-LPD supprime au responsable du traitement le droit d'invoquer le secret professionnel ou de fonction. De ce fait, il remet en cause l'existence même du secret médical ou juridique après la mort du patient. Cela est propre à entamer la confiance nécessaire que le public doit placer dans ces professions afin de garantir le bon exercice de ces dernières. Le secret professionnel, le cas échéant de fonction, doit être maintenu après la mort du patient. - Le dossier médical ou juridique d'une personne décédée peut contenir des données très sensibles que le défunt ne souhaitait pas divulguer aux membres de sa famille, même après sa mort. Ces données nécessitent une protection particulière, que l'article 12 AP-LPD n'assure pas suffisamment. - L'article 12 AP-LPD présume l'existence d'un intérêt légitime en faveur des personnes en lien de parenté directe avec le défunt ou mariées, en partenariat enregistré ou en concubinage. Or, le secret professionnel vaut précisément à l'égard de ces proches et il doit être maintenu par principe après la mort du patient. L'accès aux données médicales ou juridiques par les proches après la mort du patient est rendu ici trop aisé. - Les garde-fous prévus par l'article 12 al. 1 AP-LPD, à savoir que le défunt n'a pas de son vivant interdit expressément la consultation et qu'aucun intérêt prépondérant du défunt ou d'un tiers ne l'empêche, constituent des protections insuffisantes en matière de secret professionnel. Il paraît en effet douteux que l'ensemble des particuliers soient informés, au début de chaque relation avec celui soumis au secret professionnel, de leur droit de s'opposer à la divulgation de leurs données après leur mort. Nous reconnaissons que la consultation de données médicales d'une personne décédée doit pouvoir être accordée dans des circonstances particulières, notamment en cas de suspicion d'erreur médicale ayant conduit à la mort d'un patient ou en cas de maladie génétique. Toutefois, même dans cette hypothèse, la transmission d'informations aux proches doit être strictement encadrée et se limiter aux

					seules informations nécessaires. En conséquence, l'article 12 al. 3 AP-LPD ne peut pas subsister sous la forme proposée.
ACSI	LPD	13	1-5		L'article 13 prévoit un devoir d'informer la personne concernée de la collecte de données. La collecte de données en elle-même représente déjà un traitement des données. Comme déjà dit, l'ACSI demande le respect du principe du opt-in: le traitement de données ne doit se faire qu'avec le consentement exprès de la personne concernée. Il faut donc que cette notion soit intégrée à l'article 13. Cela vaut d'autant plus à l'alinéa 3 relatif à la communication de données à des tiers ou à des catégories de destinataires. Il est nécessaire que les tiers soient facilement identifiables et expressément nommés et notifiés aux consommateurs. La simple acceptation de conditions générales par un clic ne suffit pas à définir cette acceptation comme un accord exprès. Il faut que la personne concernée soit rendue particulièrement attentive au traitement de ses données. Par ailleurs, la transmission de données à des fins marketing, notamment à des pseudo-partenaires, doit être particulièrement cadrée et ne peut être permise sans une acceptation expresse par le consommateur.
ACSI	LPD	14	1		Selon cet alinéa, le responsable du traitement est délié du devoir d'information au sens de l'art. 13 lorsque la personne concernée dispose déjà des informations correspondantes. L'ACSI refuse cet alinéa qui amène trop d'insécurité juridique. Selon les circonstances, ces informations ont été données il y a très longtemps. Cela signifie qu'il y a une sorte de procuration en blanc au traitement des données lorsque l'information a été donnée une fois. Il faudrait dès lors que le responsable du traitement informe lors de chaque changement la personne concernée.
ACSI	LPD	15	1		La formulation, qui prévoit que le responsable du traitement informe la personne concernée lorsqu'une décision qui a des effets juridiques sur elle ou qui l'affecte de manière significative est prise exclusivement sur la base d'un traitement automatisé, n'est pas suffisante. La plupart des décisions de ce type ont des effets juridiques : cela signifie que cela laisse une importante marge d'interprétation. Le Conseil fédéral devrait définir de manière plus claire ce que sont ces décisions qui ont des effets

					juridiques.
ACSI	LPD	18	1		L'ACSI salue cet article qui va dans le bon sens. Néanmoins, le respect des principes de protection des données par défaut et dès la conception ne doit pas seulement être une obligation du responsable du traitement, cela doit aussi être une obligation des constructeurs, fabricants, développeurs. Si l'on pense à un logiciel informatique, à une caméra, un téléphone portable ou une voiture connectée, ce n'est pas le responsable du traitement (qui sera souvent l'utilisateur) qui pourra respecter ces principes, mais c'est le fabricant qui doit les appliquer et permettre leur application dès la conception / fabrication. La protection des données dès la conception n'est pas suffisante et une interdiction doit être faite aux fabricants et développeurs de prévoir des portes dérobées (backdoors) et toutes autres mesures permettant un accès aux données à l'insu de la personne concernée. De plus, la terminologie utilisée (« mesures appropriées », « prévenir les atteintes ») pour cet article réduit sa portée. Nous proposons donc une modification de l'article 18 al. 1 : Dès la conception du traitement, le responsable du traitement et le sous-traitant, notamment le développeur, le constructeur ou le fabricant, doivent prendre toutes les mesures qui assurent qu'il n'y ait pas d'atteinte à la personnalité et aux droits fondamentaux de la personne concernée.
ACSI	LPD	18	2		Le principe de la protection par défaut (privacy by default) est ancré dans cet alinéa. Revendication de longue date des organisations de consommateurs, cet alinéa répond aux besoins matériels d'une loi moderne sur la protection des données, applicable au monde numérique. L'ACSI soutient dès lors tout particulièrement cet alinéa. Dans le cas de données personnelles qui ne sont pas nécessaires à la finalité du traitement, les fabricants doivent prévoir une procédure d'opt-in pour tout transfert de données à des tiers.
ACSI	LPD	20	1		L'article 20 de l'avant-projet prévoit un droit d'accès très large pour le consommateur. Il pourra notamment demander gratuitement l'identité et les coordonnées du responsable du traitement, les

					données traitées, la finalité du traitement, la durée de conservation ou les critères pour fixer cette dernière et les informations disponibles sur l'origine des données. Cela est à saluer.
ACSI	LPD	20	5		Selon l'art. 20 al. 5, le sous-traitant doit fournir les renseignements demandés, s'il ne révèle pas l'identité du responsable du traitement. Il n'y aucune justification à ce que le sous-traitant ne puisse pas révéler qui traite les données de la personne concernée. Au contraire, celle-ci doit avoir le droit de savoir par qui ses données sont traitées. Cela va de plus à l'encontre de l'art. 13 al. 4 AP-LPD. La partie de la phrase «s'il ne révèle pas l'identité du responsable du traitement » doit dès lors être biffée.
ACSI	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.
ACSI	LPD	23	3		L'art. 23 al. 3 devrait reprendre la formulation proposée à l'art. 6 al. 1 lit. e) : En règle générale, il n'y a pas d'atteinte à la personnalité lorsque la personne concernée a rendu les données personnelles accessibles publiquement à tout un chacun et ne s'est pas opposée expressément à la collecte.
ACSI	LPD	25	1	c	S'agissant des prétentions qu'un consommateur pourra faire valoir, il a été ajouté, par rapport à la loi actuelle, la mention du droit à l'effacement. Cela correspond à la revendication du droit à l'oubli et c'est un point à saluer.
ACSI	LPD	27	3	b	L'art. 27 al. 3 lit. b devrait reprendre la formulation proposée à l'art. 6 al. 1 lit. e) : la personne concernée y a consenti ou a rendu ses données personnelles accessibles publiquement à tout un chacun et ne s'est pas opposée expressément à la collecte.
ACSI	LPD	29	2	d	L'art. 29 al. 2 lit. d devrait reprendre la formulation proposée à l'art. 6 al. 1 lit. e) : la personne concernée a rendu ses données personnelles accessibles publiquement à tout un chacun et ne s'est pas opposée expressément à la collecte.
LPD	50	Ss			Des instruments légaux sont nécessaires pour mettre de la pression pour une application effective du droit. L'élargissement du catalogue des infractions, de même qu'une augmentation importante des

					amendes est dès lors à saluer. Par contre, deux éléments importants doivent être corrigés : 1. Seules les personnes privées peuvent être amendées, soit selon notre interprétation les personnes physiques. Si tel est le cas, il s'agit d'une limitation qui n'est pas acceptable. Les sociétés doivent également pouvoir être poursuivies. Dans le monde numérique, ce sont évidemment les personnes morales qui sont responsables du traitement et non des personnes physiques. La limitation aux personnes privées des poursuites pénales est bien évidemment un affaiblissement important de l'effet préventif de ces dispositions. La poursuite pénale doit dès lors être élargie aux personnes morales. 2. Les art. 50ss ne prévoient pas de renvoi à l'art. 4 AP-LPD, qui pose les principes de la loi. Or, si des violations des principes de la loi sont constatés, celles-ci doivent également pouvoir faire l'objet d'une sanction. Le catalogue des infractions devrait dès lors être élargi à l'art. 4.
ACSI	CPC	99 113 114	3 2	d g f	L'ACSI salue particulièrement les modifications des articles du CPC qui prévoient de ne pas percevoir de sûretés ou de frais judiciaires concernant les litiges relevant de la loi sur la protection des données. En effet, il s'agit d'un domaine où la valeur litigieuse est difficilement calculable. Les frais judiciaires empêchent souvent que le particulier ouvre action, alors que celle-ci est totalement justifiée.

L'ADIDE
Association pour le dictionnaire des droits de l'enfant

Département fédéral de justice
et police
Office fédéral de la justice
3003 Berne

BA Justiz
E - 4. April 2017
Act

Genève, le 3 avril 2017

Concerne : renforcement de la protection des données – procédure de consultation

Madame, Monsieur,

L'Association pour le dictionnaire des droits de l'enfant (L'ADIDE) a été créée au mois de décembre 2016 dans le double but suivant : élaborer un Dictionnaire des droits de l'enfant destiné aux enfants de 11 à 14 ans et expérimenter des espaces de diffusion de ces mêmes droits pour cette tranche d'âge de la population.

Ses deux membres fondatrices, soussignées, ont pris connaissance avec un très vif intérêt du projet de révision totale de la loi fédérale sur la protection des données. Ce projet rejoint leurs contributions professionnelles axées sur la promotion des droits de l'enfant, et en l'occurrence la mise en valeur des droits personnels des enfants d'âge préscolaire

L'ADIDE tient à vous faire part des réflexions et propositions suivantes qui portent essentiellement sur le **renforcement et la clarification des droits de la personne et des droits touchant à la sécurité.**

Remarque générale

En matière de protection des données, ce sont les individus qui doivent assumer la défense de leur vie privée face à la collecte et à l'usage inadéquat de leurs données personnelles. En tant que « personnes concernées », ils sont à tout moment menacés d'être **réduits au statut d'objets**

- faute de pouvoir être constamment et durablement attentifs aux données qui circulent sur leur compte ;
- faute de posséder l'énergie, le temps et les ressources pour se défendre contre une entreprise qui transmet ou exploite des informations privées sans information ou accord préalable.

Certes, les individus livrent volontiers et imprudemment des fragments de leur vie privée ; ce comportement n'est de loin pas la seule explication à leur utilisation commerciale. Car l'exploitation de ces données devient souvent une condition sine qua non pour accéder à certains services.

La future loi doit avoir pour objectif de réduire le poids disproportionné qui repose sur les personnes assujetties aux collectes de données personnelles qui menacent leur vie privée. Les droits individuels doivent être renforcés, les droits de tous en général et ceux des personnes vulnérables en particulier.

Cette législation très spécifique doit poursuivre une **perspective pédagogique**, dans un but de formation des individus à la prudence et au contrôle face à leurs propres données. Cela est possible si une place suffisante est réservée au souci de lisibilité et de maniabilité de la future loi.

adresse : c/o M-F. Lücker-Babel – 5 chemin du Fort-de-l'Ecluse – 1213 Petit-Lancy / Genève
courriel : adide@romandie.com
téléph : 41 78 759 45 38

Suppression de la notion de « fichier » et de l'annonce systématique des fichiers

- L'avant-projet de loi supprime toute notion de « fichier » pour se limiter à une appellation vague de « traitement des données » (art. 3 lettre d) que le responsable du traitement devra « documenter » (art. 19). Il est proposé de renoncer au recensement des fichiers, pour des raisons de bureaucratie et de lourdeur administrative excessives (Rapport explicatif, p. 62).

- Nous sommes d'avis que de tels termes sont insuffisamment précis pour que les « personnes concernées » puissent **comprendre** l'étendue des processus en cours et la nature de leurs droits.

- Le renoncement à l'annonce systématique des « traitements de données » constitue une régression.

- Il est impératif de préciser les formes que devra prendre la documentation des « traitements », afin de donner une base légale claire à l'obligation qui incombe aux entreprises et de légitimer les contrôles qui devront ou pourront être effectués.

Exigence de sécurité

- L'exigence de sécurité (actuellement à l'art. 11) doit être élevée au rang de principe ; sa place est dans le prolongement de l'art. 4.

Question du consentement au traitement de données

- Le consentement est une des conditions de base de la licéité d'un traitement de données. L'art. 4 al. 6 est difficile à comprendre : quels sont les cas dans lesquels un consentement n'est pas nécessaire ? Quelle est l'articulation avec l'art. 13 et l'art. 24 al. 1 ?

- Pourquoi le « devoir d'informer » (art. 13) n'est-il pas couplé à un devoir de recueillir le consentement (ou de ne pas agir sans le consentement) de la personne concernée ?

Impossibilité de renoncer à tout ou partie de ses droits

- L'interdiction de renoncer à tout ou partie des droits conférés par la loi doit être stipulée à l'art. 4 et non uniquement en relation avec le « droit d'accès » (art. 20 al. 6).

Obligation de répondre avec célérité aux demandes personnelles

- Lorsque le droit d'accès est exercé (art. 20), le responsable du traitement doit avoir l'obligation de répondre avec célérité.

Mise en valeur des droits individuels

- L'interdiction du traitement de données personnelles, la rectification, l'effacement et la destruction de données et par conséquent une certaine forme du « droit à l'oubli » sont formulés comme des « prétentions » (art. 25 al. 1 – Section 5 « Dispositions particulières pour le traitement de données par des personnes privées »).

- En tant que **droits individuels essentiels**, reconnus à toute personne concernée, ils doivent être mis en exergue. Leur place est **dans le prolongement de la reconnaissance du « droit d'accès »** (art. 20).

- Là également, le responsable du traitement doit avoir l'obligation de répondre avec célérité.

Réserver une place aux personnes vulnérables et aux enfants

Leur place est extrêmement réduite dans tout l'avant-projet de loi ; elle apparaît limitée au « besoin de protection des personnes vulnérables » (art. 8 al. 1) et à la mission de « sensibiliser le public, et en particulier les personnes vulnérables, à la protection des données personnelles » (art. 49 lettre c). Ce ne sont que des « attributions » confiées au Préposé fédéral à la protection des données et pas des garanties directement apportées à ces segments de la population. Par comparaison, les données relatives à une personne décédée font l'objet d'une disposition complète et détaillée, qui est élevée au rang de « disposition générale » (section 2), par ailleurs absolument légitime et justifiée (art. 12).

L'obligation de protéger la population incombe aux autorités exécutives, législatives et judiciaires, mais aussi aux entreprises dans la mesure où leur activité est susceptible d'avoir des effets sur les individus ou les groupes d'individus et sur leurs droits fondamentaux (art. 35 al. 3 Cst). L'attention spécifique aux publics fragiles s'impose comme une évidence, elle ne peut pas être de la responsabilité unique (et très restreinte) du Préposé fédéral.

Par conséquent, des règles doivent être énoncées qui s'appliquent à tous les responsables du traitement de données, dans le but d'assurer **une protection particulière aux personnes mineures**, conformément à la prescription de l'art. 11 Cst. Les données concernant les enfants vont les accompagner leur vie durant : admission dans une école, recherche d'emploi, compétition sportive, demande de naturalisation, etc.

Cette longévité, cette permanence des données personnelles négligent totalement les caractéristiques de l'enfance, le **« droit d'avoir été un enfant »** et le fait que tout enfant aura traversé les péripéties propres à cette partie de la vie. En outre, une partie de ces données ont été fournies par les responsables légaux sans que l'enfant, même capable de discernement, ait pu y consentir. **La garantie que les données de l'enfance pourront être effacées** doit faire l'objet d'une profonde réflexion.

Nous préciserons enfin que la proposition de l'art. 24a présentée ci-dessous se rapporte au traitement de données personnelles par des organismes privés, et non par des organismes publics qui agissent sur la base de la loi ou d'un mandat officiel.

La future loi doit reconnaître

- le droit des personnes mineures à l'« autonomie informationnelle »
- leur droit d'exercer directement leurs droits dans le contexte particulier du traitement de données personnelles (cf. art. 11 al. 2 Cst)
- leur droit à une information qui leur est directement donnée et aisément accessible
- leur droit d'influer elles-mêmes sur les processus de traitement de leurs données lorsqu'elles ont atteint l'âge de 16 ans ou la majorité
- leur droit au respect de leur sphère privée par rapport aux données qu'elles ont elles-mêmes remises ou qui ont été collectées directement auprès d'elles.

Propositions concrètes relatives aux personnes mineures

Art. 4 – Principes

- al. 6 (nouveau) : « Toute personne capable de discernement est habilitée à exercer les droits que lui confère la présente loi. »

Art. 8 – Recommandations de bonnes pratiques

- dans la mesure où une disposition spécifique relative aux personnes mineures est adoptée, la mention de ce public dans l'art. 8 al. 1 ne nous paraît pas absolument nécessaire.

Article 13 – Devoir d'informer lors de la collecte de données personnelles

- al. 1 : comment comprendre la notion de « tiers », dans le cas où les parents fournissent des données personnelles relatives à leur enfant ?

- al. 6 (nouveau) : « Le responsable du traitement informe les personnes intéressées directement, le cas échéant dans une forme qui tient compte des capacités des personnes mineures ou vulnérables. » (cf. Règlement UE 2016/679, art. 12.1)

Article 23 – Atteintes à la personnalité

- al. 2, lettre e (nouveau) : « faire du profilage de personnes mineures. »

Article 24a – Données concernant les personnes mineures (nouveau)

1. Le traitement de données personnelles concernant des personnes mineures ne peut avoir lieu qu'avec le consentement express des parents ou des représentants légaux.

2. Si les personnes mineures sont capables de discernement, le consentement de ces dernières est requis en sus du consentement des parents ou des représentants légaux. (cf. Règlement de l'UE 2016/679, art. 8)

3. Les personnes mineures de plus de 16 ans peuvent elles-mêmes consentir au traitement de données, pour autant que les responsables du traitement fixent préalablement les conditions de la communication aux parents ou responsables légaux des données personnelles remises par ces personnes mineures ou obtenues d'elles.

4. Les responsables du traitement mettent fin au traitement de données personnelles concernant des personnes mineures dès que celles-ci atteignent la majorité, à moins que la personne concernée consente expressément à la poursuite du traitement. Les cas prévus à l'article 24 al. 2 lettres d et e [de l'actuel AP-LPD] sont réservés.

5. La personne mineure de plus de 16 ans capable de discernement et toute personne majeure de moins de 20 ans peut demander la fin du traitement, la rectification, l'effacement ou la destruction des données la concernant. Les cas prévus à l'article 24 al. 2 lettres d et e sont réservés.

6. [Nul ne peut renoncer d'avance aux garanties susmentionnées.]

L'extension partielle de cette protection à d'autres catégories de personnes vulnérables (personnes âgées, illettrées, endettées, etc.) pourra être étudiée (*mutatis mutandis*).

Art. 49 – Autres attributions

- il est nécessaire de compléter les attributions du préposé (lettre c (mots soulignés)) :

  c. sensibiliser le public, et en particulier les personnes mineures et les personnes vulnérables, à la protection des données personnelles ;

En résumé

La loi sur la protection des données est le seul outil législatif susceptible d'offrir une protection ciblée face au traitement des données personnelles. Elle doit énoncer clairement l'ensemble des droits de toutes les personnes concernées et les limites des traitements de données.

Elle doit aussi être vue comme un instrument destiné à sensibiliser la population et ayant une portée pédagogique, ce dont témoignent les attributions confiées au Préposé fédéral à la protection des données et à la transparence.

Vu sous cet angle, l'avant-projet de révision nécessite un rééquilibrage en faveur du besoin de protection de la population. Il doit mieux mettre en avant les droits des personnes concernées et souligner l'impératif d'une protection adéquate notamment à l'égard des groupes de la population présentant des caractéristiques particulières (personnes mineures et personnes vulnérables).

De même que l'introduction de l'article 11 de la Constitution (protection des enfants et des jeunes) a représenté un grand pas en avant, l'adoption d'une disposition spécifique consacrée aux personnes mineures sera, le jour venu, un légitime motif de fierté pour les autorités fédérales.

Veuillez agréer, Madame, Monsieur, nos salutations distinguées.

pour L'ADIDE

Marie-Françoise Lücker-Babel
Dr. iur.
Membre fondatrice de L'ADIDE

Francine Koch
Lic. pédagogie (phil. I)
Membre fondatrice de L'ADIDE

Copie : OFAS, Domaine Affaires internationales
diverses ONG suisses actives dans le domaine des droits de l'enfant

BA Justiz
E - 5. April 2017
Act

Eidg. Justiz- und Polizeidepartement
- 4. April 2017

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Dintikon, 31. März 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 Antennen-Genossenschaft Dintikon (AGD) gerne wahr.

Die AGD 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

---

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.

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 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 ha-

[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.

ben 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.

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

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.

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 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	**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
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 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 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,

VE-DSG	Anträge und Bemerkungen
	die Bearbeitung 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
	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.
[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

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" Datenbear-

VE-DSG	Anträge und Bemerkungen
	beitern 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), 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.	**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	**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"

VE-DSG	Anträge und Bemerkungen
Auswirkungen auf die betroffene Person hat.	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 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 Persönlich-	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschät-

VE-DSG	Anträge und Bemerkungen
keit 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. [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.	zungen 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, 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

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.	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. **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,

VE-DSG	Anträge und Bemerkungen
	diese in ihren Persönlichkeiten schützen.
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 Begrün-

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.	dungspflicht 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 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 be-	

VE-DSG	Anträge und Bemerkungen
arbeitet werden; 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: 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;	**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.

VE-DSG	Anträge und Bemerkungen
f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das 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:	**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
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; 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	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem 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 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 For-	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
schung, Planung und Statistik bearbeiten, wenn: 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	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [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.	

VE-DSG	Anträge und Bemerkungen
[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 [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	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Par-

VE-DSG	Anträge und Bemerkungen
Vorgehen und das Ergebnis einer allfälligen Untersuchung.	teistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte 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.	**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
[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; 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

VE-DSG	Anträge und Bemerkungen
	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.
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 unter-	**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
nehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c 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;	**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.

VE-DSG	Anträge und Bemerkungen
f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert. [2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**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. **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.

VE-DSG	Anträge und Bemerkungen
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone [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.	Keine Bemerkungen
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....	**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.

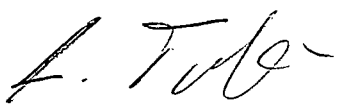
VE-DSG	Anträge und Bemerkungen
Art. 113 Abs. 2 Bst. g [2] Keine Gerichtskosten werden gesprochen in Streitigkeiten: g. nach dem Datenschutzgesetz vom ..... *Art. 114 Bst. f* Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom ..... *Art. 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 ...	

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

[Name] Armin Tobler
[Funktion] Präsident Antennen-Genossenschaft Dintikon



Amstutz Jonas BJ

Von: Olivia Solari <Olivia.Solari@agvs-upsa.ch>
Gesendet: Donnerstag, 23. März 2017 09:08
An: Amstutz Jonas BJ
Betreff: Stellungnahme VE-DSG
Anlagen: 20170323_VE-DSG Stellungnahme AGVS.doc

Sehr geehrter Herr Amstutz

Gerne übermittle ich Ihnen in der Anlage unsere Stellungnahme.

Vielen Dank für Ihre geschätzte Kenntnisnahme und bei allfälligen Rückfragen stehe ich gerne zur Verfügung.

Freundliche Grüsse
Auto Gewerbe Verband Schweiz (AGVS)

Olivia Solari
Rechtsdienst (Master of Law)

AGVS/UPSA
Wölflistrasse 5, Postfach 64
3000 Bern 22
Tel. Zentrale 031 307 15 15
Tel. direkt 031 307 15 34
Fax 031 307 15 16
olivia.solari@agvs-upsa.ch
www.agvs-upsa.ch / www.autoberufe.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 : Auto Gewerbe Verband Schweiz

Abkürzung der Firma / Organisation : AGVS

Adresse : Wöflistrasse 5, 3000 Bern 22

Kontaktperson : Olivia Solari

Telefon : 031 307 15 34

E-Mail : olivia.solari@agvs-upsa.ch

Datum : 23.03.17

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 ____ **2**

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ **3**

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
AGVS	Der AGVS nimmt zu den Regelungen des VE-DSG Stellung, welche die Privatwirtschaft, und dort insbesondere die Garagen betrifft. Auf eine Stellungnahme zu den übrigen Regeln des VE-DSG und die weiteren Anpassungen in Zusammenhang mit Schengen, wird hingegen verzichtet. Der AGVS ist mit der Verschärfung des Datenschutzes in der vorgeschlagenen Form nicht einverstanden. Ob eine Äquivalenz mit Regeln der EU erreicht werden wird, hängt von sehr vielen (auch nicht ausschliesslich im Datenschutzrecht anzusiedelnden) Fragestellungen ab, auf welche die vorliegende Gesetzgebung kaum oder gar keinen Einfluss hat. Äquivalenz darf nicht mit „Gleichförmigkeit“ gleichgesetzt und nicht um jeden Preis zu erlangen versucht werden. Auf gar keinen Fall dürfen neue Bestimmungen über das hinausgehen, was die EU-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
AGVS	DSG	2	1		Der Verzicht auf den Schutz von Daten juristischer Personen ist aus Sicht von AGVS 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.
AGVS	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.
AGVS	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;»
AGVS	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 AGVS 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.
AGVS	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.
AGVS	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: […]»
AGVS	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 AGVS 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.
AGVS	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.
AGVS	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.
AGVS	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.
AGVS	DSG	8			**Empfehlungen der guten Praxis:** Der AGVS 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.
AGVS	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.
AGVS	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.
AGVS	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.
AGVS	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.
AGVS	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.
AGVS	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.
AGVS	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“
AGVS	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.)
AGVS	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.
AGVS	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.“
AGVS	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.
AGVS	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.
AGVS	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.
AGVS	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.
AGVS	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 AGVS 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 AGVS 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.
AGVS	DSG	20/21			**Auskunftsrecht:** Die Information darüber, wie bestimmte Entscheide zustande kommen, gehört zum Geschäftsgeheimnis einer Unternehmung und ist demnach, insbesondere in der aktuell vorgesehen, detaillierten Form gemäss Art. 20 Abs. 3 VE-DSG, klar unverhältnismässig. 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.
AGVS	DSG	20	3		Die Regel von Art. 20 Abs. 3 VE-DSG muss gestrichen werden. Dies ist konsequent, da sich der AGVS 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.
AGVS	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.
AGVS	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 agvs verweist auf die diesbezügliche Stellungnahme von economiesuisse („Vorschlag der Wirtschaft“), welche vollumfänglich unterstützt wird..
AGVS	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

Amstutz Jonas BJ

Von: Morath Carmen <c.morath@amsuisse.ch>
Gesendet: Montag, 3. April 2017 13:43
An: Amstutz Jonas BJ
Betreff: Vernehmlassung
Anlagen: Stellungnahme Vernehmlassung Totalrevision DSG und weitere Erlasse.docx

Sehr geehrter Herr Amstutz

Als Beilage finden Sie die Stellungnahme unseres Verbandes betreffend

- *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*

vorab elektronisch. Das Original-Schreiben erhalten Sie auf dem Postweg.

Freundliche Grüsse

Carmen Morath

Carmen Morath
Assistentin Recht/Unternehmensführung

AM Suisse
Seestrasse 105, Postfach, 8027 Zürich
T +41 44 285 77 03, F +41 44 285 77 24
c.morath@amsuisse.ch
www.amsuisse.ch

AM Suisse
Arbeitgeberverband
Carmen Morath
Seestrasse 105, Postfach, 8027 Zürich
T +41 44 285 77 03, F +41 44 285 77 24
c.morath@amsuisse.ch
www.amsuisse.ch

Einschreiben
Bundesamt für Justiz
Herr Jonas Amstutz
Bundesrain 20
3003 Bern

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

Zürich, 3. April 2017

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 AM Suisse ist der Arbeitgeber- und Berufsverband des Metallgewerbes. Die 1'850 Mitgliedbetriebe im Stahl- und Metallbau sowie in der Landtechnik beschäftigen 20'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von 5 Milliarden Franken.

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 AM Suisse dankt für die Möglichkeit zur Stellungnahme.

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, dass nur bei nicht ausreichendem Schutz durch unternehmensinterne Prozesse und Massnahmen, eine Datenschutz-Folgeabschätzung an den Datenschutzbeauftragten zu erfolgen hätte.

- 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 Metallbaubetrieb oder ein Landtechnikunternehmen verfügt über Kundendaten. Zudem nimmt der online-Verkauf (gerade in der Landtechnik) 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 AM Suisse. 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.

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 AM Suisse ablehnt.

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 CHF 500'000.- oder Freiheitsentzug bis 3 Jahre für Widerhandlungen im DSG schiessen weit übers Ziel hinaus. Die Totalrevision des Datenschutzgesetzes darf nicht in eine Kriminalisierung der Unternehmen bzw. verantwortlicher Privatpersonen münden.

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 und eine adäquate Umsetzung 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 AM Suisse 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.

Wir danken für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

AM Suisse
Arbeitgeberverband

Christoph Andenmatten
Direktor

Cyrine Zeder
Leiterin Recht/Soziales/Unternehmensführung

Amstutz Jonas BJ

Von: Dohr Volker <volker.dohr@amag.ch>
Gesendet: Dienstag, 4. April 2017 23:51
An: Amstutz Jonas BJ
Betreff: Stellungnahme zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes VE-DSG
Anlagen: VE-DSG Stellungnahme - AMAG Automobil und Motoren .doc

Sehr geehrter Herr Amstutz

Der Bundesrat hat 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.“
Ebenfalls am 11. Januar 2017, wurde der so genannten US-Privacy Shield verkündet hat, und damit im Datenaustausch zu und mit Amerika ein doch viel niedrigeres Datenschutzniveau als vorherrschaend als akzeptabel und offenbar genügend betrachtet hat.

Die Verschärfung des Schweizer Entwurfs des DSAG verwundert daher insbesondere.

Daher bitten wir um Berücksichtigung, dass das Datenschutzgesetz nur insoweit zu revidieren, ist als dies die internationalen Vorgaben zwingend erfordern.
Jeder darüberhinausgehende „Swiss Finish“ ist im obigen Sinnes des Bundesrates abzulehnen.

Besten Dank für ihre Kenntnisnahme.

Freundliche Grüsse
Volker Dohr

amag

AMAG Automobil- und Motoren AG
Leiter Legal & Compliance
Prokurist

Utoquai 47/49, 8008 Zürich
Assistenz +41 44 269 53 10
Direkt +41 44 269 53 50
volker.dohr@amag.ch

Diese Mitteilung ist vertraulich. Wenn Sie nicht der vorgesehene Empfänger sind, bitten wir Sie, diese E-Mail zu löschen und uns umgehend zu benachrichtigen. Danke. **Ce message est confidentiel.** Si vous n'êtes pas le destinataire, nous vous prions d'effacer cet e-mail et de nous en informer immédiatement. Merci. **Questo messaggio contiene delle informazioni di natura confidenziale.** Qualora non foste il destinatario corretto, La preghiamo di comunicarlo immediatamente al mittente e di distruggere il presente messaggio. Grazie. **This message is confidential.** If you are not the intended recipient, please delete the e-mail and contact us immediately. Thank you.

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 : AMAG Automobil und Motoren AG

Abkürzung der Firma / Organisation : AMAG

Adresse : Utoquai 49, 8008 Zürich

Kontaktperson : Volker Dohr

Telefon : +41 44 269 53 50

E-Mail : volker.dohr@dohr.ch

Datum : 3.4.2017

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!

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 ____ 2

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ 4

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
AMAG	Die AMAG-Gruppe ist eine im Jahr 1945 in der Schweiz gegründete Unternehmensgruppe die bis heute zu 100 % im Schweizer Familienbesitz ist, welche hauptsächlich im Automobilhandel tätig ist und die kommende Zeit als Teil einer gesamtheitlichen Mobilität in der Schweiz mitgestalten wird. Die Unternehmensgruppe beschäftigt über 5600 Mitarbeitende, davon über 700 Lernende und gehört zu den 50 grössten Schweizer Unternehmen. Die Zukunft der Mobilität wird zu einem Grossteil von passenden Mobilitätsangeboten bestimmt, die von Informationen der Fahrzeuge und der Mobilitätssuchenden bestimmt sein werden, auch um die künftige Verkehrsstrategie des Bundes umzusetzen. Nur mittels Datenerhebung und eines Datenaustausches zu vernünftigen Rahmenbedingungen, die auch ein mittelständisch geprägtes Unternehmen leisten kann wird die Schweiz und damit auch die AMAG Automobil und Motoren AG zukünftig Mobilität aus eigenen Mitteln gestalten können. AMAG nimmt zu den Regelungen des VE-DSG kursorisch Stellung, wo die Privatwirtschaft, und insbesondere ihre Vertragspartner 300 selbständige KMU Garagenbetriebe, betroffen sind. Auf eine Stellungnahme zu den übrigen Regeln des VE-DSG und die weiteren Anpassungen in Zusammenhang mit Schengen, wird hingegen verzichtet. Der vorliegende Gesetzesentwurf widerspricht diametral den Zielsetzungen des Bundesrates zur Förderung des Wirtschaftsstandortes Schweiz und des allgemeinen Wohlstandes! Er bewirkt vielmehr einen im höchsten Masse bedenklichen Standortnachteil, der neben Grossunternehmen

	insbesondere die heimischen KMUs überfordert und existentiell gefährdet. Diese Verschärfung verwundert insbesondere da der Bund, wie zuvor bereits die Europäische Union, 14 Tage nach dem Erlass des VE-DSG, am 11. Januar 2017, den so genannten US-Privacy Shield verkündet hat, und damit im Datenaustausch zu und mit Amerika ein nach unserer Ansicht doch viel niedrigeres Datenschutzniveau als akzeptabel und offenbar genügend betrachtet hat. Aus diesen Gründen lautet die Forderung wie folgt: Das Datenschutzgesetz ist nur insoweit zu revidieren, als dies die internationalen Vorgaben **zwingend** erfordern. Jeder darüberhinausgehende „Swiss Finish“ (im vorliegenden Entwurf zum Beispiel im Bereich Profiling, Auskunftsrecht Datenschutzfolgeabschätzung und Sanktionssystem besonders gravierend) ist abzulehnen. Für die Berücksichtigung der Anliegen der Kommunikations-, Mobilitäts- und Kleingewerbebranche zur Schaffung einer verhältnismässigen und praxistauglichen Datenschutzregulierung danken wir Ihnen im Voraus und stehen Ihnen für Rückfragen gerne zur Verfügung. Im Folgenden wird auf zentrale Punkte aus Sicht der AMAG als Schweizer Mobilitätsdienstleister und seiner 300 KMU Vertragspartner, die nicht in der Lage sind zu diesem Gesetzentwurf Stellung zu nehmen, eingegangen.:

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
AMAG	DSG	3		a	*Klarstellung zum Begriff der Personendaten* Die Beibehaltung der bisherigen Auslegung und 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 anderen Seite wird im Bericht eine natürliche Person als bestimmbar erklärt, wenn sie „über Hinweise auf eine Identifikationsnummer oder über 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 sowie dem Interesse an der Identifizierung. 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 verschiedener Kommentatoren unter der EU-DSGVO einerseits eine Singularisierung für das Vorliegen von Personendaten ausreichen soll und andererseits von anderen Autoren mit überzeugenden Argumenten dies abgelehnt wird, bedarf einer Klarstellung. Zum anderen ergibt sich eine derart strenge Auslegung auch nicht aus dem erläuternden Bericht (E-SEV 108). Deshalb besteht keine Notwendigkeit, sie im Schweizer Recht einzuführen (Swiss Finish).
AMAG	DSG	3		f	*Begriff des Profilings ist zu weit* 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 oder für manuelle Entscheidungen gelten. Für die im erläuternden Bericht angesprochenen Bearbeitungen bspw. im Rahmen von Big Data Analysen genügen die übrigen Regelungen, da bei einem Profiling, das am Ende zu Personendaten führt, gelten diese Regelungen ohnehin. Darüber hinaus wird die Unsicherheit, welche konkreten Bearbeitungen in der Praxis als Profiling zu betrachten sind, durch den entsprechenden Zusatz weiter verstärkt.
AMAG	DSG	6	1	b	***Begriff der Einwilligung - keine separate Information bzw. Einwilligung*** Die vorgeschlagene Änderung hinsichtlich des 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 Kommunikation und Mobilitätsbranche von hoher 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 Kommunikation 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.
AMAG	DSG	7			**Auftragsdatenbearbeitung - keine Information hierüber geg. Dritten erforderlich** 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). Es handelt sich hierbei um **Wettbewerbsvorteile und Geschäftsgeheimnisse, mit welchen Partnern zusammengearbeitet** wird. Sie wäre in der **Praxis auch nicht praktikabel, da Geschäftspartner wechseln oder ausgelagerte Dienstleistungen zu einem späteren Zeitpunkt eventuell wieder selbst durchgeführt werden könnten**. 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.
AMAG	DSG	12			**Daten einer verstorbenen Person - Regelung ist nicht erforderlich** Die Einführung einer Regelung zu den Rechten an den Daten verstorbener Personen ist im Hinblick auf die Angemessenheit des Schweizer Datenschutzrechts nicht zwingend erforderlich da eine Bearbeitung solcher Daten kaum noch erfolgt, da keine neuen Daten erzeugt werden, ferner die Unternehmen kaum ein Interesse an einer solchen Datenbearbeitung haben und führt für die Unternehmen zum Schluss zu einem erheblichen administrativen Mehraufwand (Swiss Finish). Auf die Regelung ist daher zu verzichten.
AMAG	DSG	13			**Art. 13 und Art. 15 DSG Informationspflicht - geht in Teilen über das notwendige hinaus** 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. Dies betrifft die Informationen zum Zeitpunkt der Datenerhebung und der Zustimmung sie können nur in diesem Zeitpunkt richtig sein. Falls erforderlich sollte eine Information auf der Webseite genügen. Die

					Nennung des Verantwortlichen in Persona ist weder zielführend, und aufgrund von Personalwechsel auch nicht zielführend. Die Mitteilung einer Meldestelle ist hier genügend. Die Mitteilung einer allfälligen Datenbearbeitung durch externe Dienstleister gehört in den meisten Fällen zum Geschäftsgeheimnis und sollte ebenfalls nicht von der Informationspflicht umfasst sein. Die Information gemäss Art. 15 Abs. 1 über automatisierte Entscheidungen geht weit über das erforderliche hinaus und ist ebenfalls mit Ausnahmen oder Einschränkungen zu versehen. Abs. 2 ist gänzlich zu streichen. Diese und weitere Punkte im Zusammenhang mit der Informationspflicht stellen einen unnötigen "Swiss-Finish" dar und sind im Sinne der Digitalstrategie des Bundes auf ein vernünftiges Mass zu reduzieren damit insbesondere aufstrebende und innovative Branchen nicht durch administrativen Überhang gebremst werden.
AMAG	DSG	16	allg.		**Datenschutz-Folgenabschätzung (DSFA)** Die Anknüpfung an das Vorliegen „erhöhter Risiken“ führt zu einem viel zu weit gefassten Anwendungsbereich und geht unverständlicherweise weit über die Vorgaben der EU-DSGVO in Art. 35 hinaus. Als "Swiss Finish" ist die Datenschutz-Folgeabschätzung abzulehnen. Bei jedem Change in einer datenverarbeitenden Software müsste nach der Vorlage des Entwurfs eine Datenschutzfolgeabschätzung gemeldet werden. Das kann nicht zielführend sein, solange Risiko minimieren der Massnahmen im Challenge Prozess getroffen wurden und das Risiko überschaubar ist. Letztlich ist es im Interesse der Unternehmen Fehler in der Datenverarbeitung zu vermeiden.
AMAG	DSG	23	2	d	**Profiling nur mit Einwilligung - die grösste Verschärfung und Begünstigung ausländischer und internationaler Unternehmen die in der Schweiz ebenfalls Ihre Kunden online erreichen** 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 Kommunikation 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, insbesondere solange die Datenbearbeitungsgrundsätze eingehalten werden, ist nicht ersichtlich, wieso neben der Information stets zusätzlich auch eine Einwilligung erforderlich sein soll. **Diese Vorschrift verunmöglicht 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 Kommunikation und Angebote wären dann faktisch nur noch den grossen (insbesondere internationalen) L**og-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 wettbewerbsrechtlichen Überlegungen wohl nicht gewünscht.
AMAG	DSG	50 ff.			**Sanktionen - Verhinderung von Innovation durch Schaffung einer Angstkultur und bürokratische Sanktionsmechanismen** 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 wird bereit sein, seine Gründer und Mitarbeiter solch drastischen strafrechtlichen Risiken auszusetzen. Gute Unternehmer und Mitarbeiter werden **nicht mehr bereit sein in der Schweiz zu investieren** und strafrechtliche Verantwortung in den Unternehmen mitzutragen, wenn sie **dies im Ausland nicht müssen**. Sie werden Ihre Ideen dort umsetzen.

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

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

Freundliche Grüsse
Volker Dohr

AMAG Automobil- und Motoren AG
Leiter Legal & Compliance
Prokurist

Utoquai 47/49, 8008 Zürich
Assistenz +41 44 269 53 10
Direkt +41 44 269 53 50
volker.dohr@amag.ch

Amstutz Jonas BJ

Von:	Alain Bovard <abovard@amnesty.ch>
Gesendet:	Mittwoch, 5. April 2017 15:23
An:	Amstutz Jonas BJ
Cc:	Patrick Walder; Tanja Zangger; Diana Rüegg; Stefanie Rinaldi; Pierre-Antoine Schorderet
Betreff:	Avant projet de loi sur la protection des données, procédure de consultation
Anlagen:	170328_Datenschutz_Amnesty.docx; 170405_Datenschutz_Amnesty.pdf

Cher Monsieur,

J'ai le plaisir de vous faire parvenir en pièce jointe et juste dans les délais, la prise de position de la Section suisse d'Amnesty International sur l'avant-projet de loi sur la protection des données.

Je vous remercie par avance de bien vouloir y donner la suite qui convient et vous adresse mes salutations distinguées.

Alain Bovard
Politique des droits humains
Amnesty International
Section suisse
Speichergasse 33/Case postale
3001 Berne
T +41 31 307 22 23
F +41 31 307 22 33
M +41 78 748 99 92
Twitter :@abovard
www.amnesty.ch
http://www.facebook.com/amnesty.suisse

AMNESTY
INTERNATIONAL

Monsieur
Jonas Amstutz
Office fédéral de la Justice
3003 Berne
PER E-MAIL

Berne, le 28 mars 2017

Avant-projet de loi sur la protection des données, prise de position de la Section suisse d'Amnesty International

Au niveau international, il est de plus en plus reconnu que le traitement de données personnelles touche en principe la sphère privée et qu'il est susceptible d'affecter d'autres droits fondamentaux. Pour garantir une protection efficace de la sphère privée, des bases légales suffisantes doivent être créées pour justifier ces ingérences. La limitation de la protection de la sphère privée doit en particulier respecter les exigences fixées à l'art. 8 par. 2 CEDH (nécessité d'une base légale, existence d'un motif justificatif, proportionnalité).

La révision doit d'une part renforcer les dispositions légales de protection des données figurant dans la loi fédérale du 19 juin 1992 sur la protection des données (LPD) pour faire face au développement fulgurant des nouvelles technologies et d'autre part tenir compte des réformes du Conseil de l'Europe et de l'Union européenne en la matière.

Le but de la révision est sur le fond de garantir un traitement des données plus transparent et de renforcer le droit de chacun de disposer de ses propres données. L'avant-projet, dès lors qu'il vise à en renforcer les garanties matière de protection des droits humains, doit être salué.

Amnesty International se réjouit à ce titre du renforcement des obligations du responsable de traitement (art. 13 à 19 AP-LPD), en plus particulièrement de l'introduction du principe de protection dès la conception (art. 18 AP-LPD). Il s'agit là d'un principe essentiel pour s'assurer que le consentement de la personne concernée est réellement pris en compte. L'effet rétroactif accordé à ce principe par l'article 59 lit. b doit également être salué.

AMNESTY INTERNATIONAL Section suisse . Schweizer Sektion . Sezione svizzera . Speichergasse 33 . Case postale . 3001 Berne
T: +41 31 307 22 22 . F: +41 31 307 22 33 . info@amnesty.ch . www.amnesty.ch . CP: 30-3417-8 . IBAN CH52 0900 0000 3000 3417 8

Amnesty International salue également l'adjonction expresse du droit à l'effacement des données (art. 25 al. 1 lit. c AP-LPD) ainsi que l'octroi de compétences décisionnelles en matière de mesures provisoires (art. 42 AP-LPD) et administratives (ART. 43 AP-LPD) au Préposé fédéral à la protection des données et à la transparence.

Cela étant, la Section suisse d'Amnesty International, à la lumière du but de la révision totale de la loi, formule les remarques ci-dessous:

- ***Ad* art. 8 et 9 AP-LPD**: L'activité d'élaboration de recommandations de bonne pratique par le Préposé doit être saluée, en tant que cela formalise et développe les tâches d'information et de conseil d'ores et déjà assumées par le Préposé. De même, la participation des responsables de traitement à ce procédé est à encourager, dès lors que des processus de régulation concertée des traitements de données, en particulier dans le domaine numérique, sont à même d'en favoriser le respect. Cela étant, le caractère facultatif de ces recommandations, qui correspondent pourtant matériellement à la loi, laisse à craindre que les milieux intéressés ne s'y réfèrent que dans une mesure relative. Le défaut de conséquences du refus d'approbation par le Préposé de recommandations émises par un responsable de traitement ou par les milieux intéressés est également regrettable, en tant que le respect de la loi par les recommandations de bonne pratique émanant directement des responsables de traitement apparait comme facultative. L'introduction d'une étape supplémentaire en cas de refus d'approbation du Préposé serait donc judicieuse, le responsable de traitement ainsi débouté devant être invité à soumettre une version modifiée de sa recommandation de bonne pratique ou, à défaut, à abandonner cette dernière.

- ***Ad* art. 41 à 43 AP-LPD**: L'élargissement des pouvoirs d'investigation et de contrôle du Préposé (art. 41 AP-LPD) à l'endroit de tout responsable de traitement quant auquel il existe un soupçon de traitement contraire à la loi est sans conteste favorable à une meilleure application des normes de protection par les milieux intéressés. L'octroi de compétences décisionnelles au Préposé doit également être salué, dès lors qu'il est sans nul doute de nature à renforcer l'efficacité de la loi (art. 42 et 43 AP-LPD). Dès lors, le choix de la voie pénale, au détriment d'un pouvoir de sanction du Préposé, déçoit. L'octroi de compétences répressives à l'autorité précitée, à l'instar de ses homologues européens, est de nature à renforcer la mise en œuvre des dispositions de protection comme d'en simplifier l'exécution. *A contrario*, la multiplication des procédures en lien avec la saisine des autorités de justice pénales, de surcroît non nécessairement spécialisées en la matière, présente un risque de ralentissement des procédures. La voie de la poursuite pénale mènera en outre à davantage de sanctions des personnes physiques, en lieu et place des personnes morales.

L'avant-projet de Loi sur la protection des données ne va ainsi pas aussi loin que ce que l'on aurait pu espérer dans le renforcement des garanties de protection. Ce texte demeure toutefois et sans conteste un

renforcement des droits des personnes concernées et la Section suisse d'Amnesty International soutient son adoption.

Avec nos meilleures salutations

Amnesty International
Section suisse

Amstutz Jonas BJ

Von:	Fournier Guillaume <Guillaume.Fournier@mll-legal.com>
Gesendet:	Dienstag, 4. April 2017 17:16
An:	Amstutz Jonas BJ
Cc:	rojas@tradamarca.com; 'Aropi Secrétaire'; Président AROPI
Betreff:	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
Signiert von:	guillaume.fournier@mll-legal.com
Wichtigkeit:	Hoch

Madame, Monsieur,

L'AROPI est une association de droit suisse qui aborde tous les aspects de la protection de la propriété intellectuelle. Avec près de 200 membres, l'AROPI est l'une des grandes associations en matière de propriété intellectuelle en Suisse.
Dans le cadre de ses activités, le l'AROPI 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'AROPI 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 intellectuelle (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.

L'AROPI 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, l'AROPI 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.

En vous remerciant de l'attention que vous porterez à la présente, je vous prie de croire, Madame, Monsieur, à mes salutations distinguées.

AROPI – Guillaume Fournier, Président
www.aropi.ch

Schweizerischer Pensionskassenverband
Association suisse des Institutions de prévoyance
Associazione svizzera delle Istituzioni di previdenza
Kreuzstrasse 26
8008 Zürich

Telefon 043 243 74 15/16
Telefax 043 243 74 17
E-Mail info@asip.ch
Website www.asip.ch

Frau Bundesrätin
Simonetta Sommaruga
Eidgenössisches Justiz- und
Polizeidepartement
Bundeshaus West
3003 Bern
jonas.amstutz@bj.admin.ch

Zürich, 4. April 2017

Vernehmlassung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG)

Sehr geehrte Frau Bundesrätin

Gerne nehmen wir zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG) Stellung.

Enthält das Spezialrecht strengere Datenschutznormen oder – wie in der obligatorischen beruflichen Vorsorge – eine in sich geschlossene Datenschutzkonzeption, so gehen diese Bestimmungen ausnahmsweise jenen des allgemeinen DSG vor («lex specialis»). Soweit allerdings nicht eine abschliessende spezialgesetzliche Norm vorliegt, müssen die registrierten Vorsorgeeinrichtungen immer auch die allgemeinen Bestimmungen von Art. 4ff. DSG beachten. Schliesslich sind die Grundsätze des Datenschutzgesetzes auch bei der Auslegung bereichsspezifischer Normen zu berücksichtigen (A-4467/2011 vom 10.04.2012).
Mit Ausnahme von Art. 85a Bst. f BVG und Art. 86a Abs. 2 Bst. bbis BVG gelten die datenschutzrechtlichen Bestimmungen des BVG jedoch nicht in der weitergehenden und ausserobligatorischen beruflichen Vorsorge (vgl. Art. 49 Abs. 2 Ziff. 25a und 25b BVG; Art. 89a Abs. 6 Ziff. 5a, Abs. 7 Ziff. 2 ZGB), in welcher lediglich die Bestimmungen des DSG zur Anwendung kommen.
Für die obligatorische berufliche Vorsorge beantragen wir, im neuen Art. 85a BVG, der auch für die Freizügigkeitsstiftungen gilt (Art. 25 FZG), den Begriff «Persönlichkeitsprofile» nicht ersatzlos zu streichen, sondern durch «Profiling» zu ersetzen.

Für die über- und ausserobligatorische Vorsorge, d.h. für registrierte und nicht registrierte Vorsorgeeinrichtungen mit reglementarischen Leistungen und für nicht registrierte Vorsorgeeinrichtungen mit Ermessensleistungen, beantragen wir zudem eine Änderung von Art. 49 Abs. 2 Ziff. 25a BVG, Art. 89a Abs. 6 Ziff. 5a und Art. 89a Abs. 7 Ziff. 2 ZGB dahingehend, dass der Verweis auf

Art. 85a BVG in diese Bestimmungen aufgenommen und der Verweisungstext durch «Bearbeiten von Personendaten» entsprechend ersetzt wird. Eventualiter beantragen wir ersatzlose Streichung von Art. 4 Abs. 6, 2. Satz E-DSG und Art. 23 Abs. 2 lit. d E-DSG, da sämtliche Einrichtungen der beruflichen Vorsorge im über- und ausserobligatorischen Bereich für ihre Aufgaben Daten im Sinne des in Art. 3 lit. f E-DSG definierten Begriffs «Profiling» bearbeiten müssen.

Als dem Zweck der beruflichen Vorsorge hinderlich erachten wir im Weiteren die Strafbestimmungen von Art. 50f. E-DSG. Das geltende DSG kennt von der Übertretungsnorm gemäss Art. 34 DSG abgesehen keine nennenswerten Strafbestimmungen. Erfasst werden neu auch fahrlässige Datenschutzverstösse. Dies führt letztlich zu einer stossenden Kriminalisierung von Organen und Mitarbeitern. Die Bussenobergrenze von CHF 500'000 (für vorsätzliche Tatbegehung) und CHF 250'000 (für fahrlässige Tatbegehung) ist massiv. Es fragt sich darüber hinaus, ob die Strafbestimmungen den strafrechtlichen Prinzipien wie dem Selbstbelastungsverbot, dem Bestimmtheitsgebot und dem Verschuldensprinzip genügen. Insbesondere lehnen wir auch die Einführung einer neuen beruflichen Schweigepflicht in Art. 52 E-DSG ab, deren Missachtung eine Freiheitsstrafe bis zu drei Jahren droht.
Wir beantragen deshalb ebenso die Aufnahme der Schweigepflicht gemäss Art. 86 BVG, welche für sämtliche das BVG-Obligatorium durchführenden registrierten Vorsorgeeinrichtungen und für sämtliche Freizügigkeitsstiftungen (vgl. Art. 25 FZG) gilt, in die Art. 49 Abs. 2 BVG und Art. 89a Abs. 6 und 7 ZGB. Dadurch werden sämtliche Vorsorgeeinrichtungen und Freizügigkeitsstiftungen Art. 76 BVG unterstellt, der als lex specialis dem Art. 52 E-DSG vorgeht und dessen Strafsanktionen sich in einem vernünftigen Mass bewegen.

Die Datenschutz-Folgeabschätzung (Art. 16 E-DSG) erachten wir ebenfalls als für die Durchführung der beruflichen Vorsorge hinderlich, da diese – insbesondere für kleinere Vorsorgeeinrichtungen – im Verhältnis zum Nutzen der Folgeabschätzung als zu aufwändig erscheint. Dasselbe gilt für die in Art. 17 E-DSG normierte Meldung von Verletzungen des Datenschutzes, welche in der Praxis häufig vorkommen dürften. Eine Meldepflicht steht ebenso der Durchführung der beruflichen Vorsorge entgegen, namentlich unter dem Aspekt der scharfen Strafdrohung bei Verletzung der Meldepflicht (vgl. Art. 50 Abs. 2 lit. e E-DSG). Wir beantragen deshalb eine Reduktion der Meldepflicht auf ein vernünftiges Mass, mindestens auf das Niveau der EU. Generell sind Melde- und Informationspflichten auf das Notwendige zu reduzieren.
Würden die Vorsorgeeinrichtungen im über- und ausserobligatorischen Bereich der beruflichen Vorsorge hinsichtlich der Bearbeitung von Personendaten und der Schweigepflicht dem DSG unterstellt, so wäre es ihnen nicht mehr möglich, die für die berufliche Vorsorge essentiellen Tätigkeiten wie beispielsweise die Beurteilung von Leistungsansprüchen und die Berechnung und Gewährung von Leistungen sowie die Koordinierung derselben mit Leistungen anderer Sozialversicherungen reibungslos durchzuführen, da gemäss Art. 4 Abs. 6, 2. Satz E-DSG – im deutlichen Unterschied zum noch geltenden Art. 12 DSG – für die Bearbeitung von besonders schützenswerten Personendaten und das Profiling die Einwilligung des jeweiligen Versicherten ausdrücklich

erfolgen muss und gemäss Art. 23 Abs. 2 lit. d E-DSG das in Art. 3 lit. f E-DSG definierte «Profiling» ohne ausdrückliche Einwilligung der betroffenen Personen per se persönlichkeitsverletzend ist.

Wir danken Ihnen für die Berücksichtigung unserer Hinweise und ersuchen Sie freundlich, unsere Position zu berücksichtigen.

Mit freundlichen Grüssen

A S I P

Schweizerischer Pensionskassenverband

Jean Rémy Roulet
Präsident

Hanspeter Konrad
Direktor

Amstutz Jonas BJ

Von: Pauline Darbellay <pdarbellay@figeas.ch>
Gesendet: Freitag, 31. März 2017 15:31
An: Amstutz Jonas BJ
Cc: Vincent Hort; Hélène Wetzel; Serge Husmann
Betreff: Consultation sur l'avant-projet de LPD - Prise de position d'Assura-Basis SA et d'Assura SA
Anlagen: Prise de position Assura-Basis SA et Assura SA_31.03.17.doc

Cher Monsieur,

Dans le cadre de la consultation sur l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données, nous vous prions de trouver ci-joint les remarques générales d'Assura-Basis SA et d'Assura SA sur l'avant-projet précité.

Nous restons bien entendu à votre entière disposition pour toute éventuelle question que vous pourriez avoir et vous remercions par avance de l'attention que vous porterez à notre prise de position.

Veuillez recevoir, cher Monsieur, l'expression de nos salutations distinguées.

Pauline Darbellay

Avocate
Service juridique

Avenue C.-F. Ramuz 70
Case postale 531

CH-1009 Pully

+41 21 544 37 36

Absente lundi et mercredi

http://www.figeas.ch

pdarbellay@figeas.ch

Par respect de l'environnement, n'imprimez ce courriel qu'en cas de nécessité ! Merci.
Schonen Sie die Umwelt ! Drucken Sie diese E-Mail nur aus, wenn es unbedingt notwendig ist. Danke.
In segno di rispetto per l'ambiente, stampare questa email solo se necessario! Grazie.

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 : Assura-Basis SA et Assura SA

Abréviation de la société / de l'organisation :

Adresse : Av. C.-F. Ramuz 70, 1009 Pully

Personne de référence : Pauline Darbellay

Téléphone : 021/544.37.36

Courriel : pdarbellay@figeas.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

Remarques générales 3

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 5

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 5

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel 6

Rapport explicatif (excepté chap. 8 « Commentaire des dispositions») 6

Rapport explicatif : chap. 8 « Commentaire des dispositions » 7

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 :
Assura-Basis SA et Assura SA	De manière générale, l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données introduit de nombreuses mesures administratives lourdes qui seront irréalistes à mettre en place, voire impossible à réaliser, et ceci sans pour autant apporter de réelles garanties supplémentaires pour les personnes dont les données sont traitées. On pense notamment à : - l'anonymisation des données dès que celles-ci n'ont plus vocation à être traitées et ceci avant que leur destruction ne soit nécessaire (art. 4 al.4 AP-LPD) ; - l'augmentation de la liste des informations à communiquer obligatoirement aux personnes concernées selon l'art. 20 al. 2 AP-LPD (trop d'informations aux personnes qui ne les lisent finalement pas) ; - la communication qui doit être faite à la personne concernée en cas de sous-traitance par le responsable du traitement (identité et coordonnées du sous-traitant, les données personnelles ou catégories de données personnelles concernées). En matière d'assurance-maladie, la transmission des informations précitées aux assurés chaque fois que leurs coordonnées ou numéros de téléphone sont communiqués à des sous-traitants (sociétés de services informatiques ou spécialisées, agents, etc.) est irréalisable. Cette obligation doit impérativement être supprimée.
	En ce qui concerne le traitement automatisé des données, le fait de garantir le droit d'être entendu à la personne concernée à chaque fois qu'une décision individuelle la concernant est prise sur une base automatique est disproportionné. A titre d'exemple, si l'on prend en compte le traitement automatisé des factures des assurés, il faudrait selon l'art. 15 al. 2 AP-LPD offrir la possibilité à tous les assurés de se déterminer sur la décision acceptant ou refusant la prise en charge de certaines prestations. Ceci aurait pour effet non seulement d'alourdir les processus et d'engendrer des retards parfois conséquents dans le remboursement des frais aux assurés, mais également d'augmenter d'une part non négligeable les frais administratifs des assureurs, sans pour autant apporter de réelle plus-value aux assurés. L'art. 15 AP-LPD apporte des restrictions à la liberté contractuelle par l'introduction de nouveaux droits et obligations (devoir d'informer et droit d'être entendu) et s'ingère dans le droit matériel tel que la LPGA, la LCA, etc.

	Au vu de ce qui précède, le devoir d'informer la personne concernée du traitement automatisé de ses données est suffisant.
	Une gestion séparée des données personnelles inexactes ou dont l'exactitude ne peut être établie sur des supports informatiques différenciés est totalement disproportionnée (financièrement et techniquement) et difficile à mettre en œuvre. De plus, l'on ne comprend pas quelle serait la plus-value apportée à la personne concernée, celle-ci bénéficiant déjà d'un droit à la modification de la donnée erronée. De plus, l'exigence d'un lien de causalité entre la donnée inexacte et le traitement erroné qui en résulterait devrait être intégrée dans la loi. A défaut, la personne concernée pourrait user beaucoup trop facilement de son droit découlant de l'art. 34 al.2 AP-LPD pour empêcher le traitement de certaines de ses données et ceci même si la donnée inexacte n'aurait aucun impact sur le traitement à proprement dit.
	Finalement, la définition de « profilage » prévue à l'art. 3 let. f) AP-LPD est trop large et floue. De plus, l'exigence du consentement exprès de la personne concernée en cas de profilage (art. 4 al. 6 AP-LPD) est disproportionné car il s'agit du traitement de données personnelles qui ne sont pas nécessairement sensibles. Ainsi, un consentement libre et éclairé est suffisant. On relèvera encore qu'il est difficile d'un point de vue pratique d'obtenir le consentement exprès d'un assuré.
	Pour le surplus, Assura-Basis SA et Assura SA se joignent à la prise de position établie par santésuisse.

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 :
	AP-LPD	5	6		Le responsable du traitement ne devrait pas avoir à informer le préposé du fait qu'il recourt aux garanties standardisées étant donné que ces garanties ont déjà été approuvées par celui-ci (art. 5 al. 3 let. c) AP-LPD).

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 :

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 :

Rapport explicatif (excepté chap. 8 « Commentaire des dispositions»)

nom/société	chap. n°	remarque / suggestion :

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 :**

Eidgenössisches Justiz- und
Polizeidepartement
Frau Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

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

Bern, 04. April 2017

Stellungnahme zum Vorentwurf Totalrevision Datenschutzgesetz sowie zu weiteren Änderungen und Beschlüssen

Sehr geehrte Frau Bundesrätin

Im Dezember 2016 wurden interessierte Kreise zur Vernehmlassung über die Totalrevision des Datenschutzgesetzes sowie über weitere Änderungen und Beschlüsse eingeladen. Wir bedanken uns für die Möglichkeit zur Stellungnahme und nehmen diese hiermit fristgerecht war.

Die digitale Transformation der Wirtschaft betrifft alle Branchen und bietet der Schweizer Wirtschaft gute Chancen, sich im internationalen Wettbewerb erfolgreich zu behaupten. Gerade die wissensintensiven und innovativen Produkte und Dienstleistungen der Schweizer Unternehmen profitieren von der Digitalisierung und den dadurch verfügbaren Daten und Informationen. Gemäss der Strategie «Digitale Schweiz» vom April 2016 teilt der Bundesrat diese Sicht und setzt sich gleichermassen dafür ein, dass sich die Wirtschaft im digitalen Raum möglichst frei entfalten kann und dass die Schweizer Bevölkerung die Informations- und Kommunikationstechnologien kompetent und sicher nutzen können.

Die Bedeutung der Daten als Rohstoff einer digitalen Wirtschaft unterstreicht der Bundesrat mit seiner Absicht, eine nationale Datenpolitik festzulegen. Damit soll, so die Medienmitteilung vom 22. März 2017, die Schweiz als attraktiver Standort für eine Wertschöpfung durch Daten positioniert werden. Der vorliegende Vorentwurf zur Totalrevision des Datenschutzgesetzes muss daher in diesem Kontext beurteilt werden. Hatte das Datenschutzgesetz bisher den Zweck, den Schutz der Persönlichkeit und der Grundrechte natürlicher Personen, über die Daten bearbeitet werden, zu gewähren, so muss das zukünftige Datenschutzgesetz eine Balance zwischen Schutz und Nutzen sicherstellen. Zwischen den Ansprüchen von Individuen bezüglich Schutz persönlicher Daten und den Anforderungen einer datenbasierten Wirtschaft in einem globalen Wettbewerb.

Zentrale Aspekte der Revision sind durch den Entscheid des Europarates und die Entwicklung in der EU bereits vorgespurt. Aus Sicht der asut ist es zwingend, dass die Schweizer Datenschutzgesetzgebung von der EU als gleichwertig anerkannt wird, damit der grenzübergreifende Datenaustausch weiterhin effizient möglich bleibt. Gleichzeitig gilt es hier Mass zu halten: Die Schweiz soll sich nur soweit der EU-Gesetzgebung annähern, wie es für einen Angemessenheitsbeschluss der EU-Kommission notwendig ist. Auf zusätzliche Schweizer Anforderungen ist zu verzichten (Swiss-Finish). Eine schlanke Revision des Datenschutzgesetzes soll den Datenaustausch mit dem Ausland sicherstellen und gleichzeitig den administrativen Aufwand für Schweizer Unternehmen möglichst geringhalten.

asut
Schweizerischer Verband der Telekommunikation
Klösterlistutz 8
3013 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

@asut_ch

asut sieht daher die Notwendigkeit einer raschen Revision des Datenschutzgesetzes, wobei für eine moderate Anpassung an die Europäische Gesetzgebung eigentlich keine Totalrevision notwendig ist. Wie von Ihnen gewünscht, erhalten Sie unsere detaillierte Stellungnahme zu den einzelnen Punkten des Vorentwurfs in der beiliegenden Tabelle. An dieser Stelle möchten wir einige wenige grundsätzliche Aspekte hervorheben:

- asut begrüsst die Revision des Datenschutzgesetzes und die Schaffung moderner Rahmenbedingungen für eine Datenwirtschaft in der Schweiz. Dazu ist die Vereinbarkeit mit den Vorgaben aus dem Europarat und der EU sicherzustellen. Darüber hinaus soll auf zusätzliche Auflagen und Pflichten möglichst verzichtet werden.
- In diesem Sinne anerkennen wir, dass im Vorentwurf der Wirtschaft mit den Empfehlungen zur guten Praxis eine aktivere Rolle zuerkannt wird. Zudem unterstützen wir den Verzicht auf die Beweislastumkehr, die Datenportabilität oder die kollektive Rechtsdurchsetzung. Solche Massnahmen stellen gerade für Schweizer KMU eine unverhältnismässige Last dar und würden die Schweizer Wirtschaft im internationalen Wettbewerb unnötig schwächen.
- Wir müssen jedoch auch feststellen, dass die erweiterten Informationspflichten, Dokumentationspflichten und Meldepflichten sowie Vorgaben zu Privacy-by-Design, Privacy-by-Default oder Datenschutzfolgeabschätzungen einen erheblichen Mehraufwand für die betroffenen Unternehmen bedeuten werden. Gerade KMUs welche das Rückgrat der Schweizer Wirtschaft darstellen, werden durch diese Auflagen finanziell belastet. Daher wünschen wir uns hier einen «risikobasierten Ansatz», wonach sich der Umfang der Pflichten am Risiko der Datenbearbeitung orientiert.
- Ablehnend stehen wir zudem Neuerungen gegenüber, die weitergehen, als für einen Angemessenheitsbeschluss notwendig wäre. Ein solcher «Swiss Finish» findet sich beispielsweise bei einigen Informationspflichten, bei weitergehenden Anforderungen zum Profiling, bei tieferen Hürden zur Datenschutzfolgeabschätzung oder bei der Anzeigepflicht des EDÖB. Dieser «Swiss Finish» schadet dem Wirtschaftsstandort Schweiz und ist daher abzulehnen.
- asut anerkennt die Notwendigkeit eines moderaten Ausbaus des Sanktionssystems und der Stärkung der Stellung des EDÖB. Die massive Verschärfung des Strafregimes stellen wir jedoch in Frage, sowohl in qualitativer (Höhe der Bussen) als auch in quantitativer (Anzahl sanktionierender Bestimmungen) Hinsicht. Stossend ist zudem die strafrechtliche Sanktionierung fahrlässiger Datenschutzverletzungen durch Einzelpersonen. Dies führt zu nicht abschätzbaren Risiken für Unternehmen und Mitarbeitende und damit letztlich zu einer Lähmung der Datenwirtschaft in der Schweiz.

Wir sind überzeugt, dass mit einigen Anpassungen das Datenschutzgesetz sowohl den Anforderungen einer modernen Datenwirtschaft als auch den Bedürfnissen der Bevölkerung nach Schutz der Persönlichkeit und der eigenen Daten erfüllen kann. Unsere Vorschläge dazu finden Sie in der beiliegenden Stellungnahme. Wir bitten Sie um eine wohlwollende Prüfung unserer Anliegen.

Freundliche Grüsse

asut – Schweizerischer Verband
der Telekommunikation

Peter Grütter
Präsident

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 der Telekommunikation

Abkürzung der Firma / Organisation : asut

Adresse : Klösterlistutz 8, 3013 Bern

Kontaktperson : Christian Grasser

Telefon : +41 31 560 66 66

E-Mail : grasser@asut.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 ____ 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ 5

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 ____ Fehler! Textmarke nicht definiert.

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ____ Fehler! Textmarke nicht definiert.

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") ____ Fehler! Textmarke nicht definiert.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" ____ Fehler! Textmarke nicht definiert.

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.	Die digitale Transformation der Wirtschaft betrifft alle Branchen und bietet der Schweizer Wirtschaft gute Chancen, sich im internationalen Wettbewerb erfolgreich zu behaupten. Gerade die wissensintensiven und innovativen Produkte und Dienstleistungen der Schweizer Unternehmen profitieren von der Digitalisierung und den dadurch verfügbaren Daten und Informationen. Gemäss der Strategie «Digitale Schweiz» vom April 2016 teilt der Bundesrat diese Sicht und setzt sich gleichermassen dafür ein, dass sich die Wirtschaft im digitalen Raum möglichst frei entfalten kann und dass die Schweizer Bevölkerung die Informations- und Kommunikationstechnologien kompetent und sicher nutzen können. Die Bedeutung der Daten als Rohstoff einer digitalen Wirtschaft unterstreicht der Bundesrat mit seiner Absicht, eine nationale Datenpolitik festzulegen. Damit soll, so die Medienmitteilung vom 22. März 2017, die Schweiz als attraktiver Standort für eine Wertschöpfung durch Daten positioniert werden. Der vorliegende Vorentwurf zur Totalrevision des Datenschutzgesetzes muss daher in diesem Kontext beurteilt werden. Hatte das Datenschutzgesetz bisher den Zweck, den Schutz der Persönlichkeit und der Grundrechte natürlicher Personen, über die Daten bearbeitet werden, zu gewähren, so muss das zukünftige Datenschutzgesetz eine Balance zwischen Schutz und Nutzen sicherstellen. Zwischen den Ansprüchen von Individuen bezüglich Schutz persönlicher Daten und den Anforderungen einer datenbasierten Wirtschaft in einem globalen Wettbewerb.
Fehler! Verweisquelle konnte nicht gefunden werden.	Zentrale Aspekte der Revision sind durch den Entscheid des Europarates und die Entwicklung in der EU bereits vorgespurt. Aus Sicht der asut ist es zwingend, dass die Schweizer Datenschutzgesetzgebung von der EU als gleichwertig anerkannt wird, damit der grenzübergreifende Datenaustausch weiterhin effizient möglich bleibt. Gleichzeitig gilt es hier Mass zu halten: Die Schweiz soll sich nur soweit der EU-Gesetzgebung annähern, wie es für einen Angemessenheitsbeschluss der EU-Kommission notwendig ist. Auf zusätzliche Schweizer Anforderungen ist zu verzichten (Swiss-Finish). Eine schlanke Revision des Datenschutzgesetzes soll den Datenaustausch mit dem Ausland sicherstellen und gleichzeitig den administrativen Aufwand für Schweizer Unternehmen möglichst geringhalten.
Fehler! Verweisquelle konnte nicht gefunden werden.	asut sieht daher die Notwendigkeit einer raschen Revision des Datenschutzgesetzes, wobei für eine moderate Anpassung an die Europäische Gesetzgebung eigentlich keine Totalrevision notwendig ist. Wie von Ihnen gewünscht, erhalten Sie unsere detaillierte Stellungnahme zu den einzelnen Punkten des Vorentwurfs in der beiliegenden Tabelle. An dieser Stelle möchten wir einige wenige grundsätzliche Aspekte hervorheben: asut begrüsst die Revision des Datenschutzgesetzes und die Schaffung moderner Rahmenbedingungen für eine Datenwirtschaft in der Schweiz. Dazu ist die Vereinbarkeit mit den Vorgaben aus dem Europarat und der EU sicherzustellen. Darüber hinaus soll auf zusätzliche Auflagen und

	Pflichten möglichst verzichtet werden. In diesem Sinne anerkennen wir, dass im Vorentwurf der Wirtschaft mit den Empfehlungen zur guten Praxis eine aktivere Rolle zuerkannt wird. Zudem unterstützen wir den Verzicht auf die Beweislastumkehr, die Datenportabilität oder die kollektive Rechtsdurchsetzung. Solche Massnahmen stellen gerade für Schweizer KMU eine unverhältnismässige Last dar und würden die Schweizer Wirtschaft im internationalen Wettbewerb unnötig schwächen. Wir müssen jedoch auch feststellen, dass die erweiterten Informationspflichten, Dokumentations-pflichten und Meldepflichten sowie Vorgaben zu Privacy-by-Design, Privacy-by-Default oder Datenschutzfolgeabschätzungen einen erheblichen Mehraufwand für die betroffenen Unternehmen bedeuten werden. Gerade KMUs welche das Rückgrat der Schweizer Wirtschaft darstellen, werden durch diese Auflagen finanziell belastet. Daher wünschen wir uns hier einen «risikobasierten Ansatz», wonach sich der Umfang der Pflichten am Risiko der Datenbearbeitung orientiert. Ablehnend stehen wir zudem Neuerungen gegenüber, die weitergehen, als für einen Angemessenheitsbeschluss notwendig wäre. Ein solcher «Swiss Finish» findet sich beispielsweise bei einigen Informationspflichten, bei weitergehenden Anforderungen zum Profiling, bei tieferen Hürden zur Datenschutzfolgeabschätzung oder bei der Anzeigepflicht des EDÖB. Dieser «Swiss Finish» schadet dem Wirtschaftsstandort Schweiz und ist daher abzulehnen. asut anerkennt die Notwendigkeit eines moderaten Ausbaus des Sanktionssystems und der Stärkung der Stellung des EDÖB. Die massive Verschärfung des Strafregimes stellen wir jedoch in Frage, sowohl in qualitativer (Höhe der Bussen) als auch in quantitativer (Anzahl sanktionierender Bestimmungen) Hinsicht. Stossend ist zudem die strafrechtliche Sanktionierung fahrlässiger Datenschutzverletzungen durch Einzelpersonen. Dies führt zu nicht abschätzbaren Risiken für Unternehmen und Mitarbeitende und damit letztlich zu einer Lähmung der Datenwirtschaft in der Schweiz.

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
asut	VE DSG	1			Ein zentrales Element der Revision des Datenschutzgesetzes ist es, die Wettbewerbsfähigkeit des Wirtschaftsstandortes Schweiz zu stärken. Dies wird im erläuternden Bericht zurecht mehrfach erwähnt. asut ist der Ansicht, dass dieses Ziel neu auch im Zweckartikel festgehalten werden soll. Das Datenschutzgesetz schränkt die Datenbearbeitung nicht nur ein, sondern ermöglicht und fördert sie im Interesse der Innovation und der wirtschaftlichen Entwicklung gleichermassen.
asut **Fehler! Verweisquelle konnte nicht gefunden werden.**	VE DSG	2			Die Einschränkung des Geltungsbereiches auf natürliche Personen wird begrüsst. Der Schutz von Daten juristischer Personen ist eine Schweizer Eigenheit und hat nur eine geringe praktische Relevanz. Vielmehr wurde das Auskunftsrecht im Bereich der Daten von juristischen Personen in der Praxis oftmals für datenschutzfremde Zwecke genutzt (z.B. Beschaffung von Beweismitteln).
asut	VE DSG	3	1	f	Die Definition von „Profiling“ geht über die Vorgaben der EU-DSGVO hinaus. Anders als in der EU-DSGVO ist auch das Profiling "von Hand" miterfasst, 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 der wirtschaftlichen 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 ist aus Sicht der asut nicht sachgerecht. Es ist zu beachten, dass eine Regelung, welche auch das manuelle Profiling beinhaltet und damit über die europäischen Vorgaben hinausgeht, zu erheblichen zusätzlichen Risiken für die Unternehmen führen würde. Deshalb ist asut der Ansicht, dass die Anwendung auf „automatisierte“ Auswertungen beschränkt werden muss. Ob für das Profiling Personendaten benutzt werden oder nicht, spielt zudem keine Rolle („Daten oder

					Personendaten“). Ein Profiling ist nur dann gegeben, wenn sich das Ergebnis auf eine bestimmte oder bestimmbare Person bezieht. Die Formulierung „Daten oder Personendaten“ ist trotzdem unnötig 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. ***Aus den genannten Gründen stellt asut den Antrag, Art. 3 Abs. 1 Bst. f VE DSG wie folgt anzupassen***: *„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;*
asut	VE DSG	4	3		Das zusätzliche Wort „klar“ führt nur zu Rechtsunsicherheit und Verwirrung. Zudem ist es auch nicht nötig: Die Deutlichkeit, mit welcher auf einen bestimmten Bearbeitungszweck hinzuweisen ist, ergibt sich schon unter dem heutigen Recht aus dem Risiko, das mit ihm für die betroffene Person verbunden ist. Das Wort „klar“ ist daher ersatzlos zu streichen. ***Aus den genannten Gründen stellt asut den Antrag, Art. 4 Abs. 3 VE DSG wie folgt anzupassen***: *[3] Personendaten dürfen nur zu einem bestimmten und ~~**klar**~~ erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.*
asut	VE DSG	4	5		In Abs. 5 wird neu eine Pflicht zur Korrektur der Daten statuiert. Diese Pflicht kann sehr aufwändig sein, insbesondere wenn die Daten von der Person aufgrund eines Vertrages selbst zur Verfügung gestellt worden sind. Auch eine proaktive Überprüfung der Richtigkeit der Daten ist in der Praxis gerade in Massengeschäften nicht praktikabel und in Fällen, wo eine Person ihre Daten selber zur Verfügung stellt, auch gar nicht nötig. Schliesslich sollte festgehalten werden, dass die Vernichtungspflicht in Abs. 5 (letzter Satz) nur gilt, wenn keine gesetzlichen oder regulatorischen Aufbewahrungsvorschriften bestehen. ***Aus den genannten Gründen stellt asut den Antrag, Art. 4 Abs. 5 VE DSG wie folgt anzupassen***:

					[5] *Wer Personendaten bearbeitet, muss* ***auf entsprechende Aufforderung des Betroffenen oder eines Dritten hin*** *überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden,* ***falls hinreichende Indizien dafür vorliegen, dass die Daten unrichtig oder unvollständig sind. Die Pflicht entfällt, wenn der diesbezügliche Aufwand für den Verantwortlichen erheblich ist oder die Daten von der betroffenen Person selber zur Verfügung gestellt wurden****. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Allenfalls sind die Daten zu vernichten,* ***ausser es bestehen gesetzliche oder regulatorische Aufbewahrungsvorschriften.***
asut	VE DSG	4	6		Das Wort „eindeutig" ist unnötig. Im Bereich der Einwilligung gilt 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. Das Wort „eindeutig" soll daher ersatzlos gestrichen werden. Zudem ist asut der Ansicht, dass das Schutzbedürfnis beim Profiling keine Ausdrücklichkeit erfordert. Die Einwilligung soll beim Profiling auch konkludent erteilt werden können. ***Aus den genannten Gründen stellt asut den Antrag, Art. 4 Abs. 6 VE DSG wie folgt anzupassen***: [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 besonders schützenswerten Personendaten* ***~~und das Profiling~~*** *muss die Einwilligung zudem ausdrücklich erfolgen.*
asut	VE DSG	5	1		Es ist unklar, ob Abs. 1 unabhängig von Abs. 2 gilt. Wäre dies der Fall, dann wäre auch bei schwerwiegender Gefährdung eine Bekanntgabe ins Ausland erlaubt. Abs. 1 soll deshalb ersatzlos gestrichen werden. ***Aus den genannten Gründen stellt asut den Antrag, Art. 5 Abs. 1 VE DSG zu streichen.***
asut	VE DSG	5	2		Abs. 2 soll dahingehend präzisiert werden, dass wenn einer der Fälle von Art. 5 oder 6 vorliegt, eine Bekanntgabe zulässig ist. ***Aus den genannten Gründen stellt asut den Antrag, Art. 5 Abs. 2 VE DSG wie folgt anzupassen:*** [2] *Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die*

					Gesetzgebung des betreffenden Staates einen angemessen Schutz ***gewährleistet oder die Voraussetzungen von Art. 6 vorliegen.***
asut	VE DSG	5	3	c 1 und d 1	Die Genehmigungspflicht gemäss Abs. 3 c 1 und d 1 ist eine klare Verschärfung und sowohl für die Unternehmen als auch für den EDÖB mit hohem Aufwand verbunden. Es erscheint asut auch nicht nachvollziehbar weshalb für standardisierte Garantien oder unternehmensinternen Datenschutzvorschriften strengere Vorgaben gelten sollten als für die "spezifischen Garantien" gemäss Bst. b. Nach Ansicht von asut genügt daher eine Informationspflicht anstelle der Genehmigungspflicht. ***Aus den genannten Gründen stellt asut den Antrag, Art. 5 Abs. 3 lit. c1 und d1 VE DSG wie folgt anzupassen:*** *Genehmigung ersetzen durch Informationspflicht.*
asut	VE DSG	5	5		Da asut eine Informationspflicht als ausreichend ansieht (siehe Antrag zu Art. 5 Abs. 3 VE DSG) soll dieser Absatz gestrichen werden. Sollte an der Genehmigungspflicht festgehalten werden, müsste die Frist von sechs Monaten stark reduziert werden. Diese Frist ist sehr lang und zielt an den Bedürfnissen der Praxis vorbei. Unternehmen können in den wenigsten Fällen Projekte und Datentransfers (mindestens) sechs Monate aussetzen. In der Praxis dürften Unternehmen auf "spezifische Garantien" ausweichen was nicht zielführend sein kann. ***Aus den genannten Gründen stellt asut den Antrag, Art. 5 Abs. 5 VE DSG zu streichen. Eventualiter sei die Mitteilungsfrist auf 30 Tage zu reduzieren.***
asut	VE DSG	5	6		Diese Pflicht zur ist neu und bedeutet eine administrative Bürde für alle Unternehmen. Auch der Beauftragte wird mit solchen Informationen überhäuft werden. Zudem ist diese Pflicht dem EU Recht fremd und somit ein "Swiss Finish". ***Aus den genannten Gründen stellt asut den Antrag, Art. 5 Abs. 6 VE DSG zu streichen.***
asut	VE DSG	6	1	c 2	Es ist unklar, was mit dem Begriff "Verwaltungsbehörden" gemeint ist und dies kann zu schwierigen Abgrenzungsfragen führen. Es soll daher, wie in der EU-DSGVO der Zusatz "vor einem Gericht oder einer Verwaltungsbehörde" gestrichen werden und "unerlässlich" durch "erforderlich" ersetzt werden. In der

					Botschaft soll dann der Begriff "Rechtsansprüche" dahingehend definiert werden, dass dieser auch straf- und verwaltungsrechtliche Massnahmen erfasst. ***Aus den genannten Gründen stellt asut den Antrag, Art. 6 Abs. 1 lit. c 2 VE DSG wie folgt anzupassen:*** c. *die Bekanntgabe im Einzelfall ~~unerlässlich~~ erforderlich ist für:* *1. die Wahrung eines überwiegenden öffentlichen Interesses, oder* *2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen ~~vor einem Gericht oder einer Verwaltungsbehörde~~;*
asut	VE DSG	6	2		Diese Pflicht zur Information des Beauftragten ist neu und bedeutet eine sehr hohe administrative Bürde für alle Unternehmen. Der Beauftragte wird mit solchen Informationen überhäuft werden und nicht in der Lage sein, diese innert nützlicher Frist zu bearbeiten. Zudem ist diese Pflicht dem EU Recht fremd, somit ein “Swiss Finish”. Sie ist ersatzlos zu streichen. ***Aus den genannten Gründen stellt asut den Antrag, Art. 6 Abs. 2 VE DSG zu streichen.***
asut	VE DSG	7	3		Abs. 3 entspricht in den Grundzügen der Regelung der EU-DSGVO. In der EU-DSGVO wurde jedoch klargestellt, dass auch eine generelle Einwilligung möglich ist, ohne Bezug auf die Unterauftragsbearbeiter. Die DSGVO verlangt für diesen Fall eine Informationspflicht des Auftraggebers vor Beizug eines neuen Unterauftragsbearbeiters und ein Vetorecht des Auftraggebers. Vor diesem Hintergrund erscheint eine Anpassung von Abs. 3 angebracht. Auch das Erfordernis der Schriftlichkeit geht u.E. zu weit und insbesondere wäre auch zu klären, was unter "Schriftlichkeit" genau gemeint ist. ***Aus den genannten Gründen stellt asut den Antrag, Art. 7 Abs. 3 VE DSG wie folgt anzupassen:*** *[3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen**, wobei auch eine generelle Einwilligung möglich ist. Der Auftragsbearbeiter hat in einem solchen Fall, den Verantwortlichen beim Beizug vorgängig zu informieren und dem Verantwortlichen steht ein Vetorecht zu**.*

asut	VE DSG	8 – 9			Als Branchenverband begrüsst asut ausdrücklich das neue Konzept der Empfehlungen der guten Praxis. Die grossen Herausforderungen im Bereich des Umgangs mit Daten können im Zeitalter der Digitalisierung und von "Big Data" nur zusammen angegangen und sinnvoll gelöst werden. Wie in den Erläuterungen richtigerweise festgehalten wird, bergen die vielen neuen und unbestimmten Rechtsvorschriften (Datenschutz-Folgeabschätzung, Modalitäten der Informationspflichten, Privacy-by-Default, Privacy-by-Design etc.) für die Unternehmen eine grosse Unsicherheit in Bezug auf ein korrektes Verhalten (vgl. Ziffer 8.1.2.5, S. 52). Damit besteht die Gefahr, dass die Unternehmen übervorsichtig agieren, was sich negativ auf die Entwicklung von neuen, innovativen Geschäftsmodellen und Dienstleistungen auswirken wird. Diese Gefahr wird durch die vorgesehene massive Verschärfung des Sanktionsregimes zusätzlich erhöht. Die zeitnahe Ausarbeitung von konkreten Empfehlungen wird daher zentral sein für die (Wieder-)Herstellung der notwendigen Rechtssicherheit. Für den Wirtschaftsstandort Schweiz ist es ausserdem von grosser Wichtigkeit, dass die Empfehlungen praxisnah ausgestaltet werden. Der Einbezug sowie die Berücksichtigung der Interessen der betroffenen Branchen und Unternehmen muss daher zwingend vorgeschrieben werden. Den Erläuterungen ist zu entnehmen, dass Art. 8 Abs. 1 VE DSG auch in diesem Sinne zu verstehen ist. In diesem Zusammenhang ist es jedoch überlegenswert, anstelle des EDÖB eine unabhängige Kommission mit Vertretern aus der Praxis einzusetzen, welche über die Genehmigung von Empfehlungen der guten Praxis bestimmt. Weiter unterstützt asut die in Art. 9 Abs. 2 VE DSG vorgesehene Regelung, wonach die Datenschutzvorschriften auch auf andere Weise eingehalten werden können, als die Empfehlungen der guten Praxis vorsehen. Dies scheint bereits aus rechtstaatlichen Überlegungen angezeigt.
asut	VE DSG	10			Die Ausdehnung der fakultativen Zertifizierungsmöglichkeit auf bestimmte Dienstleistungen wird begrüsst. Verarbeitungsvorgänge dürften im Vergleich zu Produkten oder Datenbearbeitungssystemen zunehmend an Bedeutung gewinnen.
asut	VE 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 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. Bei genauerem Betrachten fokussiert die Regelung wohl auf Daten einer verstorbenen Person auf Social-Media-Plattformen. Dann soll dies aber 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 des Fernmeldegeheimnisses, von Amts- und Berufsgeheimnissen in bereits bestehenden gesetzlichen Regelungen, für Telekommunikationsunternehmen z.B. nach Art. 43 FMG. 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. Dasselbe gilt für das Fernmeldegeheimnis. Nach alledem ist Art. 12 VE-DSG jedenfalls geeignet, statt der – heute nach Erbrecht bestehenden – Rechtssicherheit eher Widersprüche zu bestehenden gesetzlichen Regelungen zu produzieren. ***Aus den genannten Gründen stellt asut den Antrag, Art. 12 VE DSG zu streichen.*** Stattdessen ist soweit sinnvoll zu prüfen, inwieweit gezielte spezialgesetzliche Regelungen z.B. in Ergänzung von Art. 28 ff. ZGB sinnvoll erscheinen.
asut	VE-DSG	13	1-5		Zu Art. 1: Die Informationspflicht bei der Beschaffung von Personendaten geht deutlich weiter als die bisherige Regelung von Art. 14 DSG. So gilt die Informationspflicht gemäss Art. 13 Abs. 1 VE DSG neu für alle Personendaten während sie bisher auf besonders schützenswerte Daten und Persönlichkeitsprofile

					beschränkt war. Diese Ausdehnung dürfte vom Übereinkommen SEV 108 gefordert werden (Vgl. Art. 7bis). Auch die EU-DSGVO enthält eine ähnliche Regelung. Damit die Aufwände für die Unternehmen in der Praxis aber in einem vertretbaren Rahmen bleiben und die betroffenen Personen nicht von Informationen überflutet werden ist es wichtig, dass diese auch in allgemeiner Form (z.B. über eine standardisierte Datenschutzerklärung auf einer Webseite) erfolgen können. Dies müsste in Abs. 1 präzisiert werden zumal aus den Erläuterungen nicht klar hervorgeht, ob eine allgemeine Form in allen Fällen ausreichen würde. Zu Art. 2: Der genaue Umfang der zu übermittelnden Informationen gemäss Abs. 2 VE DSG bleibt unbestimmt. In den Erläuterungen wird diesbezüglich auch explizit von einer flexiblen Regelung gesprochen damit sichergestellt wird, dass die Verantwortlichen keine unnötigen Informationen übermitteln müssen. Dies ist zwar grundsätzlich zu begrüssen, aber es gilt darauf hinzuweisen, dass selbst eine fahrlässige Verletzung dieser flexiblen Informationspflicht gemäss Vorentwurf sanktioniert werden soll. Zwecks Risikominimierung dürften daher die Verantwortlichen viel mehr Informationen liefern als tatsächlich gefordert wäre, was selbstredend nicht das Ziel der Norm sein kann. Die Strafbarkeit für die Verletzung dieser Norm ist aus diesem Grunde zu hinterfragen zumal eine Verletzung der Informationspflicht nicht automatisch auch eine Verletzung der Persönlichkeit zur Folge haben muss (siehe dazu Anträge zu Art.50 VE DSG). Zu Art. 4: Vollumfänglich abzulehnen ist die Pflicht zur Information über die Identität und Kontaktdaten der Auftragsbearbeiter gemäss Abs. 4 VE DSG. Diese Informationspflicht geht zu weit und ist weder im Übereinkommen E-SEV noch in der EU-DSGVO vorgesehen ("Swiss Finish"). Die Bestimmung würde zu einer Flut von Informationen führen, die auch von den betroffenen Personen nicht erwünscht sein kann. In fast jedem Unternehmen der ICT-Branche ist der Beizug von externen Auftragsbearbeitern wie Projektberatern, Lieferanten, IT-Spezialisten, Call-Center Mitarbeitern, Revisionsstellen etc. gang und gäbe und ständigen Veränderungen unterworfen. Es wäre schlichtweg nicht praktikabel bei jeder Änderung die Identität und die Kontaktdaten all dieser Auftragsbearbeiter sämtlichen betroffenen Personen mitzuteilen. Der Aufwand wäre enorm und das Unterfangen sinnlos. Tatsächlich bleibt der Verantwortliche für die Bearbeitung der Personendaten durch seine Hilfspersonen vollumfänglich verantwortlich und die Auftragsdatenbearbeitung ist gemäss Art. 7 VE DSG bereits sehr strengen Regeln unterworfen. Insbesondere darf ein Auftragsbearbeiter die Daten nur so bearbeiten, wie es der Verantwortliche selbst tun dürfte. Zu Art. 5: Über die Regelungen des Übereinkommens E-SEV und der EU-DSGVO hinaus geht auch Abs. 5

					VE DSG, der eine Information der betroffenen Person bei einer indirekten Datenbeschaffung spätestens bei der Speicherung vorsieht. Auch diese Regelung erscheint praxisfremd da bei einer Datenbeschaffung die Daten meist zuerst gespeichert und erst dann gelesen werden. In Anlehnung an die Regelung der EU-DSGVO sollte hier eine angemessene Frist vorgesehen werden. ***Aus den genannten Gründen stellt asut den Antrag, Art. 13 VE DSG wie folgt anzupassen***: [1] *Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden.* ***Die Information kann mittels einer standardisierten Datenschutzerklärung erfolgen.*** [4] ***streichen*** [5] *Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person* ***innerhalb von 3 Monaten*** ~~*spätestens bei der Speicherung der Daten*~~ *informiert ……werden.*
asut	VE DSG	14	4	a	Der Katalog der Ausnahmeregelung ist enger gefasst als dies die Regelungen des Übereinkommens E-SEV und der EU-DSGVO vorsehen. Gemäss Abs. 4 Bst. a ist eine Berufung auf überwiegende private Interessen nur möglich, wenn die Personendaten nicht an Dritte weitergegeben werden. Diese Einschränkung macht keinen Sinn. Letztlich ist einzig entscheidend, ob die Interessen des Verantwortlichen überwiegen oder nicht. ***Aus den genannten Gründen stellt asut den Antrag, Art. 14 Abs. 4 Bst. a VE DSG wie folgt anzupassen***: *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;***~~
asut	VE DSG	15			Bei der Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung handelt es sich um eine neue Anforderung welche vom Übereinkommen E-SEV 108 gefordert sein dürfte. Damit die Aufwände für die Unternehmen in einem vertretbaren Rahmen bleiben, soll die Anhörungspflicht gemäss Abs. 2 in der Praxis jedoch konsequent auf Entscheide mit erheblichen Auswirkungen beschränkt bleiben.
asut	VE DSG	16	1		Die Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung stellt eine weitere neue Anforderung

			3-4		dar, welche in den Grundzügen vom Übereinkommen E-SEV gefordert sein dürfte. Auch dieses schreibt Datenschutz-Folgeabschätzungen vor. Die Anforderung dürfte aufgrund der sehr unbestimmten Formulierungen und fehlenden Empfehlungen der Praxis zu grossen Rechtsunsicherheiten führen. Insbesondere erscheint sehr offen, wann von einem "erhöhten" Risiko für die Persönlichkeit gesprochen werden kann. Gemäss den Erläuterungen (S.61) muss bereits dann von einem solchen gesprochen werden, wenn die Verfügungsgewalt der betroffenen Person erheblich eingeschränkt werden kann. Die "Hürde" scheint daher eher tief angesetzt. Zwecks Risikominimierung dürften die Unternehmen folglich bei den meisten Datenbearbeitungen entsprechende Abklärungen durchführen, zumal auch bei einer Verletzung dieser Norm hohe Sanktionen drohen. Um die Aufwände für die Unternehmen in einem vertretbaren Rahmen zu halten, sollen solche Datenschutzfolge-Abschätzungen nach Ansicht von asut jedoch die Ausnahme als die Regel darstellen. Analog den EU-Anforderungen ist es daher angebracht, diese Pflicht auf "hohe" Risiken zu beschränkten. Weiter ist es nicht gerechtfertigt, auch den Auftragsbearbeiter in die direkte Pflicht zu nehmen. Eine solche Ausdehnung der Durchführungspflicht ist weder im Übereinkommen E-SEV noch in der EU-DSGVO vorgesehen und wird in den Erläuterungen auch nicht begründet. Für jede Datenbearbeitung bleibt der Verantwortliche in der Pflicht. Entsprechend liegt es auch in seiner alleinigen Verantwortung, eine Datenschutz-Folgeabschätzung vorzunehmen oder durch einen Auftragsbearbeiter bzw. eine Hilfsperson vornehmen zu lassen. Der Auftragsbearbeiter darf seinerseits die Daten gemäss Art. 7 VE DSG auch nur so bearbeiten wie der Verantwortliche es selbst tun dürfte. Der Auftragsbearbeiter darf mit anderen Worten gar keine weitergehenden Bearbeitungen durchführen für die sich allenfalls eine Datenschutz-Folgeabschätzung aufdrängen würde. Zu streichen ist die vorgesehene Melde- und Prüfungspflicht. Eine solche allgemeine Meldepflicht ist in der EU-DSGVO nicht vorgesehen und würde zu problematischen Verzögerungen bei der Realisierung von Vorhaben und Projekten führen. Unternehmen müssten einen Vorlauf von einigen Monaten einplanen, da stets mit möglichen Einwänden des EDÖB gerechnet werden müsste. Eine solche überbordende Regulierung schadet der Wirtschaft und würde auch auf Seiten des EDÖB unnötig viele Ressourcen binden. Allenfalls liesse es sich rechtfertigen, solche Konsultationsverfahren auf die wirklich kritischen Fälle beschränken. ***Aus den genannten Gründen stellt asut den Antrag, Art. 16 VE DSG wie folgt anzupassen***:

					[1] *Der 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.* [3] ***streichen*** [4] ***streichen***
	VE DSG	17	1		Art. 17 sieht im Gegensatz zur EU DSGVO keine Frist zur Vornahme einer Meldung an den EDÖB vor. Die Frage der Auslegung des Begriffs der Unverzüglichkeit ist zudem offen, was zu Unsicherheiten führen kann. Art. 17 spricht zudem von einer Meldepflicht für eine „unbefugte" Datenverarbeitung, ohne dass Bagatellverstösse ausgeschlossen würden, da der erste Teilsatz sich nicht auf den zweiten Teilsatz (Meldepflicht bei Datenschutzverletzungen beschränkt auf Fälle, in denen die Verletzung nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt). Dies ist anzupassen. ***Aus den genannten Gründen stellt asut den Antrag, bei Art. 17 Abs. 1 VE DSG die Meldepflicht gegenüber dem EDÖB auf hohe Risiken einzuschränken und den Begriff der Unverzüglichkeit zu präzisieren.***
	VE DSG	17	2		Der Formulierungsvorschlag knüpft das Recht des EDÖB, die Benachrichtigung der Betroffenen zu verlangen, ohne dass dieses Recht mit objektiven Kriterien verbunden ist. Dies ist entsprechend anzupassen. Ebenso wenig wird präzisiert, innert welcher Fristen der Betroffene informiert und welche Informationen der Betroffene schlussendlich erhalten muss. Aufgrund der Tragweite für die betroffene Person, aber auch das entsprechende Unternehmen sind solche Voraussetzungen möglichst präzise zu formulieren, zumal dies auch weitere (zivilrechtliche und weitere) Folgen haben kann.
	VE DSG	17	4		Unklar ist auch hier, zu welchem Zeitpunkt der Auftragsverarbeiter den Verantwortlichen informieren muss, da der Begriff «unverzüglich» nicht weiter präzisiert wird. Der Verantwortliche sollte dann informiert werden, wenn ausreichend Kenntnisse über die Verletzung vorliegen, ansonsten diese Information gar

					nicht vom Verantwortlichen weiterverwendet werden kann. ***Aus den genannten Gründen stellt asut den Antrag, Art. 17 Abs. 4 VE DSG wie folgt anzupassen***: *[4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung**, sobald er davon Kenntnis hat**.* Zudem wird keine Differenzierung in Bezug auf die Schwere des Eingriffs gemacht: Jede unbefugte Datenbearbeitung soll zu einer Informationspflicht führen, was jedoch weder Sinn macht, noch den heutigen Gegebenheiten Rechnung trägt. Damit ist auch hier eine Differenzierung insbesondere nach Schwere der Verletzung, aber auch des potentiellen Risikos des Betroffenen vorzunehmen und entsprechend bereits auf Gesetzesstufe zu präzisieren. ***Aus den genannten Gründen stellt asut den Antrag, Art. 17 Abs. 4 VE DSG hinsichtlich Schwere des Eingriffs zu präzisieren und auf Datenschutzverletzungen mit erhöhtem Risiko einzuschränken.***
asut	VE DSG	18	1-2		Die neuen Vorgaben "Privacy-by-Design" sowie "Privacy-by-Default" entsprechen den Anforderungen des Übereinkommens E-SEV 108 und dürften daher auch ins Schweizerische Rechte übernommen werden müssen. Unklar bleibt, welche materiell neuen Pflichten damit konkret verbunden sein werden. Beide Grundsätze ergeben sich nämlich bereits aus anderen DSG-Bestimmungen. Die Pflicht technische Vorkehrungen zu treffen, damit der Verstoss gegen Datenschutzvorschriften möglichst minimiert wird, ergibt sich aus Art. 11 VE DSG (Sicherheit von Personendaten). Die Pflicht zu datenschutzfreundlichen Voreinstellungen, damit grundsätzlich nur diejenigen Daten bearbeitet werden, die für den jeweiligen Zweck erforderlich sind, ergibt sich bereits aus Art. 4 VE DSG (Grundsatz der Verhältnismässigkeit und Zweckbindung). Vor dem Hintergrund der sehr offenen Formulierung wird es für die Rechtsunterworfenen daher schwierig abzuschätzen, was genau neu getan werden muss damit kein Rechtsverstoss vorliegt. Entsprechend ist auch hier kritisch zu hinterfragen, ob es sich rechtfertigt, eine (sogar fahrlässige) Verletzung dieser Vorgaben unter Strafandrohung zu stellen (siehe Bemerkungen und Anträge zu Art. 51 VE DSG).
asut	VE DSG	19	1	Bst. a	Auch die neue Pflicht zur Dokumentation der Datenbearbeitung ist sehr offen formuliert und lässt der rechtsanwenden Behörde einen enormen Ermessensspielraum. Leider sind auch den Erläuterungen wenig

					Anhaltspunkte zu entnehmen, wie diese Bestimmung von den Unternehmen verstanden werden muss. Es bleibt somit unklar in welchen Fällen und in welchem Umfang Datenbearbeitungen künftig dokumentiert werden müssen. Eine konkretisierende Einschränkung wonach nur strukturierte und wiederkehrende Datenbearbeitungen von der Dokumentationspflicht erfasst werden, drängt sich nach Ansicht von asut auf. ***Aus den genannten Gründen stellt asut den Antrag, Art. 19 Abs. 1 Bst. a VE DSG wie folgt anzupassen***: a. Sie **führen ein Verzeichnis aller regelmässigen Verarbeitungsaktivitäten die ihrer Zuständigkeit unterliegen.** ~~dokumentieren ihre Datenbearbeitung;~~
asut	VE DSG	20	1		Gemäss Art. 8 Abs. 1 Bst. b des Übereinkommens E-SEV können Kostenbeiträge erhoben werden. Es muss daher möglich bleiben, für entsprechende Aufwendungen einen Kostenersatz zu erheben und es wäre stossend, wenn die Auskunft selbst bei querulatorischen oder wiederholten und extrem aufwändigen Anfragen gratis sein müsste. 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 Aufwendungen Kostenersatz verlangen. ***Aus den genannten Gründen stellt asut den Antrag, Art. 20 Abs. 1 VE DSG wie folgt anzupassen***: [1] Jede Person kann vom Verantwortlichen ~~**kostenlos**~~ Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.
asut	VE DSG	20	2	b	Bst. b ist unklar formuliert. Es sollte präzisiert werden, dass die Information nur die Kategorien der bearbeiteten Personendaten beinhalten soll. Dies wäre in Übereinstimmung mit Art. 15 Bst. b EU-DSGVO. ***Aus den genannten Gründen stellt asut den Antrag, Art. 20 Abs. 2 Bst. b VE DSG wie folgt anzupassen***: b. die **Kategorien** der bearbeiteten Personendaten;
asut	VE DSG	20	2	f	Die Herkunft soll nur dann angegeben werden müssen, falls die Daten nicht bei der betroffenen Person erhoben wurden. Dies entspricht Art. 15 Abs. 1 Bst. g EU-DSGVO.

					Aus den genannten Gründen stellt asut den Antrag, Art. 20 Abs. 2 Bst. f VE DSG wie folgt anzupassen: f. **wenn die Personendaten nicht bei der betroffenen Person erhoben werden,** die verfügbaren Informationen über die Herkunft der Personendaten;
asut	VE DSG	20	2	g	Die Begriffe „Empfängerinnen und Empfänger“ in Art. 13 Abs. 3 VE DSG der Daten schliessen auch Auftragsbearbeiter gemäss Art. 13 Abs. 4 VE DSG ein. Abgesehen davon ist es nicht praktikabel und kann operativ nicht sichergestellt werden, sämtliche Auftragsbearbeiter inkl. Identität und Kontaktdaten zu nennen (vgl. auch EU-DSGVO, wonach in Art. 15 Abs. 1 lit. b nur die Angabe von Kategorien von Empfängern verlangt wird). Zur weiteren Begründung siehe oben die Kommentierung zu Art. 13 Abs. 4 VE DSG. ***Aus den genannten Gründen stellt asut den Antrag, Art. 20 Abs. 2 Bst. g VE DSG wie folgt anzupassen***: f. gegebenenfalls die Informationen nach Art. 13 Abs. 3 ~~und 4~~.;
asut	VE DSG	20	3		Dieser Absatz geht weit über die Vorgaben der EU-DSGVO hinaus und enthält einen operativ sehr aufwändigen "Swiss Finish". Alle Entscheidungen in einer Unternehmung basieren letzten Endes immer auf Daten, die auf Systemen gespeichert sind. Entsprechend werden Unternehmen dazu gezwungen, jede Entscheidung zu begründen. Erhält bspw. eine Unternehmung von einer Person Werbung für ein bestimmtes Produkt oder eine Dienstleistung und entscheidet sich die Unternehmung dazu, dieses Produkt oder die Dienstleistung nicht zu beziehen, dann wäre sie gegenüber dieser Person für den Entscheid rechenschaftspflichtig. Auch eine Einschränkung des Absatzes auf automatisierte Einzelentscheide würde keine grosse Besserung bringen: In diesem Fall wäre eine Unternehmung jedes Mal rechenschaftspflichtig, wenn ihr Spamfilter eine E-Mail als Spam markiert. Sinn macht eine Auskunftspflicht bei automatisierten Einzelentscheidungen höchstens dann, wenn die Entscheidungen gegenüber der betroffenen Person rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen. Zudem sollte die Bestimmung eingeschränkt werden auf Fälle, in denen die betroffene Person explizit

					nach Zusatzinformationen zu einem bestimmten Entscheid fragt. Anfragen, welche lediglich der Ausforschung oder Schikane dienen oder welche zu ungenau sind ("Liefert mir alle verfügbaren Daten zu sämtlichen Einzelentscheidungen in eurer Unternehmung"), sollen damit möglichst vermieden werden. ***Aus den genannten Gründen stellt asut den Antrag, Art. 20 Abs. 3 VE DSG wie folgt anzupassen***: 3 ~~Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere~~ **Bei** automatisierten Einzelentscheidungen**, welche gegenüber der betroffenen Person rechtliche Wirkung entfalten oder die betroffene Person in ähnlicher Weise erheblich beeinträchtigen,** erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung, **wenn sie spezifisch nach den Zusatzdaten zu einem bestimmten Entscheid fragt**.
asut	VE DSG	23	2	d	Bst. d ist eine Schweizer Spezialität ("Swiss Finish") und als solche ersatzlos zu streichen. Es scheint stossend, dass das Profiling (welches im aktuellen Entwurf sogar das manuelle Profiling umfasst) per se als Persönlichkeitsverletzung gelten soll, was einen Rechtfertigungsgrund erfordert, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden ist. ***Aus den genannten Gründen stellt asut den Antrag, Art. 23 Abs. 2 Bst. d VE DSG zu streichen.***
asut	VE DSG	23	3		Wenn die betroffene Person die Personendaten allgemein zugänglich gemacht hat und eine Bearbeitung nicht ausdrücklich untersagt hat, sollte nie eine Persönlichkeitsverletzung vorliegen. Die Bestimmung „In der Regel" ist unnötig und würde zudem zu Rechtsunsicherheit führen. ***Aus den genannten Gründen stellt asut den Antrag, Art. 23 Abs. 3 VE DSG wie folgt anzupassen***: 3 ~~In der Regel~~ **Es** liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat,
asut	VE DSG	41 ff.			Es erscheint grundsätzlich gerechtfertigt, die Stellung des Beauftragten im Vergleich zum heutigen Recht zu stärken. Die neuen Untersuchungs- und Ermittlungsbefugnisse des Beauftragten dürften in der Tat ein wichtiges Element sein, damit die Europäische Kommission den Angemessenheitsbeschluss gegenüber der Schweiz erneuert. Die neuen Kompetenzen gemäss VE DSG geben dem EDÖB die Möglichkeiten bei einem möglichen Verstoss gegen die Datenschutzvorschriften direkt einzuschreiten und eine rechtskonforme Datenbearbeitung anzuordnen (Verfügungskompetenz). Wer einer solchen Anordnung

					nicht Folge leistet, kann gemäss Art. 50 Abs. 2 Buchstabe e VE DSG mit einer sehr hohen Busse bestraft werden. Nach wie vor Anwendung findet ausserdem Art. 292 StGB. Mit diesen Eingriffskompetenzen wird die nötige disziplinierende und präventive Wirkung erzielt und es dürften die wesentlichen Rahmenbedingungen für die Ratifizierung des Datenschutzkonvention E-SEV 108 geschaffen sein (Vgl. Erläuternder Bericht S. 77 f.). Einige der nachfolgend aufgeführten Verschärfungen im 7. Abschnitt des VE DSG gehen nach Ansicht von asut jedoch zu weit und lassen sich nur schwer rechtfertigen.
asut	VE DSG	41	3		Im Gegensatz zur EU-DSGVO werden hier dem Beauftragten polizeiliche Befugnisse eingeräumt. Dieser "Swiss Finish" ist abzulehnen, bringt er doch in der Praxis kaum mehr Erkenntnisse. ***Aus den genannten Gründen stellt asut den Antrag, Art. 41 VE DSG wie folgt anzupassen***: [3] 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;
asut	VE DSG	44	3		Gemäss Art. 55 VwVG hat eine Beschwerde grundsätzlich aufschiebende Wirkung. Es wird nicht begründet weshalb hier eine strengere Regelung als im allgemeinen Verwaltungsrecht gelten sollte. ***Aus den genannten Gründen stellt asut den Antrag, Art. 44 Abs. 3 VE DSG wie folgt anzupassen***: [3] Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt **~~keine~~** aufschiebende Wirkung zu.
asut	VE DSG	45			Eine Anzeigepflicht erscheint unter Berücksichtigung des gemässigten Opportunitätsprinzips nicht angebracht und ist weder in der EU-DSGVO noch in der E-SEV vorgesehen. Es handelt sich daher auch hier um einen "Swiss finish". Nach Ansicht von asut wäre es sinnvoller dem EDÖB eine Anzeigebefugnis einzuräumen. ***Aus den genannten Gründen stellt asut den Antrag, Art. 45 VE DSG wie folgt anzupassen***:

					Art. 45 Anzeiger**echt**~~pflicht~~ Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so **kann er dies den Strafverfolgungsbehörden mitteilen.**
asut	VE DSG	50-51			**Vorbemerkungen zu Strafbestimmungen** Der bereits angesprochene Umstand, dass eine Vielzahl der Tatbestände, welche gemäss Art. 50 f. VE-DSG unter Strafe gestellt werden sollen, zu unbestimmt formuliert sind, lässt die Art. 50 f. VE-DSG im Hinblick auf das strafrechtliche Bestimmtheitsgebot als bedenklich erscheinen. Generell wird es für die Rechtsunterworfenen aufgrund des erheblichen Auslegungsspielraumes schwierig sein, zu verstehen, was sie genau tun dürfen und was nicht. Dies scheint nicht zuletzt auch hinsichtlich der Höhe der Bussen, die persönlichen Charakter haben, als problematisch und unverhältnismässig. Generell sollten nur Verstösse, welche die betroffenen Personen in ihrer Privatsphäre verletzt, bestraft werden, was bei einer unterlassenen Datenschutz-Folgenabschätzung oder Dokumentation der Datenbearbeitung nicht der Fall ist. ***Aus den genannten Gründen stellt asut den Antrag, die Strafwürdigkeit der einzelnen Tatbestände von Art. 50 f. VE-DSG aus Gründen der Verhältnismässigkeit sowie aus rechtsstaatlichen Überlegungen (Verletzung des strafrechtlichen Bestimmtheitsgebots) zu überdenken.*** Im Hinblick auf die Höhe der Bussen gilt es weiter zu beachten, dass es sich beim Datenschutzgesetz im Gegensatz zum Banken- oder Spielbankengesetz nicht um eine bewilligungspflichtige Tätigkeit handelt. Es muss unterschieden werden, ob eine illegale Bank oder Spielbank betrieben wird oder ob beispielsweise vergessen wird, dem EDÖB einen Vertrag zu melden. Generell scheint ein Vergleich mit dem Markenschutzgesetz, welches bei Vorsatz eine Busse von maximal CHF 100‘000 vorsieht, sachgerechter. Von einer Bestrafung fahrlässigen Verhaltens soll generell abgesehen werden, zumal der Gesetzgeber jüngst im Rahmen der Beratungen zum neuen Geldspielgesetz ausufernde Fahrlässigkeitsdelikte mit hohen Bussen ablehnt und es regelmässig keine Rechtfertigung gibt, Übertretungshandlungen bei fahrlässiger Tatverübung unter Strafe zu stellen. Der Verzicht der Bestrafung fahrlässigen Verhaltens drängt sich im vorliegenden Kontext auch mit Blick auf das zu beachtende strafrechtliche Bestimmtheitsgebot auf. ***Aus diesen Gründen stellt asut den Antrag, die Höhe der Maximalbusse bei vorsätzlichem***

					Verhalten auf CHF 100'000 zu senken und von einer Bestrafung fahrlässigen Verhaltens vollumfänglich abzusehen. Schliesslich erscheint fraglich, dass der persönliche, strafrechtliche Charakter der Art. 50 f. VE-DSG überhaupt zielführend sein wird. Insbesondere mit Datenschutzthemen beauftragte Personen, die in ihrer Tätigkeit geschützt und gestärkt werden sollten, werden durch die Schaffung eines persönlichen Strafbarkeitsrisikos (insbesondere der Möglichkeit fahrlässiges Verhalten zu bestrafen) unter Druck gesetzt und exponiert. Dies wird dazu führen, dass Mitarbeiter in strafrechtlich bedrohten Datenschutzfragen zunehmend zurückhaltend agieren und keine Entscheidungen treffen werden, ohne sich durch einen Rechtsexperten abzusichern, was mit Sicherheit zu einer Verteuerung der Datenbearbeitung führen wird. Aus denselben Gründen werden viele Unternehmen vorsichtshalber wesentlich mehr Informationen liefern, als sie eigentlich müssten, was zu einer massiven Mehrbelastung des EDÖB führen wird.
asut	VE DSG	50	1	b	Der Verweis in Ziffer 2 auf Art. 13 Abs. 4 ist zu streichen. Diese Vorschrift geht über die Regelung des EU Rechts hinaus und ist somit als "Swiss Finish" abzulehnen (vgl. Bemerkungen zu Art. 13. Abs. 4). ***Aus den genannten Gründen stellt asut den Antrag, Art. 50 Abs. 1 lit. b2 VE DSG wie folgt anzupassen***: 2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2~~,~~ **und** 3 ~~**und 4**~~ zu liefern
asut	VE DSG	50	1	c	Die Strafbarkeit betreffend der Unterlassung die Ergebnisse der Datenschutz-Folgeabschätzung dem EDÖB mitzuteilen, ist ebenfalls zu streichen. Bei der Bestimmung betr. Datenschutz-Folgeabschätzung handelt es sich um eine neue Bestimmung, deren Anforderungen noch unklar sind (vgl. Bemerkungen zu Art. 16). ***Aus den genannten Gründen stellt asut den Antrag, Art. 50 Abs. 1 lit. c VE DSG zu streichen.***
asut	VE DSG	50	2	a	Der Verweis auf Art. 5 Abs. 6 ist streichen. Diese Vorschrift geht über die Regelung des EU Rechts hinaus und ist als "Swiss Finish" abzulehnen. Ausserdem stellt sie eine grosse administrative Bürde für alle Unternehmen dar (vgl. Bemerkungen zu Art. 5 Abs. 6). ***Aus den genannten Gründen stellt asut den Antrag, Art. 50 Abs. 2 lit. a VE DSG wie folgt***

					anzupassen: a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b **~~und Absatz 6~~** zu informieren;
asut	VE DSG	50	2	c	Eine Strafandrohung bei verweigerter Mitwirkung bzw. Kooperation ist mit dem strafprozessualen Schweigerecht unvereinbar, da die unter Strafdrohung erwirkten Auskünfte unter Umständen in einem nachfolgenden Strafsanktionsverfahren verwendet werden könnten. ***Aus den genannten Gründen stellt asut den Antrag, Art. 50 Abs. 2 lit. c VE DSG zu streichen.***
asut	VE DSG	50	4		Dieser Absatz ist wie bereits dargelegt ersatzlos zu streichen. Es ist klar, dass fahrlässige Verstösse gegen das Datenschutzgesetz nicht einfach hinzunehmen sind, die Kriminalisierung eines einzelnen Mitarbeiters oder einer einzelnen Mitarbeiterin wäre jedoch stossend. ***Aus den genannten Gründen stellt asut den Antrag, Art. 50 Abs. 4 VE DSG zu streichen.***
asut	VE DSG	51	1	d-f	Wie bereits ausgeführt, handelt es sich dabei um neue Pflichten, die zu unbestimmt formuliert sind und im Hinblick auf das strafrechtliche Bestimmtheitsgebot als bedenklich erscheinen. Sie sind somit zu streichen. ***Aus den genannten Gründen stellt asut den Antrag, Art. 51 Abs. 1 lit. d-f VE DSG zu streichen.***
asut	VE DSG	51	2		Dieser Absatz ist wie bereits dargelegt ersatzlos zu streichen. Es ist klar, dass fahrlässige Verstösse gegen das Datenschutzgesetz nicht einfach hinzunehmen sind, die Kriminalisierung eines einzelnen Mitarbeiters oder einer einzelnen Mitarbeiterin wäre jedoch stossend. ***Aus den genannten Gründen stellt asut den Antrag, Art. 51 Abs. 2 VE DSG zu streichen.***
asut	VE DSG	53			Grundsätzlich sollte die Möglichkeit bestehen, die Busse in bestimmten Fällen dem Unternehmen aufzuerlegen. Dies erscheint insbesondere dann angebracht, wenn die Privatsphäre der betroffenen Person durch den Verstoss nicht bzw. kaum tangiert worden ist. Die Höhe der Busse sollte dieser Möglichkeit nicht im Wege stehen. ***Aus den genannten Gründen stellt asut den Antrag, Art. 53 VE DSG wie folgt anzupassen***: *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 197413 über das Verwaltungsstraf recht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären~~.
Asut	VE DSG	55			Es ist nicht ersichtlich, inwiefern der Bedarf besteht, eine spezialgesetzliche Verfolgungsverjährung von fünf Jahren anstelle der im Strafgesetzbuch (Art. 109 StGB) vorgesehenen Verfolgungsverjährung von drei Jahren einzuführen. Dieser Artikel sollte daher als unnötig gestrichen werden. ***Aus den genannten Gründen stellt asut den Antrag, Art. 55 VE DSG zu streichen.***
Asut	VE DSG	59			Es ist eine klarere Übergangsregelung notwendig, um eine sinnvolle Einführung dieses Gesetzes sicherzustellen. Eine entsprechende Übergangsbestimmung räumt der Praxis genügend Anpassungszeit ein und gibt dem EDÖB die wohl notwendige Vorbereitungszeit, welche aufgrund der ausgebauten Kompetenzen und Verantwortlichkeiten notwendig scheint. Der Entwurf stellt eine unzufriedenstellende stufenweise Einführung vor. Einerseits wird eine Frist von zwei Jahren für die Einführung von Datenschutz-Folgeabschätzungen und für die Einführung der Anforderungen an *Privacy-by-Default* und *Privacy-by-Design* eingeräumt, andererseits werden weitere neue Pflichten wie die Genehmigung von Auslandtransfers oder die Anwendbarkeit der Informations- und Auskunftspflichten nicht weiter erläutert. Diese Regelung lässt Fragen offen. Derweilen ist unklar, warum die Übergangsregelung von zwei Jahren nicht generell für das ganze Gesetz gelten sollte. Entsprechend wird vorgeschlagen, die Frist von zwei Jahren auf die Anwendbarkeit des ganzen Gesetzes auszudehnen. Damit wäre auch dem europäischen Beispiel der EU-DSGVO gefolgt. ***Aus den genannten Gründen stellt asut den Antrag, Art. 59 VE DSG wie folgt zu ändern***: Die Bestimmungen dieses Gesetzes werden nach einer Frist von 24 Monaten angewendet.

asw
ausgezeichnet.

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

PDF und DOC per E-Mail an jonas.amstutz@bj.admin.ch

Wallisellen, 3. April 2017

Stellungnahme der ASW zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Die ASW
Die ASW Allianz Schweizer Werbeagenturen ist die Standesorganisation der inhabergeführten, mittelständischen Kommunikationsagenturen in der Schweiz. Sie hat über 50 Aktivmitglieder. Diese beschäftigen mehr als 300 festangestellte Mitarbeitende und zeichnen zusammen für ein jährliches Kommunikationsvolumen von rund CHF 600 Mio. verantwortlich.

Einleitendes
Die Aktivmitglieder der ASW betreuen fast ausnahmslos Kommunikations-Etats von Schweizer KMU. Wir wissen deshalb um die finanziellen, organisatorischen, personellen und administrativen Möglichkeiten dieser Unternehmen, die sich der Digitalisierung der Gesellschaft und damit auch der Handhabung von schützenswerten Personendaten nicht entziehen können.

Geschäftsstelle ASW
Breitestrasse 1
Postfach 466
CH 8304 Wallisellen

T +41 44 831 15 50
F +41 44 831 1424

info@asw.ch
www.asw.ch

Stellungnahme
Die ASW begrüsst grundsätzlich die Revision des DSG, erachtet es jedoch als völlig ausreichend, wenn die internationalen Vorgaben (SEV 108) eingehalten werden. Alle weiter gehenden Verschärfungen (Swiss Finish) erachten wir als kontraproduktiv, zumal sie die Handhabbarkeit von elektronisch erfassten und elektronisch zu übermittelnden Personendaten durch Schweizer KMU nahezu verunmöglichen und im Endeffekt einen Standortnachteil nach sich ziehen würden.

Schweizer KMU wären mit dem zurzeit vorliegenden "Swiss Finish" völlig überfordert, müssten eine Abkoppelung vom zunehmend digitalisierten internationalen Geschäft hinnehmen und wären nicht mehr in der Lage, mit ausländischen Marktpartnern einen ökonomisch vertretbaren Informationsaustausch aufrecht zu erhalten.

Zusammenfassung
Die ASW Allianz Schweizer Werbeagenturen **befürwortet grundsätzlich** eine Revision des Datenschutzgesetzes, erachtet es jedoch als **völlig ausreichend und sachdienlich**, wenn die **internationalen Vorgaben** übernommen werden. Eine darüber hinaus gehende Verschärfung ist unseres Erachtens wirtschaftsschädigend und deshalb strikte abzulehnen.

Im Übrigen verweisen wir auf die Eingabe des Schweizer Dialogmarketing Verband SDV, die im Detail auf einzelne Punkte eingeht, die wir an dieser Stelle nicht erneut aufführen müssen.

Für die Berücksichtigung der Anliegen der mittelständischen, inhabergeführten Kommunikations-Agenturen in der Schweiz sowie deren Auftraggeber, fast ausnahmslos Schweizer KMU, danken wir im Voraus.

Freundliche Grüsse
ASW Allianz Schweizer Werbeagenturen
Geschäftsstelle

Benno Frick, Geschäftsführung
www.asw.ch/kontakt

Amstutz Jonas BJ

Von: Christoph Wolnik <c.wolnik@auto-schweiz.ch>
Gesendet: Dienstag, 4. April 2017 16:36
An: Amstutz Jonas BJ
Cc: f.launaz@auto-schweiz.ch; Andreas Burgener
Betreff: Vernehmlassungsantwort Datenschutzgesetz
Anlagen: 2017-04-04 Vernehmlassungsantwort DSG auto-schweiz.docx; 2017-04-04 Vernehmlassungsantwort DSG auto-schweiz.pdf

Sehr geehrter Herr Amstutz

Im Anhang lasse ich Ihnen gerne die Vernehmlassungsantwort von auto-schweiz zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) als Word- sowie als PDF-Datei zukommen.

Ich wünsche Ihnen einen angenehmen Abend.

Freundliche Grüsse

Christoph Wolnik, M.A.
Public Relations

auto-schweiz
Vereinigung Schweizer Automobil-Importeure
Wölflistrasse 5 | Postfach 47 | 3000 Bern 22
Telefon +41 31 306 65 65
c.wolnik@auto-schweiz.ch
www.auto.swiss

auto schweiz suisse

www.facebook.com/autoschweiz
www.twitter.com/autosuisse

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 : auto-schweiz

Abkürzung der Firma / Organisation :

Adresse : Wöflistrasse 5, Postfach 47, 3000 Bern 22

Kontaktperson : Andreas Burgener, Direktor

Telefon : 031 306 65 65

E-Mail : a.burgener@auto-schweiz.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!

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 2

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 3

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
auto-schweiz	Die Vereinigung Schweizer Automobil-Importeure auto-schweiz nimmt zu den Regelungen des VE-DSG Stellung, welche die Privatwirtschaft, und dort insbesondere die offiziellen Marken-Importeure von Fahrzeugen betreffen. Auf eine Stellungnahme zu den übrigen Regeln des VE-DSG und die weiteren Anpassungen in Zusammenhang mit Schengen, wird hingegen verzichtet. Auto-schweiz ist mit der Verschärfung des Datenschutzes in der vorgeschlagenen Form nicht einverstanden. Ob eine Äquivalenz mit Regeln der EU erreicht werden wird, hängt von sehr vielen (auch nicht ausschliesslich im Datenschutzrecht anzusiedelnden) Fragestellungen ab, auf welche die vorliegende Gesetzgebung kaum oder gar keinen Einfluss hat. Äquivalenz darf nicht mit „Gleichförmigkeit“ gleichgesetzt und nicht um jeden Preis zu erlangen versucht werden. Auf gar keinen Fall dürfen neue Bestimmungen über das hinausgehen, was die EU-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
auto-schweiz	DSG	2	1		Der Verzicht auf den Schutz von Daten juristischer Personen ist aus Sicht von auto-schweiz 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.
auto-schweiz	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.
auto-schweiz	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;» Im Weiteren ist die Formulierung „Daten oder Personendaten“ irreführend und unnötig. Der Hinweis auf „Daten“ sollte gestrichen werden. Zudem ist neu das Profiling ohne ausdrückliche Einwilligung der betroffenen Person per se eine Persönlichkeitsverletzung, nicht wie bisher nur die Weitergabe der entsprechenden Daten. Eine solche Regelung kennt auch die DSGVO nicht. Es sollte an der bisherigen Rechtslage festgehalten werden.

					Zu den besonders schützenswerten Daten gehören neu auch genetische und biometrische Daten, wobei letztere insofern eingeschränkt sind, als es sich um Daten handelt, die eine natürliche Person eindeutig identifizieren (Art. 3 Bst. c Ziff. 4 VE DSG). Es sollten jedoch nicht jene biometrischen Daten erfasst sein, die eine natürliche Person eindeutig identifizieren, sondern nur solche, die zum Zweck bearbeitet werden, dies zu tun. Die Konvention 108 geht auch nicht weiter. Dies sollte präzisiert werden.
auto-schweiz	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 auto-schweiz 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.
auto-schweiz	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.
auto-schweiz	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: […]»
auto-schweiz	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 auto-schweiz 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. Zudem ist die Frist zur Genehmigung von Datenexportverträgen mit einem halben Jahr viel zu lang angesetzt.
auto-schweiz	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.
auto-schweiz	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.

auto-schweiz	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.
auto-schweiz	DSG	8			**Empfehlungen der guten Praxis:** Auto-schweiz 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.
auto-schweiz	DSG	13	2		**Informationspflichten:** **Ganz grundsätzlich sollten die Regeln zur Informationspflicht überarbeitet werden. Eine risikobasierte Transparenzpflicht würde völlig genügen und auch einer „Informationsflut“ vorbeugen.** Im VE-DSG fehlt leider eine Bestimmung, wonach es genügen würde, dass eine Gesellschaft statt einer Detailinformation bei jeder Datenbeschaffung mit einer Information auf seiner Webseite arbeiten kann, obwohl dies der heutigen Praxis des EDÖB entspricht und die Voraussetzungen der Konvention 108 erfüllt. 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.
auto-schweiz	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.
auto-schweiz	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.
auto-schweiz	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.
auto-schweiz	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.

	DSG	14	4		Der Ausnahmekatalog von Art. 14 Abs. 4 VE-DSG geht weiter als von der Konvention 108 gefordert. Entscheidend kann nicht sein, ob eine Berufung auf überwiegende private Interessen nur dann möglich ist, wenn die Personendaten nicht an Dritte weitergegeben werden, sondern ob das Interesse des Datenbearbeiters dem Interesse an der Information der betroffenen Person überwiegt. Dies betrifft insbesondere Konzerne, welche Daten auch innerhalb des Konzerns nicht weitergeben dürften. Es darf jedoch keine Rolle spielen, ob gewisse Tätigkeiten von einem eigenen Arbeitnehmer oder von einer spezialisierten Gruppengesellschaft ausgeführt werden.
auto-schweiz	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.
auto-schweiz	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“
auto-schweiz	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 vollautomatisierten 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.)
auto-schweiz	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.
auto-schweiz	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.“
auto-schweiz	DSG	16	2		Der Begriff „Persönlichkeit oder Grundrechte“ entspricht nicht der Schweizer Gesetzessystematik und sollte durch den Begriff „Persönlichkeitsverletzung“ ersetzt werden (vgl. insb. Art. 23 ff. VE-DSG). In der Schweiz haben Grundrechte keine Drittwirkung.
auto-schweiz	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.
auto-schweiz	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.
auto-schweiz	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.
auto-schweiz	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. Auto-schweiz 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 ein 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 auto-schweiz 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.
auto-schweiz	DSG	20/21			**Auskunftsrecht:** Die Information darüber, wie bestimmte Entscheide zustande kommen, gehört zum Geschäftsgeheimnis einer Unternehmung und ist demnach, insbesondere in der aktuell vorgesehen, detaillierten Form gemäss Art. 20 Abs. 3 VE-DSG, klar unverhältnismässig. 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. Ausserdem muss eine Auskunft immer kostenlos sein. Es fehlt gar eine Bestimmung, welche dazu ermächtigen würde, auf dem Verordnungsweg Ausnahmen vorzusehen. Solche Ausnahmen sind in der

					DSGVO vorgesehen. In der Schweiz müssen demgegenüber auch querulatorische, widerholte oder extrem aufwändige Anfragen stets kostenlos beantwortet werden.
auto-schweiz	DSG	20	3		Die Regel von Art. 20 Abs. 3 VE-DSG muss gestrichen werden. Dies ist konsequent, da sich auto-schweiz 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.
auto-schweiz	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.
	DSG	24	2		In Art. 24 Abs. 2 VE DSG heisst es neu, dass in den aufgeführten Fällen das überwiegende private Interesse nur noch „möglicherweise“ gegeben ist. Dies führt zu Rechtsunsicherheit.
auto-schweiz	DSG	50 ff.			**Sanktionen** Betreffend Sanktionen war erwartet worden, dass – entsprechend der Konvention 108 – Administrativsanktionen eingeführt werden, wie dies auch in der DSGVO hauptsächlich umgesetzt ist. Nun sollen jedoch private, strafrechtliche Sanktionen gegen die einzelnen involvierten Organe und Mitarbeiter ausgesprochen werden. Auch ein fahrlässiger Verstoss wird massiv geahndet. Und zudem wird nicht derjenige gebüsst, der Personendaten bewusst zweckwidrig oder unverhältnismässig verwendet, sondern derjenige, der vergisst, diese Datenschutzverletzung dem EDÖB zu melden.

					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. In diesem Zusammenhang ist auch fragwürdig, ob der Auftragsbearbeiter seinen (unter Strafandrohung stehenden) Pflichten (etwa zur Durchführung einer Datenschutz-Folgenabschätzung gemäss Art. 16, Privacy by Design, Privacy by Default gemäss Art. 18, Information von Datenempfängern über etwaige Berichtigungen und Löschungen gemäss Art. 19) aufgrund seiner Kenntnisse überhaupt nachkommen kann. 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. Auto-schweiz verweist auf die diesbezügliche Stellungnahme von economiesuisse („Vorschlag der Wirtschaft“), welche vollumfänglich unterstützt wird.. Speziell ist darauf hinzuweisen, dass der EDÖB die Kompetenz erhalten soll, gegen Datenbearbeiter verwaltungsverfahrensrechtliche Untersuchungen durchzuführen und gegen diese Verfügungen zu erlassen, sowohl in Form von vorsorglichen Massnahmen wie auch um eine Datenbearbeitung anzupassen, sie zu stoppen, einschliesslich der Bekanntgabe ins Ausland, oder um Daten zu vernichten. Diese weitgehenden Kompetenzen sind rechtsstaatlich fragwürdig und nicht akzeptabel. Problematisch ist in diesem Zusammenhang auch die fehlende aufschiebende Wirkung von Beschwerden gegen vorsorgliche Massnahmen. Zudem soll der EDÖB auch das Recht haben, ohne Vorankündigung Hausdurchsuchungen durchzuführen und sich Zugang zu allen notwendigen Daten und Informationen zu verschaffen.
auto-schweiz	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

auto-schweiz

François Launaz
Präsident

Andreas Burgener
Direktor

Amstutz Jonas BJ

Von: Schmid Rafaela <schmid@reflecta.ch>
Gesendet: Dienstag, 4. April 2017 15:46
An: Amstutz Jonas BJ
Cc: Chevallaz Roger
Betreff: Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes - Stellungnahme von AudioVision Schweiz
Anlagen: AVCH_170404_Schreiben DSG-Revision.pdf; Totalrevision-des-Datenschutzgesetzes_Stellungnahme_AVCH.DOCX

Sehr geehrter Herr Amstutz

Sie finden anbei die Stellungnahme von AudioVision Schweiz zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz.

Wir danken Ihnen für die Berücksichtigung unser Anliegen.

Bei Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

Rafaela Schmid

reflecta ag
Zieglerstrasse 29
Postfach 530
CH - 3000 Bern 14
+41 (0)31 387 37 97 | Zentrale
+41 (0)31 387 37 42 | Direkt
+41 (0)79 543 62 93 | Mobile
+41 (0)31 387 37 99 | Fax

www.reflecta.ch
schmid@reflecta.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 : Audiovision Schweiz

Abkürzung der Firma / Organisation : AVCH

Adresse : Postfach 530, Zieglerstrasse 29, 3000 Bern 14

Kontaktperson : Roger Chevallaz, Geschäftsführer

Telefon : 031 387 37 17

E-Mail : info@audiovisionschweiz.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 ____ 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ 5

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.
AVCH	VEDSG	3			

					Soweit die Datenbearbeitung durch private Verfahrensparteien unter den Anwendungsbereich geltender 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,
AVCH	VEDSG	14	2-3		

					nicht Rechtsdurchsetzungs-Interessen, im Vordergrund stehen; Bericht S. 58). Auch **eigene überwiegende Interessen** würden unter erhöhter Rechtsfertigungslast stehen (Bericht S. 58); und wären 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.**
AVCH	VEDSG	21			
AVCH	VEDSG	14			

					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 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.).
AVCH	VEDSG	24	2		

					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 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	179^{novies}			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.*

Amstutz Jonas BJ

Von: Witzig Tobie <Tobie.Witzig@az-direct.ch>
Gesendet: Freitag, 31. März 2017 08:27
An: Amstutz Jonas BJ
Betreff: Stellungnahme der AZ Direct AG zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Wichtigkeit: Hoch

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrter Herr Amstutz

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 als direkt betroffenes Schweizer Unternehmen gerne wahr.

Wir verstehen, dass die Anpassungen im Zusammenhang mit der Revision des Übereinkommens SEV 108 zum Schutz des Menschen (E-SEV 108) und der Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen mit dem VE DSG in Angriff genommen werden müssen. Jedoch hätte eine über die EU-Richtlinie 2016/679 («DSGVO») hinausgehende Regelung, wie sie unserer Meinung nach im aktuellen Entwurf vorgesehen ist, für die Schweizer Wirtschaft insgesamt und insbesondere für die Werbe- und Dialogmarketing-Branche (zu der auch wir gehören) fatale Folgen.

Wir plädieren dafür, im neuen Datenschutzgesetz für Unternehmen ein Maximum an Flexibilität und ein Minimum an Belastung zu wahren. Das System der Selbstregulierung, welches sich in der Schweiz etabliert hat, sollte so weit als möglich Bestand halten. Die diversen im Vergleich zum EU-Raum überschiessenden Regelungen im Sinne eines «Swiss Finish» sollten zwingend angepasst werden. Diese würden zu einer klaren Benachteiligung von Schweizer Unternehmen gegenüber ausländischen, grenzüberschreitend tätigen Unternehmen führen. Die Folge wäre eine Behinderung von Innovation am Standort Schweiz, insbesondere bei der Entwicklung von datengetriebenen Geschäftsmodellen, welche schlussendlich auch im Interesse der Konsumenten sind.

Wir hoffen auf eine wohlwollende Prüfung und Berücksichtigung unserer Anliegen.

Freundliche Grüsse
Tobie Witzig

Tobie Witzig
Chief Executive Officer

Der neue Marketingbudget-Booster:
AZ Business Web Leads identifiziert für Sie Firmen, die Ihre Homepage besuchen, und liefert Ihnen die dazugehörigen Kontaktdaten. Interessiert? Rufen Sie an: +41 41 248 44 55.

AZ Direct AG
Blegistrasse 1
CH-6343 Rotkreuz
Schweiz

Tel: +41 41 248 44 44
Direct: +41 41 248 44 50
Mobile: +41 79 470 96 56
Fax: +41 41 248 44 88

Tobie.Witzig@az-direct.ch
www.az-direct.ch

part of arvato: a Bertelsmann company

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 : AZ Direct AG

Abkürzung der Firma / Organisation : AZ

Adresse : Blegistrasse 1, 6343 Rotkreuz

Kontaktperson : Tobie Witzig (CEO)

Telefon : 041 248 44 50

E-Mail : tobie.witzig@az-direct.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!

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 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 6

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 17

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten 17

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") 18

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" 19

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
AZ	Wir begrüssen die Bemühungen, dass die Anpassungen im Zusammenhang mit der Revision des Übereinkommens SEV 108 zum Schutz des Menschen (E-SEV 108) und der Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen mit dem VE DSG in Angriff genommen werden. Wir verstehen, dass diesbezüglich der Handlungsspielraum bei der Gesetzesrevision beschränkt ist. Jedoch ist eine weitgehende Anpassung an die EU-Richtlinie 2016/679 («DSGVO») oder sogar eine darüberhinausgehende Regelung im Sinne eines «Swiss Finish» für die Schweizer Wirtschaft insgesamt und insbesondere für die Werbe- und Dialogmarketing-Branche inklusive der in diesen Bereichen mit der Zurverfügungstellung der benötigten Daten für die Werbung beschäftigten Unternehmen nicht erforderlich bzw. nicht wünschenswert. Ein solcher «Swiss Finish» würde zu einer klaren Benachteiligung Schweizer Unternehmen gegenüber ausländischen, grenzüberschreitend tätigen Unternehmen führen. Zumindest ist faktisch davon auszugehen, dass in diesem Fall für ausländische Unternehmen das Risiko von Strafsanktionen bei Verletzung des DSG ebenfalls deutlich geringer ausfallen würde.
AZ	Insgesamt ist uns aufgefallen, dass sowohl im VE DSG als auch in den Erläuterungen dazu an keiner Stelle auf das Bestehen eines **berechtigten Interessens** der Werbe- und Dialogmarketing-Branche und generell der Wirtschaft hingewiesen wird, **dass Personendaten für Direktwerbung** und insbesondere für die Akquisition von Neukunden oder auch zur Ausweitung von bestehenden Geschäftsbeziehungen **verwendet werden können**. Dies entspricht in einem Land wie der Schweiz, welches sich grundsätzlich zur Markwirtschaft bekennt, einem zentralen und legitimen Bedürfnis. Im Gegensatz zur EU-Richtlinie 2016/679 («DSGVO»), wo dieses Interesse explizit anerkannt wurde (vgl. insbesondere RZ 47, S. 9 DSGVO: «Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden» sowie RZ 70, S.13 DSGVO, wo explizit darauf verwiesen wird, dass eine Widerspruchsmöglichkeit bei Direktwerbung gegeben sein muss), fehlt ein solcher Hinweis in der Schweiz vollständig. Das Gefühl entsteht dabei, dass vorliegend einseitig Interessen von betroffenen Personen und des Beauftragten gewürdigt wurden. Es wurden auch erhebliche, teils deutlich über die Minimalvoraussetzungen in der zu revidierende Konvention des Europarats (E-SEV 108) hinausgehende Bestimmungen aufgenommen. Der dadurch entstehende «**Swiss Finish**» droht zu erheblichen Mehraufwänden - oft auch ohne erkennbaren Mehrwert - zu führen. Dies geht u.E. in zahlreichen Bereichen zu weit und führt in der Praxis zu kaum umsetzbaren Ergebnissen. Bei einer Anwendung vieler der jetzt vorgeschlagenen Bestimmungen im VE DSG entsteht der Eindruck, dass das bisher in der Wirtschaft essentielle und rechtlich unter Einhaltung der bestehenden Rahmenbedingungen nicht zu beanstandende Dialogmarketing und insbesondere auch die Möglichkeit der Miete und des Verkaufs von Adressdaten zu diesem Zweck faktisch verunmöglicht oder zumindest erheblich behindert werden soll. Die damit verbundenen berechtigten Interessen der Wirtschaft sollten deshalb anerkannt und besser mitberücksichtigt werden.

AZ	Generell erachten wir die Einführung der weitreichenden und mit massiven Sanktionen, versehenen **neuen Strafbestimmungen** in Art. 50ff VE DSG, welche zu einer potentiellen Kriminalisierung von Mitarbeitern von Unternehmen auf allen Stufen führen kann, als **sehr problematisch**. Zudem führen die sehr weitgehende Meldepflicht gegenüber dem EDÖB und ebenfalls dessen Anzeigepflicht dazu, dass selbst bei kleineren Fällen und selbst bei leicht fahrlässigem Handeln rasch einmal die Eröffnung von Strafverfahren drohen kann. Dabei sind die einzelnen handelnden Mitarbeiter gemäss VE DSG sehr rasch mit schwierigen Auslegungsfragen konfrontiert. Eine Verurteilung und bereits die Involvierung in entsprechenden Strafverfahren kann für diese sogar zu Arbeitsverlust und zu sozialem Abstieg, allenfalls sogar zu einer Bedrohung der finanziellen Existenz führen. Wird zudem beachtet, dass einige der vorgeschlagenen Straftatbestände zu wenig bestimmt und zu weit gefasst sind (vgl. unten), wird offensichtlich, dass diese Bestimmungen über das Ziel hinausschiessen und dass grundsätzlich nicht die Mitarbeiter des jeweils handelnden Unternehmens, sondern das Unternehmen selbst mit angemessenen Administrativ-Sanktionen (z.B. auf der Basis der E-SEV 108) zur Rechenschaft gezogen werden sollten. Diese sind besser geeignet, durch das Ergreifen und Koordinieren von Massnahmen die datenschutzrechtlichen Anforderungen für das eigene Unternehmen zu definieren und entsprechende Massnahmen festzulegen. Es ist ja auch primär das Unternehmen selbst, welches von der eigenen Wirtschaftstätigkeit und unter Umständen auch von einer Missachtung gesetzlicher Bestimmungen profitiert. Werden die Mitarbeiter bestraft, könnte es für viele Unternehmen einfacher sein, sich von diesen zu trennen als sich effektiv mit den notwendigen Anpassungen der internen Prozesse befassen zu müssen. Der Sündenbock ist damit rasch identifiziert und bestraft. Es erscheint jedoch fairer, hier die Unternehmen verantwortlich zu machen. Zudem ist die drohende Diskrepanz zwischen der schnell möglichen Strafverfolgung von Unternehmen bzw. deren Mitarbeitern in der Schweiz zur deutlich erschwerten, wenn teilweise nicht sogar verunmöglichten Strafverfolgung von ausländischen Unternehmen und deren Mitarbeitern im Ausland zu verhindern. Schliesslich erachten wir auch die deutlich ausgeweiteten Mitwirkungs- und Meldepflichten im VE DSG im Hinblick auf das strafrechtliche Selbstbelastungsverbot als problematisch.
AZ	Einzelne **Befugnisse und Pflichten des Datenschutzbeauftragten** sind u.E. zu überdenken und zu begrenzen. Dazu gehören insbesondere der Wegfall der aufschiebenden Wirkung von Rechtsmittel gegen Massnahmen des EDÖB (vgl. unten).
AZ	Im Dialogmarketing ist zu berücksichtigen, dass durch die Möglichkeit der **Selektion** (Scoring; insb. Bildung von Gruppenprofilklassen) von verschiedenen, nur teilweise persönlichen Merkmalen in vielen Fällen eine Effizienzsteigerung der darauf vorgenommenen Werbung ermöglicht wird. Dies hat positive Auswirkungen auf die Ressourcenverwendung. Das Publikum kann gezielter angesprochen werden. Dabei entstehen in der Regel durch die temporäre Selektion keine neuen Personendaten. Es entsteht damit auch kein Persönlichkeitsprofil der betroffenen Personen. Es werden lediglich die Erfolgschancen der jeweils beabsichtigten Werbekampagnen erhöht. Dies stellt insbesondere bei den wenig aggressiven Werbeformen (z.B. via Postzustellung) kaum eine erhebliche Gefährdung der Interessen der betroffenen Personen dar und es ergeben sich daraus auch keine rechtlichen Folgen für betroffene Personen. Diesen wird lediglich - allenfalls besser auf ihre Bedürfnisse abgestimmte - Werbung angezeigt, welche sie einfach (z.B. durch Vernichtung des Werbeschreibens) ignorieren können. Auf der anderen Seite wird jedoch das nach wie vor legitime Werbeinteresse der Wirtschaft gebührend berücksichtigt. Zu denken ist hier zudem an die Interessen von Nonprofit-Organisationen und

	von politischen Parteien. Die vorgesehenen weitgehenden Regelungen zum «**Profiling**» gehen in diesem Bereich zu weit. **Es sollte dazu am bisherigen schweizerischen Konstrukt mit dem Persönlichkeitsprofil festgehalten werden** oder dieses leicht angepasst werden. Ist dies nicht möglich, sollte eine Einschränkung des Profiling **höchstens analog der Regelung in der DSGVO** erfolgen. Insbesondere ist in letzterem Fall auf die zwingende Voraussetzung der undifferenzierten und aufgrund der weiten Definition des Begriffs «Profiling» weitreichenden «ausdrücklichen Einwilligung» durch betroffene Personen zu verzichten und an deren Stelle eine Interessenabwägung zu ermöglichen. Werbung ist in einer Markwirtschaft ein zentraler Motor für deren Funktionieren, was eine differenziertere Regelung des Profilings dringend notwendig macht.
AZ	Unnötige Verdoppelungen von **Pflichten für den Auftragsdatenbearbeiter** führen zu Unklarheiten der Aufteilung der Verantwortung gegenüber dem Verantwortlichen und zu unnötigem administrativem Aufwand. Die vorgesehen selbständigen Verpflichtungen der Auftragsdatenbearbeiter sollten gestrichen bzw. auf das absolute Minimum reduziert werden.
AZ	Es wird begrüsst, dass sich an der bisherigen Praxis und dem Recht in Bezug auf das «**Recht auf Versessen**» nichts ändert und keine neue Regelung aufgenommen wird. Die bisherigen Regeln und die Grundsätze der Datenbearbeitung reichen aus, um diesbezügliche Fragen praxisgerecht zu handhaben.
AZ	Es wird begrüsst, dass die in der DSGVO vorgesehene **Pflicht zur Daten-Portabilität** nicht übernommen wurde, da eine solche Pflicht höchstens in sehr beschränkten Fällen aus dem Bereich Social Media sinnvoll sein könnte und eine breite, allgemeine Anwendung zu zusätzlichem, unnützem Aufwand und schwierigen, unbeabsichtigten Abgrenzungsfragen führen würde.
AZ	An verschiedenen Stellen wie beispielsweise in Art. 16 VE DSG werden auch im Zusammenhang mit Privaten die Verpflichtung zur Wahrung von «Grundrechten» erwähnt. Die Grundrechte sind sicherlich von den Behörden im Umgang mit den Bürgern zu berücksichtigen. Gegenüber den Privaten ist deren Erwähnung jedoch verwirrend und sollte überall gestrichen werden. Die Grundrechte verpflichten grundsätzlich nicht die Privaten, sondern den Staat. **Eine Drittwirkung von Grundrechten besteht in der Schweiz nicht und sollte auch nicht punktuell eingeführt werden.**
AZ	Uns erschient es zudem sinnvoll, Unternehmen die **freiwillige Möglichkeit** einzuräumen, **einen betrieblichen Datenschutzbeauftragten (bDSB) einzuführen**. Unsinnig wäre aber, eine allgemeine Pflicht zur Einsetzung eines solchen bDSB einzuführen. Damit wird den ganz unterschiedlichen datenschutzrechtlichen Exponierungen und Bedürfnissen der schweizerischen Unternehmen Sorge getragen. Gleichzeitig wir damit die Professionalisierung von exponierteren Unternehmen im Bereich des Datenschutzes erhöht. Mit der Bestellung eines bDSB sollten gewisse Erleichterungen, wie Freistellungen von Meldepflichten, verbunden werden (z.B. zu Art. 15, 16 und 17 VE DSG). Dies würde ausserdem ebenfalls den Beauftragten entsprechend entlasten.

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
AZ	VE DSG	2	1		Der Wegfall des Anwendungsbereichs auf **juristische Personen** ist insbesondere zur Angleichung an die ganz überwiegende europäische Rechtslage zu begrüssen.
AZ	VE DSG	3	1	f.	Der Begriff «**Profiling**» wird im Vorentwurf viel zu weit definiert. Der E-SEV 108 verlangt keine umfassende Regelung zum Profiling, sondern höchstens zu automatisierten Entscheidungen, welche betroffene Personen erheblich beeinflussen (vgl. Art. 8 Ziff. 1. Bst. a. E-SEV 108). Die bisherige Verwendung des Begriffs «Persönlichkeitsprofil» im DSG war diesbezüglich zudem präziser und sollte, wenn möglich, beibehalten werden. Die jetzige Definition, welche sogar deutlich über die Anforderungen in der DSGVO hinausgeht, führt dazu, dass in Zukunft eine unbeabsichtigt grosse Anzahl an Handlungen und Datenbearbeitungen, welche oftmals gar nicht zu neuen Personendaten führen, riskieren, als Profiling qualifiziert zu werden. Aufgrund von Art. 23 Abs. 2 VE DSG ist derzeit vorgesehen, dass ein Profiling ohne ausdrückliche Einwilligung per se eine Persönlichkeitsverletzung darstelle und es bestehen einschneidende Sanktionen dafür. Dies gefährdet neben der sinnvollen Selektion von statistischen, anonymen Daten zusammen mit Personendaten zur Bildung von Gruppenprofilklassen und damit zur Verbesserung der Wirksamkeit persönlicher Werbung auch potentiell viele neue, vielversprechende Entwicklungen im Bereich «BIG DATA», welche der Verbesserung von Produkten und Dienstleistungen dienen können. Durch die Hintertür wird hier somit versucht, dieses Thema im Sinne einer sehr weitgehenden Beschränkung zu regeln, ohne dass eine differenziertere Auseinandersetzung erfolgen kann. Sogar ein «Profiling» von Hand wird sodann im VE DSG im Gegensatz zu der Regelung in der EU erfasst. Dies würde damit sogar bedeuten, dass ein Arzt, welcher anhand erfasster Patientendaten versucht eine Krankheit oder den Krankheitsverlauf seines Patienten vorauszusagen, dafür eine ausdrückliche Einwilligung des Patienten bedarf. Auch die zusätzliche Erwähnung von «Daten» zusätzlich zu «Personendaten» ist äusserst heikel und führt zu schwierigen Abgrenzungen. Es ist nur dann von einer datenschutzrechtlich relevanten Handlung auszugehen, wenn das Resultat eines Profilings zu (neuen) Personendaten führt.

					Zum Ganzen sind auch die zutreffenden Argumente von David Rosenthal in «Der Vorentwurf für das ein neues Datenschutzgesetz: Was er bedeutet» in Jusletter 20. Februar 2017, Rz7f. und Rz17, zu beachten. **Vom Wechsel auf das Konzept des «Profiling» sollte zugunsten des bisherigen Konzeptes (insb. Beibehaltung des «Persönlichkeitsprofils») abgesehen werden. Ist dies nicht möglich, ist der Umfang so weit wie möglich zu begrenzen, indem insbesondere nur automatisiertes Profiling erfasst wird und indem von der verwirrenden und unpräzisen Erwähnung von «Daten» neben «Personendaten» abgesehen werden sollte. In jedem Fall darf aber eine Definition nicht über die Regelung im DSGVO hinausgehen.** Ein «Swiss Finish» wäre hier äusserst heikel und würde Schweizer Firmen gegenüber ausländischen Firmen, insbesondere auch wegen der vorgesehenen Strafsanktionen und eingeschränkten Verfolgbarkeit solcher Delikte im Ausland, deutlich benachteiligen. Steigen zudem die Anforderungen in diesem Zusammenhang an die von betroffenen Personen einzuholenden Einwilligungen, werden in der Regel ausländische Grosskonzerne (Bsp. Facebook) profitieren, da sie sehr einfach und kostengünstig über Anpassung der Nutzungsbedingungen und Einholung entsprechender Zustimmungen steigende Voraussetzungen rasch umsetzen können. In diesem Bereich sind somit zahlreiche Schweizer Unternehmen und vor allem KMUs schwerwiegend benachteiligt. Schliesslich wird hier quasi durch die Hintertür versucht, das Thema «BIG DATA» vorsorglich und übermässig restriktiv zu regeln, was rasch zu einer Kriminalisierung innovativer Mitarbeiter führt, welche die weitreichenden Folgen der vorgeschlagenen Regelung zum Profiling nicht kennen bzw. diese fahrlässig nicht beachten.
AZ	VE DSG	3	1	h	Es ist nicht ersichtlich, wieso der Verantwortliche neben dem Entscheid über Zweck und Mittel ausdrücklich auch über den genaueren Umfang der Bearbeitung entscheiden muss. Diese Formulierung ist selbst in der DSGVO nicht so vorgesehen, weshalb die Ergänzung zum **Umfang der Bearbeitung** unseres Erachtens **gestrichen** werden sollte.
AZ	VE DSG	4.	3		Es ist nicht ersichtlich, wieso hier das Wort «klar» den erkennbaren Zweck noch weiter einschränken soll. Damit wird nur die Problematik der weit definierten Strafbarkeit in der VE DSG noch weiter zuungunsten der Arbeitnehmer verschärft. Die handelnden Mitarbeiter, werden damit noch rascher persönlich strafbar. Diese Kriminalisierung von Arbeitnehmern geht unseres Erachtens zu weit, weshalb **das Wort «klar» gestrichen werden sollte**.
AZ	VE DSG	4	5		Es ist u.E. nicht notwendig, den Wortlaut dieser Bestimmung gegenüber der ursprünglichen Regelung

					anzupassen, insbesondere auch da gemäss den Erläuterungen keine materielle Änderung beabsichtigt ist. Eine **permanente Nachführungspflicht** im ersten Satz der Bestimmung erscheint uns ausserdem uferlos und sie **sollte gestrichen werden**.
AZ	VE DSG	4	6		Die Erwähnung der Voraussetzung einer **ausdrücklichen Einwilligung** generell, zumindest jedoch **für das Profiling** geht hier u.E. zu weit. Dazu verweisen wir vorab auf unsere weiteren Ausführungen zum Profiling in dieser Stellungnahme und insbesondere zu Art. 3 Abs. 1 lit. f. VE DSG oben. Wir erachten diese Voraussetzung zumindest im Hinblick auf das Profiling als unnötig und nicht genügend präzise (vgl. dazu ebenfalls FN 27, in «Der Vorentwurf für das ein neues Datenschutzgesetz: Was er bedeutet» von David Rosenthal in Jusletter 20. Februar 2017). Zumindest d**ie Voraussetzung einer ausdrücklichen Einwilligung zum Profiling sollte deshalb gestrichen werden.** Es sollte in den Erläuterungen zudem auch klargestellt werden, dass sich an der bisherigen Praxis in der Schweiz zur Erteilung und zum Verständnis einer Einwilligung nichts ändert.
AZ	VE DSG	5, 6			Diese Regelungen gehen ebenfalls im Sinne eines «**Swiss Finishs**» über das Notwendige hinaus. Es besteht u.E. kein Grund die bestehende Regelung zur Bekanntgabe von Daten ins Ausland anzupassen, da diese bereits mit E-SEV 108 kompatibel ist.
AZ	VE DSG	7			Allgemein erachten wir es auch bei dieser Klausel nicht als sinnvoll, von der bestehenden Regelung abzuweichen und weitergehende Bestimmungen im Sinne eines **Swiss Finishs** einzuführen.
AZ	VE DSG	7	2		**Die Einführung einer gegenüber der bisherigen Bestimmung angepasste Pflicht zur «Vergewisserung» und insbesondere der Satz «Der Bundesrat präzisiert die weiteren Pflichten des Auftragsdatenbearbeiters» sollten gestrichen werden**, da diese einen unnötigen «Swiss Finish» darstellen und da weite Delegationsbefugnisse des Bundesrats für die Festsetzung von weiteren Pflichten des Auftragsbearbeiters gar nicht notwendig sind. Ein ausreichender Sinn und Zweck für eine solche Bestimmung ist u.E. nicht ersichtlich.
AZ	VE DSG	7	3		Die gesetzlich vorgesehene Zustimmung des Verantwortlichen bei Beizug eines anderen Auftragsdatenbearbeiters ist nicht erforderlich. In der heutigen digitalen Zeit ist für eine effiziente Arbeitsteilung und stetige Optimierung der eigenen Leistungen notwendig, mit Subunternehmen

					zusammenzuarbeiten (z.B. Beizug eines professionellen, zertifizierten Hosting- oder Housinganbieters für die Bereitstellung von benötigter IT-Infrastruktur) und diese im Bedarfsfall rasch ersetzen zu können. Die Bestimmung geht deshalb klar über das Notwendige hinaus und führt zu unnötigem Zusatzaufwand ohne ersichtlichen Mehrwert. Die Pflichten des Verantwortlichen erscheinen uns auch ohne diese Regulierung klar, da er stets für die Einhaltung datenschutzrechtlicher Anforderungen sorgen muss. **Dieser Absatz sollte deshalb ersatzlos gestrichen werden**. In jedem Fall wäre aber die Voraussetzung einer «schriftlichen Zustimmung» den heutigen Gepflogenheiten einer «**dokumentierten Zustimmung**» anzupassen.
AZ	VE DSG	8			Wir begrüssen grundsätzlich die Möglichkeit, dass Empfehlungen der guten Praxis ermöglicht werden. Angesichts der stets steigenden und nicht auf einzelne Branchen abgestimmte Anforderungen im Bereich Datenschutz und der besonderen Position der Werbebranche, sind solche Empfehlungen dringend erforderlich, um aufgrund der drohenden Sanktionen die benötigte Rechtssicherheit und Klarheit zu verbessern. Aufgrund des Umstandes, dass sich der EDÖB bisher unseres Erachtens tendenziell in der Rolle des «Datenschützers» gesehen hat und seine Äusserungen verschiedentlich über das gesetzlich Erforderliche hinausgingen, besteht jedoch die Befürchtung, dass der Beauftragte hier nicht die richtige Person ist, um solche Empfehlungen objektiv, unter Beachtung der verschiedenen berechtigten Interessen und Anforderungen aus der Praxis aufzusetzen und zu beurteilen. Wir halten deshalb **ein neutrales, inklusive mit Vertretern aus der Praxis zusammengesetztes Gremium** anstelle des Beauftragten als geeigneter, entsprechende Empfehlungen aufzusetzen und zu beurteilen. Ist dies nicht möglich ist zumindest die Befugnis des Beauftragten darauf zu beschränken, dass er Vorschläge betroffener Verbände nur genehmigen kann und nicht von sich aus eigene Vorschläge durchsetzen kann. Zudem sollte in diesem Fall auch ein Rechtsmittel gegen Genehmigungs- bzw. allfällige Nichtgenehmigungsentscheide des Beauftragten möglich sein.
AZ	VE DSG	12			Es ist für uns nicht ganz nachvollziehbar, weshalb hier im Datenschutz ein spezielles Recht für den Umgang mit Daten von verstorbenen Personen vorgesehen werden muss. In vielen Bereichen, wie dem Dialogmarketing verlieren Daten von Personen mit dem Tod sowieso meist den Bearbeitungszweck. Ausserdem bestehen im Privatrecht sonst klare gesetzliche Regelungen bzw. eine ausreichende Rechtspraxis, welche Rechte die Nachkommen haben. Wir befürchten, dass diese Regelung eher zu Mehraufwand und allenfalls zu zusätzlichen Streitigkeiten zwischen und mit Nachkommen führen wird, als

					dass sie einen effektiven Zusatznutzen entfalten könnte. Ausserdem ist sie so auch nicht im E-SEV 108 oder der DSGVO vorgesehen. **Die Bestimmung sollte deshalb ersatzlos gestrichen werden.**
AZ	VE DSG	13 (14)			Generell sind wir auch im Hinblick der erheblichen (Straf-)Sanktionen besorgt, wie die umfangreichen und ausgeweiteten Informationspflichten sinnvoll und in jedem Fall ausreichend in der Praxis zu gewährleisten sind. Während eine Information in Datenschutzerklärungen auf den jeweiligen Firmenwebseiten als realisierbar erscheint, ist dies gemäss den Erläuterungen auf Seite 56 offenbar nicht zwingend ausreichend. Es wird insbesondere erwähnt, dass Betroffene nicht nach diesen Informationen suchen müssen. Diese Bestimmung sollte, wenn immer möglich, so angepasst werden, dass ausdrücklich **die Publikation der Informationen auf der Firmenwebseite (z.B. in einer Datenschutzerklärung) ausreicht, um die diesbezügliche Informationspflicht erfüllen zu können**. Bei Bestellungen und dergleichen sollte ebenfalls ein Verweis auf solche Informationen auf einer Webseite genügen. Es ist hier eine **abschliessende** und klare **Auflistung** der Informationen anzustreben, um die Rechtssicherheit zu erhöhen. Übermässige Informationen, welche eher verwirren und unnötige Zusatzaufwände generieren sind zu vermeiden. Die betroffene Person kann bei Bedarf immer noch eine Auskunft über zusätzliche Informationen verlangen.
AZ	VE DSG	13	4		Es sollte keine unnötige Pflicht zur Mitteilung von Angaben zu Auftragsdatenbearbeiter vorgesehen werden. Es reicht, dass der Verantwortliche selbst für die datenschutzkonforme Datenbearbeitung verantwortlich ist und dafür auch bei den Auftragsdatenbearbeitern im Rahmen des Gesetzes besorgt ist. Es ist nicht ersichtlich, weshalb ein Verantwortlicher jedes Mal, wenn er anschliessend einen Auftragsdatenbearbeiter (z.B. Hosting-Dienstleister) wechselt oder zusätzliche Auftragsdatenbearbeiter beizieht (z.B. Backup-Center zur Erhöhung der Datensicherheit) jedes Mal erneut informationspflichtig werden soll. Diese über die internationalen Anforderungen hinausgehende Regelung (= «Swiss Finish») führt u.E. nur zu unnötigem zusätzlichem Aufwand, zu einem zusätzlichen Risiko der Strafbarkeit bei (fahrlässigem) Vergessen der Information und zu noch ausführlicheren und damit leserunfreundlicheren Datenschutzerklärungen. Aufgrund des Gesetzes kann der handelnde Verantwortliche ja sowieso nicht einen Wechsel des Auftragsdatenbearbeiters vorsehen, welcher das DSG verletzten würde (z.B. Beizug eines Auftragsdatenbearbeiters aus einem Land ohne angemessenem Datenschutzlevels). In der Praxis führt eine solche Pflicht vor allem zu erheblichem Mehraufwand für die Wirtschaft ohne nennenswerten

					Zusatznutzen für die betroffenen Personen. **Abs. 4 sollte deshalb ersatzlos gestrichen werden**.
AZ	VE DSG	13	5		Die bei Beschaffung von Personendaten von Dritten erforderliche Information sollte nicht spätestens bei Speicherung, sondern auch nachträglich innert **angemessener Frist** (z.B. innert einem Monat) erfolgen können, wie dies selbst in der DSGVO in Art. 14 Abs. 3 lit. a vorgesehen ist. Die Information sollte so wie oben zu Art. 13 erwähnt möglich sein (insb. Hinweis auf Datenschutzerklärung auf Webseite).
AZ	VE DSG	14	4		Es ist nicht ersichtlich, weshalb hier der Katalog der Ausnahmen von der Informationspflicht anders bzw. enger definiert wird als in der E-SEV 108. Insbesondere ist nicht ersichtlich, weshalb bei einer **Weitergabe an Dritte** eine Berufung auf ein überwiegendes privates Interesse nicht möglich sein soll. Das macht u.E. in der Praxis überhaupt keinen Sinn. Die Bestimmung sollte entsprechend eingeschränkt werden.
AZ	VE DSG	16			Diese Bestimmung geht über die Anforderungen aus der E-SEV 108 und sogar der DSGVO hinaus. Dies ist generell zu vermeiden und eine entsprechende Reduktion sollte vorgenommen werden. Die Datenschutz-Folgeabschätzung wird in jedem Fall zu erheblichem Zusatzaufwand der Unternehmen führen. **Regeln im Sinne eines «Swiss Finish» sind hier unbedingt zu vermeiden**, um Rechtsnachteile von Schweizer Unternehmen gegenüber dem Ausland zu verhindern und die bereits jetzt zu erwartenden Zusatzkosten aus der Gesetzesrevision nicht noch weiter ansteigen zu lassen.
AZ	VE DSG	16	1		Ein **«erhöhtes**» Risiko sollte auf ein **«hohes»** Risiko gemäss der Regelung in der DSGVO angepasst werden, um die negativen Folgen eines «Swiss Finish» in diesem wichtigen, potentiell kostspieligen Punkt zu eliminieren. Gleiches gilt für die Erwähnung der Pflicht des Auftragsdatenbearbeiters. Die Pflicht sollte, wie auch in der DSGVO vorgesehen auf den Verantwortlichen beschränkt werden. Er ist und bleibt verantwortlich, selbst wenn er diesbezüglich versuchen wird, seine Pflicht auf den Auftragsdatenbearbeiter zu überbinden. Zudem wäre es hilfreich in den Erläuterungen oder vom EDÖB weitere Präzisierungen zu Erforderlichkeit einer solchen DS-Folgeabschätzung in konkreten Einzelfällen zu erhalten, um die diesbezüglichen Auslegungsrisiken zu reduzieren.
AZ	VE DSG	16	3		Diese Meldepflicht an den Beauftragten ist nicht in der E-SEV 108 vorgesehen. Selbst in der DSGVO (Art. 36 Abs. 1) muss die Aufsichtsbehörde nur dann konsultiert werden, wenn der Verantwortliche zum Schluss kommt, dass trotz von ihm ergriffene Schutzmassnahmen ein hohes Risiko der Verletzung der

					Persönlichkeit der betroffenen Personen bleibt. Die meisten Unternehmen und insbesondere im Bereich des Dialogmarketings wird von der vorgesehenen Meldepflicht bei vorsichtiger Anwendung des neuen Gesetzes und Beachtung der Strafandrohung einen ganz erheblichen Zusatzaufwand durch diese Meldepflicht bewältigen müssen. Ein effektiver, verhältnismässiger Nutzen daraus ist u.E. nicht gegeben. Wir sind deshalb der Auffassung, dass diese **Meldepflicht ganz zu streichen** oder – falls dies nicht möglich ist – mindestens auf das Mass der DSGVO zu reduzieren ist.
AZ	VE DSG	16	4		Vorab sind wir für die Streichung der Meldepflicht wie oben ausgeführt. Wird diese beibehalten, muss geklärt werden, welche Folge eine solche Meldung hat. Wir sind hier der Auffassung, dass ein Zuwarten mit der vorgesehenen Datenbearbeitung bis zum Entscheid des Beauftragten und insbesondere die viel zu grosszügig vorgesehene dreimonatige Frist, welche dann noch durch mögliche Nachforderungen zusätzlicher Informationen verlängert werden kann, eine zu starke Einschränkung der wirtschaftlichen Handlungsfähigkeit betroffener Unternehmen darstellt. Die **Fristen des Beauftragten sollten deshalb erheblich gekürzt und eingeschränkt werden.**
AZ	VE DSG	17			Die **Meldepflicht** ist ohne ersichtlichen Grund strenger als dies im E-SEV 108 oder sogar in der DSGVO vorgesehen ist. Sie sollte entsprechend **eingeschränkt** werden. Eine Meldung sollte nur bei **ganz erheblichen Verletzungen** greifen, wo ein Eingreifen des Beauftragten wirklich gerechtfertigt und sinnvoll erscheint und wo darüber hinaus tatsächlich ein Kontrollverlust über die Daten erfolgt, ansonsten könnte diese Bestimmung unnötig zu einer grossen Anzahl von Meldungen und/oder von strafbaren Handlungen durch die Mitarbeiter des Unternehmens führen, beispielsweise wenn diese eine Meldung fahrlässig unterlassen. Für die Meldung sollte auch zeitlich ein **angemessener Spielraum** zur Ermittlung sinnvoller Massnahmen durch das Unternehmen eingeräumt werden, um überstürzte und ungeordnete Meldungen, bei welchen der Beauftragte vermutlich sowieso wenig bewirken kann, zu verhindern. Im übrigen Verweisen wir hierzu auch auf die Ausführungen von David Rosenthal in «Der Vorentwurf für das ein neues Datenschutzgesetz: Was er bedeutet» in Jusletter 20. Februar 2017, Rz93ff, welchen wir uns anschliessen.
AZ	VE DSG	18			Die vorliegende Bestimmung erscheint uns höchst auslegebedürftig. Je nach Branche müssen vermutlich die Anforderungen unter Beachtung der Interessen individuell konkretisiert werden. Aus diesem Grund erscheint uns die Unterstellung einer Verletzung von Art. 18 unter die Sanktionsfolgen von Art. 51 Abs. 1

					auch mit Blick auf das Bestimmtheitsgebot problematisch. Die **Strafbarkeit sollte hierzu gestrichen werden**. Soll im Bereich des Dialogmarketings die aus marktwirtschaftlichen Überlegungen notwendige Ansprache von Neukunden nicht vollkommen ad absurdum getrieben werden, muss ein Spielraum der Auslegung von Art. 18 möglich sein, ohne dass eine sofortige Strafbarkeit der handelnden Mitarbeiter droht.
AZ	VE DSG	19	1	a	Die Dokumentationspflicht sollte allgemein nicht weitergehen, als die Voraussetzungen in E-SEV 108 bzw. als die DSGVO. Dies ist insbesondere erforderlich, da hier ansonsten aufgrund erheblichen Administrativaufwands Schweizer Unternehmen benachteiligt werden (vgl. auch Kommentar unten zu den Erläuterungen zu dieser Bestimmung). Diese **Bestimmung sollte deshalb einschränkt und präzisiert werden** (insb. nur regelmässige Datenbearbeitungen und keine Dokumentation von Datenschutzverletzungen). Dies ist insbesondere auch deshalb notwendig, da wir bei einer unbestimmten, weiten Definition der Dokumentierungspflicht einen ganz erheblichen Zusatzaufwand befürchten, welcher im Rahmen der bisherigen Vorarbeiten zur Revision auch nicht bzw. nicht genügend berücksichtigt wurde. Soll hier die gesamte Schweizer Wirtschaft zu uferlosen Dokumentationen auf Vorrat verpflichtet werden, stellt dies eine sinnlose Vergeudung von Ressourcen dar.
AZ	VE DSG	19	1	b	Die jederzeitige Mitteilungspflicht an Empfängerinnen und Empfänger von Personendaten ist nicht in der E-SEV 108 vorgesehen und sie führt in der Praxis insbesondere bei Beachtung der Erläuterungen zu einem erheblichen Mehraufwand und schwierigen Auslegungs- und Abgrenzungsfragen. Werden zum Beispiel für eine Werbekampagne einem Adressbezüger einmalig Adressdaten zur Ansprache von Neukunden für eine einzelne Kampagne zur Verfügung gestellt, würde eine wörtliche Anwendung dieser Klausel dazu führen, dass dem Adressbezüger anschliessend quasi lebenslänglich sämtliche Änderungen der Daten etc. und erst noch kostenlos zur Verfügung gestellt werden müssten. Diese Bestimmung ist so nicht durchsetzbar und sie berücksichtigt auch in keiner Weise, dass eine Weitergabe von Daten an Empfängerinnen und Empfänger durchaus nur für einen bestimmten einmaligen Zweck oder eine bestimmte begrenzte Dauer erfolgt. Später ist eine zwingende Mitteilung unsachgemäss und sinnlos. Diese Bestimmung ist deshalb **ersatzlos zu streichen**.
AZ	VE DSG	20	1		Die Kostenlosigkeit des Auskunftsrechts, verbunden mit der weiterreichenden Auskunftspflicht führt zu erheblichen Zusatzkosten und auch einem derzeit kaum eingeschränkten Missbrauchspotenzial. Weder E-

					SEV 108 noch die DSGVO sehen eine solche jederzeit zwingende Kostenlosigkeit vor. Es sollte deshalb eine **angemessene Entschädigungsmöglichkeit vorgesehen** werden. Aufgrund der Kostenlosigkeit wird der Missbrauch des Auskunftsrechts (z.B. als Rache durch Mitarbeiter oder unzufriedenen Kunden) gefördert. Zumindest sollten ausreichende **Ausnahmen** von der Kostenlosigkeit und – wo sinnvoll – generell ein Ausschluss eines Auskunftsrechts bestimmt werden. Dies gilt insbesondere, sofern eine Auskunft bereits früher erteilt wurde bzw. die angefragten Informationen bereits früher zugestellt wurden und sofern Auskünfte ohne erkennbaren Grund, querulatorisch oder in einer anderen Form gegen Treu und Glauben verstossend verlangt werden usw. (vgl. dazu auch Art. 12 Abs. 5 lit. a DSGVO).
AZ	VE DSG	20	3		Diese Bestimmung weicht ohne ersichtlichen Grund von den Anforderungen an automatisierte Entscheidungen in Art.15 VE DSG ab. Sie ist **zu löschen** bzw. auf die dort erwähnten rechtlichen Wirkungen oder erheblichen Auswirkungen auf die betroffene Person **zu beschränken**. Zudem sollte in den Erläuterungen zu Art. 20 Abs. 2 sowie zu Art. 15 VE DSG erwähnt werden, dass der Begriff «rechtliche Wirkung» eng auszulegen ist. Diese Wirkung muss direkt und offensichtlich mit der automatisierten Entscheidung erfolgen. Hypothetische spätere oder konstruierte rechtliche Wirkungen (z.B. für persönliche Werbung mit gewissen Vorteilspreisen etc., welche dazu führen, dass gewisse Kunden bei einem allfälligen späteren Rechtsgeschäft einen besseren Preis erzielen können als andere) sind zu vermeiden, um den Anwendungsbereich und eine allfällige Strafbarkeit bei Verletzung dieser Norm genügend klar zu präzisieren.
AZ	VE DSG	23	2	d	Das viel zu weit definierte «Profiling» gemäss VE DSG ohne ausdrückliche Einwilligung (vgl. oben) wird hier per se als Persönlichkeitsverletzung aufgeführt. Diese **Bestimmung sollte u.E. ersatzlos gestrichen werden**. Im Gegensatz zur Bekanntgabe von besonders schützenswerten Daten ist es nicht ersichtlich und wird in den Erläuterungen auch nicht näher begründet, weshalb hier eine per se Persönlichkeitsverletzung vorgesehen werden muss. Auch hier besteht wieder eine erhebliche Gefahr, dass potentiell eine grosse Anzahl von Mitarbeitern im Geschäftsleben im Zusammenhang mit sinnvollen Auswertungen von Daten, um beispielsweise die Effizienz eigener Produkte und Dienstleistungen zu steigern, riskieren, sich zumindest fahrlässig strafbar zu machen. Dies ist zudem verbunden mit erheblichen drohenden Straffolgen. Hier entsteht wiederum der Eindruck, dass mit der vorliegenden Regelung erheblich über das Ziel hinausgeschossen wird und damit ein zu vermeidender «Swiss Finish» vorgesehen wird. Diese Vorschrift könnte erhebliche negative, nicht beabsichtigte Folgen für die Schweizer Wirtschaft und die

					Werbebranche im Besonderen nach sich ziehen. Insbesondere könnten hier wiederum internationale Grosskonzerne, vorab im Social Media-Bereich, für welche die jederzeitige Einholung praktisch beliebiger Einwilligungen möglich ist, zusätzlich begünstigt werden und Schweizer KMU hätten das Nachsehen.
AZ	VE DSG	25	2		Es ist für uns nicht nachvollziehbar, weshalb neben der Möglichkeit eines Bestreitungsvermerks zusätzlich noch eine Einschränkung der Bearbeitung der bestrittenen Daten verlangt werden kann. Diese Einschränkung ist offenbar ohne jegliche zusätzlichen Anforderungen möglich. Dies geht zu weit und der **letzte Satz der Bestimmung sollte deshalb gelöscht werden**. Falls dies nicht möglich ist, sollte er so angepasst werden, dass eine Einschränkung ausdrücklich nur bei Vorliegen überwiegender Interessen möglich ist.
AZ	VE DSG	44	3		Wir erachten es als problematisch, dass Beschwerden gegen vorsorgliche Massnahmen per se keine aufschiebende Wirkung haben sollen. Je nach Einzelfall könnten solche Massnahmen massive Nachteile für die Betroffenen zur Folge haben, welche der EDÖB oft nicht angemessen einschätzen kann. Den von solchen vorsorglichen Massnahmen Betroffenen sollte deshalb unbedingt die Möglichkeit eingeräumt werden, sich vor einer unabhängigen Instanz gegen überschiessende vorsorgliche Massnahmen des EDÖB wehren zu können. Das **bisherige System**, nachdem der EDÖB solche Massnahmen vom Bundesverwaltungsgericht beantragen muss, **erscheint hier deutlich angemessener und sinnvoller** zu sein (vgl. dazu David Rosenthal, «Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet», in: Jusletter 20. Februar 2017, Rz 124).
AZ	VE DSG	50ff			Vorab verweisen wir auch auf unsere allgemeine Stellungnahme zu **übermässiger Sanktionsregelung** oben. Sanktionen sollten u.E. **auf die Anforderungen von E-SEV 108 reduziert** werden. Die Auswirkungen durch E-SEV 108 und die teilweise direkte Anwendbarkeit von der DSGVO auf Schweizer Unternehmen mit Auslandberührung sind bereits erheblich, weshalb die Sanktionen nicht über die Minimalanforderungen hinausgehen sollten. Der Aufwand wird in jedem Fall für KMU sogar überproportional steigen. Zudem sollten Sanktionen gegen die Unternehmen und nicht eine Kriminalisierung einer Vielzahl von Mitarbeitern im Vordergrund stehen. Der persönliche, strafrechtliche Charakter der vorgeschlagenen Sanktionen führt zu einer Angstkultur der Mitarbeiter in einem Betrieb. Dies folgt insbesondere auch aufgrund der Strafbarkeit der fahrlässigen Begehung. Die Begehung einer Straftat ist ebenfalls möglich, wenn ein Mitarbeiter eine Meldung schlicht vergisst oder aus Angst vor einer

					Vergiftung des Klimas in der Belegschaft es unterlässt, eine Persönlichkeitsverletzung eines Arbeitskollegen oder sogar eines Vorgesetzten zu melden. Der Kreis der möglichen «Täter» wird auch mit Blick auf die weite Anwendbarkeit der neuen Gesetzesbestimmungen ungebührlich weit gesteckt. Es ist hier u.E. äusserst fraglich, ob diese Bestimmungen tatsächlich als genügend bestimmt angesehen werden können, um die vorgesehen Strafsanktionen zu rechtfertigen. Kommt hinzu, dass die kantonalen Strafverfolgungsbehörden sich auch mit den neuen, komplexen datenschutzrechtlichen Bestimmungen infolge fehlendem Fachwissen schwertun könnten und damit ausserdem das Risiko von uneinheitlicher Rechtspraxis zusätzlich erhöht würde. Die Sanktionen sind deshalb grundlegend anzupassen. Diesbezüglich schliessen wir uns dem sinnvollen Vorschlag eines **Grobkonzepts der economiesuisse** an. Vor allem unterstützen wir primär verwaltungsrechtiche Sanktionen gegen Unternehmen und erst subsidiär eine Haftung bei vorsätzlichem Handeln durch Mitarbeiter vorzusehen. Dabei sollte insbesondere auch der Strafkatalog überarbeitet und eingeschränkt, Strafminderungsgründe bei aktiver Mitwirkung in einem Verfahren und bei einer Implementierung geeigneter Compliance-Massnahmen durch die Unternehmen vorgesehen und die Rolle des EDÖBs entsprechend angepasst werden. Solche Massnahmen erscheinen uns ebenfalls geeigneter, den Datenschutzlevel in der Schweiz insgesamt zu heben als das im VE DSG vorgeschlagene Sanktionssystem.
AZ	VE DSG	52			Es ist u.E. kein Bedürfnis ersichtlich, wieso die bisherige Bestimmung in Art. 35 DSG durch eine solch weitgehende neue Bestimmung einer beruflichen Schweigepflicht ersetzt werde muss. Es können damit beliebige Fälle umfasst werden und die Kriminalisierung im Geschäftsleben wird weiter ausgebaut ohne einen erkennbaren Zusatznutzen zu ermöglichen. Die **bisherige Regelung sollte deshalb nicht erweitert werden**.
AZ	VE DSG	59			Die Übergangsbestimmung ist nur sehr punktuell ausgestaltet und sie reicht u.E. nicht aus, um die umfangreichen, sich abzeichnenden Anpassungen rechtzeitig umzusetzen. Die Frist von 2 Jahren sollte **generell für alle Bestimmungen** analog der Regelung für die DSGVO festgelegt werden. Dazu ist ebenfalls noch zu beachten, dass viele der in der Praxis dringend benötigten Zusatzinformationen erst noch aus Verordnung bzw. Empfehlungen der guten Praxis hervorgehen werden, welche derzeit noch nicht feststehen.

					Ausserdem sollte festgehalten werden, dass eine **Rückwirkung des Gesetzes** auf bisher rechtmässig erhobenen Personendaten **ausgeschlossen** ist. Die Bestimmung sollte nur für neu beschaffte bzw. erhobene Daten geltend, um die erheblichen Folgen der neuen Bestimmungen und die damit verbundenen Aufwände und Kosten in einem verträglichen Ausmass zu halten.

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
AZ	

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

Name/Firma	Bemerkung/Anregung
AZ	

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

Name/Firma	Kapitel-Nr.	Bemerkung/Anregung
AZ	Zusammen-fassung und 1	Generell fehlen hier u.E. die Berücksichtigung oder Erwähnungen der Interessen der Wirtschaft und insbesondere auch der Werbebranche. Es wird nicht auf die bisher gewachsene Abgrenzung zwischen erlaubtem und als unlauter verbotenem Handeln bei persönlicher Werbung eingegangen. In einer Marktwirtschaft wie der Schweiz besteht ein erhebliches Interesse daran, dass Unternehmen ihre Produkte und Dienstleistungen neuen und bestehenden Kunden anbieten können und, dass dafür eine Datenbearbeitung unter Befolgung gewisser Rahmenbedingungen (vor allem Sterneinträge, Robinsonlisten, «Spam»-Verbot etc.) grundsätzlich möglich sein muss und dass diese nicht einfach faktisch durch neue, datenschutzrechtliche Auflagen verunmöglicht werden. Im Gegensatz zu der DSGVO wird nirgends auf das diesbezüglich bestehende berechtigte Interesse eingegangen. Dies erachten wir als einseitig und zu wenig ausgewogen. Zumindest in den Erläuterungen sollte deshalb ein entsprechendes Interesse anerkennend erwähnt werden.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
AZ	3 Bst. a	Der Hinweis auf die bisherige Definition von Personendaten und die Befolgung der «relativen Methode» zur genaueren Bestimmung ist u.E. richtig und wird begrüsst. Jedoch erachten wir die Ausführungen im Zusammenhang mit der Bestimmbarkeit einer Person zu «…Hinweise auf eine Identifikationsnummer oder eine Online-Identität…» als missverständlich und gefährlich. Geht es, wie bei der Online-Werbung bei Verwendung von IP-Adressen nur um die Ermöglichung der Kategorisierung eines Nutzers und nicht um dessen persönliche, namentliche Identifikation, werden keine Personendaten erfasst, ansonsten ein grosser Teil der Werbung im Internet plötzlich (zumindest bei Betrieb der entsprechenden Infrastruktur in der Schweiz) nicht mehr zulässig wäre. Mit der Bildung von Kategorien und der Ermöglichung besser auf die Nutzer abgestimmter Werbung wird die Effizienz der Werbung deutlich gesteigert, ohne dass dabei jedoch neue Personendaten geschaffen werden. **Die Botschaft sollte deshalb in diesem Punkt entsprechend angepasst werden. Sie sollte dabei auf die unveränderte geltende Praxis und Rechtsprechung und insbesondere die eingangs zitierten Hinweise zu Identifikationsnummer oder Online-Identität sollten gestrichen oder präzisiert werden.**
AZ	3 Bst. f	Ebenfalls geht es u.E. viel zu weit, einen zusätzlichen Begriff «Daten» im Gesetz im Zusammenhang mit dem äusserst weit verstandenen Profiling aufzunehmen, um jegliche in Zukunft auch rein hypothetisch mögliche Personenzuweisung vorsorglich einzuschränken. Damit werden mögliche sinnvolle Entwicklungen, für welche durchaus berechtigte Interessen bestehen können, zum Vorherein unnötig eingeschränkt oder gar verhindert. Das sollte auch in den Erläuterungen entsprechend angepasst werden. Der Begriff «Profiling» sollte nur solche Auswertungen erfassen, welche tatsächlich zu einer **erheblichen Beeinträchtigung der Persönlichkeit** einer betroffenen Person führen und nicht zum vornherein jegliche möglichen, die Persönlichkeit kaum oder höchstens unerheblich betreffende Auswertungen kategorisch verhindern. Es wäre u.E. auch durchaus möglich, am bisherigen Modell des Persönlichkeitsprofils festzuhalten und auf spezielle Regelungen des Profiling (ggfs. mit Ausnahme der Erwähnung zusammen mit den qualifizierten, automatischen Entscheidungen) zu verzichten.
AZ	4 Abs. 6	Am Ende dieses Kapitels werden Ausführungen zur ausdrücklichen Einwilligung gemacht. Die Erläuterungen könnten so verstanden werden, dass für die ausdrückliche Einwilligung insbesondere das aktive Anklicken eines Kästchens oder ähnlich immer erforderlich ist. Damit werden die Grenzen zu einem «Opt-In» wie es zum Beispiel bei der Verwendung von E-Mailadressen gemäss Art. 3 Abs. 1 lit. o UWG erforderlich ist, verwässert. Dies sollte in der Botschaft entsprechend relativiert werden. Ein Opt-Out sollte bei

		entsprechender Information ausreichen. Generell sollte auf die generelle Voraussetzung einer «ausdrücklichen Einwilligung» wie weiter oben erwähnt verzichtet werden und in den Erläuterungen klargestellt werden, dass hier keine Änderung der Rechtslage in der Schweiz beabsichtigt ist. Im Übrigen sollte hier auch klargestellt werden, dass eine Einwilligung auch in AGBs und dergleichen vorgesehen werden kann.
AZ	4 Abs. 6	Zu *Absatz 6* wird ausserdem erwähnt, dass eine Einwilligung «den gesamten Zweck der Bearbeitung abdecken muss». Dies sollte so präzisiert werden, dass die Einwilligung den Zweck der Bearbeitung abdeckt, für welchen sie eingeholt wird (vgl. David Rosenthal in «Der Vorentwurf für das ein neues Datenschutzgesetz: Was er bedeutet» in Jusletter 20. Februar 2017, Rz 28).
AZ	8	Wie bereits in der Stellungnahme zu dieser Bestimmung weiter oben erwähnt, sollte besser ein neutrales Gremium für die Empfehlungen und Genehmigung derselben vorgesehen werden. In jedem Fall sollte jedoch nicht der EDÖB selbst von sich aus solche Empfehlungen ausarbeiten, sondern diese höchstens genehmigen können. Gegen den Genehmigungsentscheid ist aufgrund der erheblichen praktischen Auswirkungen solcher Empfehlungen ein Rechtsmittel zu ermöglichen.
AZ	13	Die zu dieser Bestimmung gemachten Ausführungen sollten auch in den Erläuterungen entsprechend gespiegelt werden. Insbesondere sollte die Möglichkeit der Publikation der Informationen auf der Webseite (insb. Datenschutzerklärung) und des Verweises auf diese erwähnt werden. Die Informationspflicht sollte sich zudem auf den Zeitpunkt der Datenbeschaffung beschränken und grundsätzlich keine Nachinformation erfordern. Ausserdem ist bei indirekter Datenbeschaffung eine Frist analog der DSGVO einzuräumen (vgl. oben).
AZ	18	Wie zu dieser Bestimmung vorne erwähnt, sollte auch in den Erläuterungen auf den notwendigen Spielraum bei der Umsetzung dieser Klausel im Einzelfall hingewiesen werden.
AZ	19 Bst. a	Die Erläuterungen zu Art. 19 Bst. a VE DSG sollten eingeschränkt werden, indem klargestellt wird, dass nur regelmässige Datenbearbeitungen zu dokumentieren sind und nur strukturierte Datensammlungen erfasst werden sollten. Eine Pflicht zur Dokumentierung jeglicher Datenbearbeitungen sowie von sämtlichen Datenschutzverletzungen, wie letzteres gemäss Erläuterung offenbar vorgesehen ist, geht u.E. viel zu weit und würde wortwörtlich jede Korrespondenz mit einer Person bzw. jeden Einzelfall umfassen. Selbst die DSGVO ist in diesem Bereich präziser formuliert. In Anbetracht des zu erwartenden Zusatzaufwandes ist auch hier eine Reduktion auf das absolut Wesentliche unbedingt angezeigt.
AZ	23 Abs. 3	Der letzte Satz zu *Absatz 3* sollte nicht in die Botschaft übernommen werden. Die Bearbeitung von Daten, welche im Wissen und

		Willen einer Person publiziert wurden, ist gemäss bisherigem Recht in der Regel selbst dann rechtmässig, wenn sie unter Verletzung der Bearbeitungsgrundsätze erfolgt (vgl. dazu David Rosenthal in «Der Vorentwurf für das ein neues Datenschutzgesetz: Was er bedeutet» in Jusletter 20. Februar 2017, Rz 19).
AZ	50 ff.	Die Erläuterungen sollten die notwenigen Anpassungen bzw. Neudefinierung des Sanktionssystems wiedergeben und dabei insbesondere den Vorschlag der economiesuisse (Grobkonzepts) erläutern.
AZ	Art. 179^{novies} StGB	Die Ausweitung der Strafbarkeit gemäss der neuen Bestimmung und Anpassung des Wortlautes führt zu einer erschwerten Abgrenzung zu den sonstigen Straftatbeständen im VE DSG. Der bisherige Anwendungsbereich sollte hier u.E. nicht weiter ausgebaut werden.
AZ	Art. 179^{decies} StGB	Diese neue Klausel erachten wir als sinnvoll, um die Problematik des Identitätsmissbrauchs im Internet besser adressieren zu können.

Amstutz Jonas BJ

Von: Danielle Kaufmann <danielle.kaufmann@unibas.ch>
Gesendet: Sonntag, 2. April 2017 13:36
An: Amstutz Jonas BJ
Cc: Herbert Staub (herbert.staub@bis.ch)
Betreff: Stellungnahme des Bibliotheksverbands (BIS) zur DSG-Totalrevision
Anlagen: DOKU_Stellungnahme_DSG_BIS_20170309_dka.doc

Sehr geehrte Frau Bundesrätin
sehr geehrte Damen und Herren

Besten Dank für die Möglichkeit zur Stellungnahme im Rahmen der Vernehmlasung zur Totalrevision des Datenschutzgesetzes, von der der **Bibliotheksverband - Bibliothek Information Schweiz (www.bis.ch)** gerne Gebrauch macht.

Die Bibliotheken, Dokumentationsstellen und Archive sind täglich konfrontiert mit Personendaten. Sei es mit den Daten ihrer Nutzerschaft oder auch mit Daten, die sich in den Werken befinden, die die Gedächtnisinstitutionen in ihren Beständen sammeln, aufbewahren und zugänglich machen. Die Institutionen sind sich der Verantwortung für einen sorgfältigen und korrekten Umgang mit diesen Daten sehr bewusst. Gerade anhand der Kombination der Personendaten der Nutzer mit deren jeweiligen Ausleihdaten kann ein sogenanntes Profiling der betroffenen Person gemacht werden, weshalb die Bibliotheken und andere Gedächtnisinstitutionen mit diesen Daten besonders vorsichtig umgehen und diese nur so lange als erforderlich aufbewahren. Neben den entsprechenden gesetzlichen Grundlagen sind die Bibliotheken auch ihrem eigenen Ethikkodex (http://www.bis.ch/fileadmin/ressourcen/arbeitsgruppen/Ethikcode_d.pdf) verpflichtet, der unter anderem auch die Vertraulichkeit im Umgang mit den Daten der Nutzer vorschreibt.
Gleichzeitig wollen die kulturellen Gedächtnisinstitutionen bezüglich der Daten in ihren Beständen – seien es beispielsweise persönliche Briefe in einem Archiv, Fotografien von Menschen in einer Dokumentationsstelle oder digitalisierte historische Tageszeitungen – ihrem Auftrag des Bewahrens und Zugänglichmachens von Dokumenten gerecht werden, um damit Rückschlüsse auf die Vergangenheit zu ermöglichen und zwar originalgetreu ohne Veränderungen durch die Gegenwart. In diesem Sinn begrüsst der Bibliotheksverband, dass der Entwurf für das revidierte Datenschutzgesetz die Interessen der kulturellen Gedächtnisinstitutionen bei der Regelung für ein Recht auf Vergessen grundsätzlich berücksichtigt hat und damit einen unverfälschten, uneingeschränkten und auch langfristigen Zugang zu Dokumenten und Informationen sichert.

Im Anhang überlasse ich Ihnen fristgerecht die detaillierte Stellungnahme im vorgegebenen Formular.

Wir danken Ihnen für die wohlwollende Kenntnisnahme unserer Anmerkungen. Selbstverständlich stehe ich Ihnen für Rückfragen jederzeit gerne zur Verfügung.

Mit freundlichen Grüssen

Danielle Kaufmann

UNIVERSITÄT BASEL
Universitätsbibliothek
Danielle Kaufmann, lic. iur.
Projektleitung Competence Center in Digital Law
Rechtsdienst Universitätsbibliothek Basel
Präsidentin AG Urheber- & Datenschutzrecht BIS

Schönbeinstrasse 18-20
4056 Basel, Schweiz
Tel. +41 (0)61 207 31 22
Fax +41 (0)61 207 31 03
e-mail Danielle.Kaufmann@unibas.ch
URL http://www.ub.unibas.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 : Bibliotheken Information Schweiz

Abkürzung der Firma / Organisation : BIS

Adresse : Bleichemattstrasse 42, 5000 Aarau

Kontaktperson : lic. iur. Danielle Kaufmann

Telefon : 061 207 31 22

E-Mail : danielle.kaufmann@unibas.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 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 4

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 6

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten 7

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") 7

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" 7

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
Fehler! Verweisquelle konnte nicht gefunden werden.	Die Bibliotheken, Dokumentationsstellen und Archive sind täglich konfrontiert mit Personendaten. Sei es mit den Daten ihrer Nutzerschaft oder auch mit Daten, die sich in den Werken befinden, die die Gedächtnisinstitutionen in ihren Beständen sammeln, aufbewahren und zugänglich machen. Die Institutionen sind sich der Verantwortung für einen sorgfältigen und korrekten Umgang mit diesen Daten sehr bewusst. Gerade anhand der Kombination der Personendaten der Nutzer mit deren jeweiligen Ausleihdaten kann ein sogenanntes Profiling der betroffenen Person gemacht werden, weshalb die Bibliotheken und andere Gedächtnisinstitutionen mit diesen Daten besonders vorsichtig umgehen und diese nur so lange als erforderlich aufbewahren. Neben den entsprechenden gesetzlichen Grundlagen sind die Bibliotheken auch ihrem eigenen Ethikkodex (http://www.bis.ch/fileadmin/ressourcen/arbeitsgruppen/Ethikcode_d.pdf) verpflichtet, der unter anderem auch die Vertraulichkeit im Umgang mit den Daten der Nutzer vorschreibt. Gleichzeitig wollen die kulturellen Gedächtnisinstitutionen bezüglich der Daten in ihren Beständen – seien es beispielsweise persönliche Briefe in einem Archiv, Fotografien von Menschen in einer Dokumentationsstelle oder digitalisierte historische Tageszeitungen – ihrem Auftrag des Bewahrens und Zugänglichmachens von Dokumenten gerecht werden, um damit Rückschlüsse auf die Vergangenheit zu ermöglichen und zwar originalgetreu ohne Veränderungen durch die Gegenwart. In diesem Sinn begrüsst der Bibliotheksverband, dass der Entwurf für das revidierte Datenschutzgesetz die Interessen der kulturellen Gedächtnisinstitutionen bei der Regelung für ein Recht auf Vergessen grundsätzlich berücksichtigt hat und damit einen unverfälschten, uneingeschränkten und auch langfristigen Zugang zu Dokumenten und Informationen sichert.
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	8	2		Die Bibliotheken begrüssen die neu geschaffene Möglichkeit der Ausarbeitung von Empfehlungen der guten Praxis. Der Bibliotheksverband wird gerne davon Gebrauch machen, entsprechende Empfehlungen ausarbeiten und sie vom Datenschutzbeauftragten genehmigen lassen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	12	4		Hier fehlt aus unserer Sicht die Ausnahme zum Recht auf Vergessen (vgl. dazu auch die Anmerkung zu Art. 34 Abs. 4 E-DSG). Verlangt ein Erbe die Löschung der Daten des Erblassers, kann sich die Bibliothek nur auf überwiegende Interessen von Dritten oder der verstorbenen Person selber berufen, nicht aber auf eigene Interessen oder gesetzliche Pflichten, wie beispielsweise Aufbewahrungspflichten.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	19		b	Hier fehlt die Begrenzung auf Fälle, in denen die betroffene Person ein schützenswertes Interesse hat. Für Bibliotheken und andere Gedächtnisinstitutionen würde diese absolute Regelung zu einem unverhältnismässigen Aufwand führen, wobei die Beurteilung der Verhältnismässigkeit beim Umfang der möglichen Daten für sich alleine schon ein Problem darstellen würde. Die Bestimmung käme beispielsweise zur Anwendung, wenn die Ausleihdaten der Benutzer gelöscht werden, was die Bibliotheken aus Datenschutzgründen in regelmässigen Abständen unternehmen müssen: die Bibliotheken müssten jeweils alle entsprechenden Nutzer darüber informieren. Die Bestimmung muss aus unserer Sicht daher auf Fälle begrenzt sein, in denen eine Person die Nachinformation aus berechtigten Gründen verlangt.
Fehler! Verweisquelle konnte nicht	DSG	25	4		Hier fehlt die ausdrückliche Erwähnung des Rechts auf Vergessen (vgl. dazu auch die Anmerkung zu Art. 34 Abs. 4 E-DSG)

gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	29	5		Art. 29 Abs. 5 E-DSG liefert eine gesetzliche Grundlage für die Veröffentlichung von Personendaten im Internet durch die Bundesbehörden. Zudem wird die Löschung dieser Personendaten geregelt. Demnach sind veröffentlichte Personendaten aus den automatisierten Informations- und Kommunikationsdiensten wieder zu löschen, wenn kein öffentliches Interesse mehr daran besteht, dass sie allgemein zugänglich sind. Wir schätzen die Absicht, die Personendaten im Internet auch wieder zu löschen. Doch ist festzuhalten, dass die jeweilige Bundesbehörde die Daten auf ihrer Website löschen kann, dies jedoch nicht mit der Löschung der Daten im Internet gleichzusetzen ist. Einmal im Internet publizierte Daten können abgegriffen, d.h. kopiert und wieder anderweitig verwendet werden, was denn auch regelmässig geschieht und mit dem Schlagwort «Das Internet vergisst nichts!» zusammengefasst wird. Es entzieht sich folglich der Verfügungsmacht der jeweiligen Bundesbehörde, die Daten im Internet vollumfänglich zu entfernen, weshalb besondere Zurückhaltung in Bezug auf Veröffentlichungen geboten ist.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	34	4		Bislang herrschte für Bibliotheken und andere kulturelle Gedächtnisinstitutionen in Bezug auf den geltenden Art. 25 DSG Unsicherheit, wie bei einer Durchsetzung eines schutzwürdigen Interesses vorzugehen ist. Wir begrüssen die explizite Behandlung von Gedächtnisinstitutionen in dieser Fragestellung, einerseits weil es Sicherheit in der Zurverfügungstellung digitalisierter Informationen betrifft und andererseits den Bearbeitungsaufwand reduziert. Dabei stellt sich uns allerdings die Frage, warum die Einschränkung von Art. 34 Abs. 4 E-DSG des Rechts auf Vergessens nur bei Bundesorganen gelten soll und nicht auch bei privaten Datenbearbeitern. In **Art. 25 E-DSG** sind anders wie in Art. 34 Abs. 4 E-DSG die Interessen der Gedächtnisinstitutionen nicht ausdrücklich erwähnt, sondern nur in den Erläuterungen beispielhaft aufgezählt. Wir fordern, dass die Bibliotheken, Archive und

					andere Gedächtnisinstitutionen, welche keine Bundesorgane sind, hier gleichgestellt werden und in Art. 25 E-DSG der entsprechende Absatz eingefügt wird. Im Weiteren fehlt die Ausnahme zum Recht auf Vergessen ebenfalls in **Art. 12 Abs. 4 E-DSG**, wonach Erben einen Löschungsanspruch haben bezüglich der Daten des Erblassers. Auch in diesem Fall muss aus unserer Sicht eine Interessenabwägung zwischen den Interessen der Allgemeinheit an dem unverfälschten, uneingeschränkten und nachhaltigen Zugang zu Dokumenten und Informationen und den Interessen der Erben erfolgen und der Entscheid darf nicht alleine den Erben überlassen sein. Eine ausdrückliche Erwähnung der gegenläufigen Interessen der Gedächtnisinstitutionen in Art. 12 Abs. 4 und Art. 25 E-DSG bedeutet für Bibliotheken, Archive und ähnliche Institutionen mehr Rechtssicherheit.
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: Thomas Aegerter <thomas.aegerter@bisnode.com>
Gesendet: Freitag, 31. März 2017 15:10
An: Amstutz Jonas BJ
Betreff: Stellungnahme der Bisnode D&B Schweiz AG zu VE DSG
Anlagen: 2017_03_23_Stellungnahme_DSG_Bisnode.doc

Wichtigkeit: Hoch

Sehr geehrter Herr Amstutz,

Gemäss Medienmitteilung vom 21. Dezember 2016 hat der Bundesrat interessierte Kreise dazu eingeladen zum Vorentwurf der Totalrevision des Datenschutzgesetzes (DSG) Stellung zu beziehen.

Gerne machen wir von dieser Möglichkeit Gebrauch und senden Ihnen unsere Stellungnahme nach sorgfältiger Prüfung fristgerecht im Anhang.

Wir bitten Sie, unsere Einwände sorgfältig zu prüfen und stehen Ihnen für weitere Ausführungen und Fragen gerne zur Verfügung.

Freundliche Grüsse,

THOMAS AEGERTER
Leader Data Management

BISNODE D&B SCHWEIZ AG
Direct: +41 44 735 64 42
Mobile: +41 79 592 06 77
Fax: +41 44 735 63 20
thomas.aegerter@bisnode.com
Grossmattstrasse 9, CH-8902 Urdorf
www.bisnode.ch

Folgen Sie Bisnode D&B auf Social Media:
LinkedIn - XING - Twitter - Facebook - Google+ - Youtube

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 : Bisnode D&B Schweiz AG

Abkürzung der Firma / Organisation : Bisnode

Adresse : Grossmattstrasse 9, 8902 Urdorf

Kontaktperson : Thomas Aegerter

Telefon : +41 44 735 64 42

E-Mail : thomas.aegerter@bisnode.com

Datum : 23.03.2017

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

Allgemeine Bemerkungen 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 3

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 18

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten 18

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") 19

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" 19

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.	
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
Bisnode	DSG	1			Gemäss dem Wortlaut des VE DSG würden zwar juristische Personen nicht mehr unter den Schutzbereich des VE DSG fallen, im Handelsregister eingetragene Einzelunternehmen und Mitglieder von Personengesellschaften jedoch schon. Eine derartige Unterscheidung zwischen juristischen Personen und

					im Handelsregister eingetragenen Einzelunternehmen sowie von Mitgliedern von Personengesellschaften ist nicht sachgerecht und daher nicht vertretbar. **Änderung**: Juristische Personen, im Handelsregister eingetragene Einzelunternehmen und Mitglieder von Personengesellschaften sollen ausdrücklich aus dem Schutzbereich des DSG genommen werden.
Bisnode	DSG	2	2	c	Die Unterstellung von Datenbearbeitungen im Rahmen von hängigen Gerichtsverfahren birgt ein grosses Missbrauchspotenzial. Die Parteien werden in diese Falle das datenschutzrechtliche Auskunftsbegehren zur Beweismittelbeschaffung zweckentfremden, da hierfür eine niedrigere Hürde besteht als z.B. für das Editionsverfahren gemäss ZPO. Ist ein Verfahren vor Gericht hängig, wird die Persönlichkeit der Parteien durch die jeweils anwendbaren Verfahrensbestimmungen geschützt. **Änderung**: Bisnode ist der Meinung, dass der Wortlaut des aktuellen DSG beibehalten werden sollte.
Bisnode	DSG	3		f	Der Begriff „Profiling“ wurde aus dem EU-Recht übernommen. Es ist davon auszugehen, dass diese Übernahme in der Umsetzung dazu führen würde, dass sich Gerichte und sonstige anwendende Stellen an der europäischen Rechtsprechung orientieren. Eine solche Entwicklung ist abzulehnen. Die Bestimmung über das Profiling wurde zudem überhaupt nicht im Sinne der europäischen Bestimmungen übernommen. Während das „Profiling“ nach dem europäischen Recht ausschliesslich die automatisierte Verarbeitung von Personendaten erfasst, fällt gemäss dem Wortlaut des VE-DSG jede Auswertung von Daten und Personendaten unter diesen Begriff. Die europäischen Bestimmungen bezwecken, dass eine betroffene Person nicht einer ausschliesslich auf einer automatisierten Verarbeitung (d.h. ohne die Beurteilung durch eine natürliche Person) beruhenden Entscheidung unterworfen werden kann. Die in der VE-DSG vorgesehene Regelung führt nun allerdings dazu, dass jede Art von Voraussage von Vornherein pönalisiert wird und zwar auch solche, die von natürlichen Personen aufgrund einer manuellen Durchsicht von Daten getroffen werden. Zusätzlich liegt gemäss dem VE-DSG ein Profiling auch dann vor, wenn Daten ausgewertet werden, die keine Personendaten darstellen, um wesentliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität. Bisnode lehnt diese Regelung ab, denn das DSG ist bestimmungsgemäss dann anwendbar,

					wenn Personendaten bearbeitet werden. Gemäss Art. 23 Abs. 1 lit. d VE-DSG stellt jedes Profiling ohne eine Einwilligung eine unrechtmässige Datenbearbeitung dar und zwar unabhängig davon, ob die Auswertung überhaupt eine Auswirkung auf die betroffene Person hat. Zusammen mit dem Umstand, dass auch die Auswertung von „Daten" unter den Begriff des Profilings fällt, wird dies in der Praxis dazu führen, dass bereits für jede manuelle Durchsicht von Daten eine Einwilligung benötigt wird. Dies ist praktisch nicht umsetzbar. **Änderung**: Bisnode ist der Meinung, dass die aktuell gültige Definition der „Persönlichkeitsprofile" in der VE-DSG belassen und der Begriff des „Profilings" gestrichen werden sollte.
Bisnode	DSG	3		h und i	Die Pflichten des Verantwortlichen und des Auftragsdatenbearbeiters sind nicht klar abgegrenzt. Zudem werden dem Auftragsdatenbearbeiter Pflichten auferlegt, die dieser praktisch nicht erfüllen kann. Insbesondere kann hier die Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung gemäss Art. 16 VE-DSG genannt werden. Der Auftragsbearbeiter wird nicht über alle notwendigen Informationen für die Durchführung einer solchen Folgeabschätzung verfügen. Auch die Information einer betroffenen Person über jede Berechtigung, Löschungen oder Vernichtung seiner Personendaten soll gemäss Art. 19 lit. b VE-DSG sowohl dem Verantwortlichen als auch dem Auftragsbearbeiter gesetzlich auferlegt werden. Hierbei wird übersehen, dass ein Auftragsbearbeiter Personendaten nur so bearbeiten darf, die der Verantwortliche es dürfte. Der Verantwortliche bleibt dabei gegenüber den betroffenen Personen für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich und haftet ihnen gegenüber für das Verhalten seiner Auftragsbearbeiter wie für eigenes. Der Verantwortliche kann daher beispielsweise die Pflichten für die Durchführung einer Datenschutz-Folgeabschätzung oder die Informationspflichten an den Auftragsbearbeiter übertragen, wenn er dies für notwendig erachtet. Hierbei wird er sich die entsprechenden Kontrollrechte über den Auftragsbearbeiter einräumen lassen, um so eigene Interessen zu schützen. Eine gesetzliche Verpflichtung der Auftragsbearbeiter ist daher nicht nur unnötig und unverhältnismässig und wird in der Praxis zu Doppelspurigkeiten führen. Sie stellt für den Verantwortlichen zudem ein Risiko dar, da er allenfalls in bestimmten Bereich den Auftragsbearbeiter nicht mehr kontrollieren kann, weiterhin aber für dessen Verhalten haftet. **Änderung**: Bisnode ist der Meinung, dass der Begriff des „Inhaber der Datensammlung" beibehalten

					werden sollte. **Alternativ:** Bisnode ist eventualiter der Meinung, dass die Pflichten des Auftragsdatenbearbeiters reduziert werden sollten. Insbesondere vertritt sie die Meinung, dass der Auftragsdatenbearbeiter nicht zur Durchführung einer Datenschutz-Folgeabschätzung verpflichtet werden sollte.
Bisnode	DSG	4	3		Neu soll der Zweck der Datenbeschaffung für die betroffene Person „klar" erkennbar sein. Gemäss der Botschaft des Bundesrates ist hierbei allerdings keine Änderung gegenüber dem bestehenden Recht beabsichtigt. Aus diesem Grund vertritt Bisnode die Meinung, dass die Einfügung des Wortes „klar" in der Praxis zu vermeidbaren Unklarheiten der Anwendung und Auslegung führen wird. **Änderung**: Bisnode ist der Meinung, dass das Wort „klar" gestrichen werden sollte.
Bisnode	DSG	4	4		Der Grundsatz der Verhältnismässigkeit sagt bereits aus, dass Personendaten nur so lange aufbewahrt werden dürfen, wie es der Zweck der Bearbeitung erlaubt. Eine Wiederholung in Art. 4 Abs. 4 VE-DSG ist daher unnötig. **Änderung**: Bisnode ist der Meinung, dass Art. 4 Abs. 4 VE-DSG gestrichen werden sollte.
Bisnode	DSG	4	5		Die aktuell gültige Bestimmung über die Datenrichtigkeit in Art. 5 Abs. 1 DSG ist klarer formuliert. Zudem geht aus dem Erläuterungsbericht hervor, dass keine materiellen Änderungen beabsichtigt sind. Wird nun der Wortlaut des Gesetzes dennoch geändert, so kann dies in der Praxis zu Unsicherheiten in der Anwendung führen. Zudem ist insbesondere der Einschub *„[…] und wenn nötig nachgeführt wurden."* unklar und nicht notwendig. **Änderung**: Bisnode ist der Meinung, dass die geltende Bestimmung in Art. 5 Abs. 1 DSG beibehalten werden sollte. **Alternativ**: Bisnode ist eventualiter der Meinung, dass der Teilsatz *„[…] und wenn nötig nachgeführt wurden."* sowie die Sätze *„Unrichtige und unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten."* gestrichen werden sollten.

Bisnode	DSG	4	6		**Änderung**: Bisnode ist der Meinung, dass das „Profiling“ aus der Bestimmung gestrichen werden sollte.
Bisnode	DSG	5	3	d	**Änderung**: Bisnode ist der Meinung, dass die Genehmigungspflicht gemäss Art. 5 Abs. 3 lit. d VE-DSG gestrichen und dafür die geltende Informationspflicht in Art. 6 Abs. 3 DSG und Art. 6 VDSG beibehalten werden sollte.
Bisnode	DSG	5	4-5		**Änderung**: Bisnode ist der Meinung, dass die Genehmigungspflicht gemäss Art. 5 Abs. 4-5 VE-DSG gestrichen und dafür die geltende Informationspflicht in Art. 6 Abs. 3 DSG und Art. 6 VDSG beibehalten werden sollte. Zudem vertritt Bisnode die Meinung, dass dem Auftragsbearbeiter keine Informationspflicht auferlegt werden sollte (vgl. Ausführungen zu Art. 3 lit. h und i VE-DSG).
Bisnode	DSG	5	6		**Änderung**: Bisnode ist der Meinung, dass dem Auftragsdatenbearbeiter keine Informationspflicht auferlegt werden sollte (vgl. Ausführungen zu Art. 3 lit. h und i VE-DSG).
Bisnode	DSG	6	2		Eine Meldepflicht an den Beauftragten in den Fällen des Art. 6 Abs. 1 lit. b, c und d ist unverhältnismässig und nicht sachgemäss, denn entsprechende Datenbekanntgaben ins Ausland in Ausnahmefällen sind häufig zeitsensibel. Die Meldepflicht würde zudem dazu führen, dass dem Beauftragten Geschäftsgeheimnisse sowie allfällige weitere heile Informationen preisgegeben werden müssten, ohne dass dies aus datenschutzrechtlicher Sicht notwendig wäre. Ausserdem unterliegt der Beauftragte dem Öffentlichkeitsgesetz, sodass die preisgegebenen Informationen über ein Öffentlichkeitsgesuch von Dritten eingesehen werden könnten. Zudem wird die Einführung einer solchen Meldepflicht dazu führen, dass der Beauftragte mit einer sehr grossen Anzahl von Meldungen konfrontiert werden würde, deren Bearbeitung für ihn wohl problematisch sei dürft. **Änderung**: Bisnode ist der Meinung, dass die Meldepflicht in Art. 6 Abs. 2 VE-DSG ersatzlos gestrichen werden sollte. **Alternativ:** Sollte die Meldepflicht übernommen werden, ist Bisnode eventualiter der Meinung, dass der Auftragsbearbeiter nicht unter diese Meldepflicht gestellt werden sollte (vgl. Ausführungen zu Art. 3 lit. h

					und i VE-DSG).
Bisnode	DSG	7	2		Da der Auftragsbearbeiter die Personendaten nur so bearbeiten darf, wie der Verantwortliche es dürfte, präzisieren sich seine Pflichten aus dem ursprünglichen Bearbeitungszweck sowie aus den Anweisungen des Verantwortlichen. Eine Präzisierung in den bundesrätlichen Ausführungsbestimmungen ist daher unverhältnismässig und unnötig. **Änderung**: Bisnode ist der Meinung, dass die Bundeskompetenz, „die weiteren Pflichten des Auftragsbearbeiters“ präzisieren zu können, gestrichen werden sollte.
Bisnode	DSG	7	3		**Änderung**: Bisnode ist der Meinung, dass eine generelle Einwilligung zum Beizug von Subunternehmern ermöglicht werden sollte. Zudem sollte klargestellt werden, dass mit «schriftlich» in diesem Zusammenhang nicht die gesetzliche Schriftform gemäss Art. 13 OR gemeint ist, sondern dass die Einwilligung in einer dokumentierten Form erfolgen muss. Outsourcingverträge sind in der Regel Innominatkontrakte mit Elementen des Auftrags- und / oder Werkvertragsrechts und können als solche formfrei (somit insbesondere ohne Unterschrift) abgeschlossen werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	8			Sollte der Beauftragte die Kompetenz zum Erlass von Empfehlungen der guten Praxis erhalten, so würde er faktisch die Stellung des Gesetzgebers einnehmen. Dies, weil davon auszugehen ist, dass die Empfehlungen in der Praxis und insbesondere auch von den Gerichten bei der Auslegung des DSG herangezogen und daher unmittelbare Wirkung auf die Rechtsanwendung haben werden. Rechtsmittel für die Empfehlungen des Beauftragten sind allerdings keine vorgesehen. Auch der Beizug von „interessierten Kreisen“ würde diesen Einfluss des Beauftragten nicht verringern. Diese interessierten Kreise müssen ausschliesslich angehört werden. Der Beauftragte hat aber nicht die Pflicht, ihre Inputs auch tatsächlich beim Erlass von Empfehlungen zu berücksichtigen. Zudem besteht das Risiko, dass interessierte Kreise ausschliesslich einseitige Interessen vertreten, was für eine ausgewogene Regulierung wiederum nicht förderlich wäre. **Änderung**: Bisnode ist der Meinung, dass Art. 8 VE-DSG ersatzlos gestrichen werden sollte.
Bisnode	DSG	9			Art. 9 Abs. 1 VE-DSG führt die gesetzliche Vermutung ein, dass die datenschutzrechtlichen Bestimmungen

					eingehalten werden, wenn sich der Datenbearbeiter an die Empfehlungen der guten Praxis hält. Die Auswirkungen auf die Beweislast sind unklar. Es ist jedoch davon auszugehen, dass die Regelung in der Praxis zu einer Beweislastumkehr zulasten des Verantwortlichen führen würde. **Änderung**: Bisnode ist der Meinung, dass Art. 9 VE-DSG ersatzlos gestrichen werden sollte.
Bisnode	DSG	12			Das Datenschutzgesetz ist ausgerichtet auf den Schutz der Persönlichkeit ausgerichtet. Die Persönlichkeit einer Person endet jedoch gemäs Art. 31 ZGB mit dem Tod. Will man den Umgang mit Informationen über einen Verstorbenen regeln, ist das DSG nicht das richtige Gesetz. **Änderung**: Bisnode ist der Meinung, dass Art. 12 Abs. 4 VE-DSG ersatzlos gestrichen werden sollte.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	13	1-2		Der Wortlaut von Art. 13 Abs. 1 VE-DSG könnte so ausgelegt werden, dass jede betroffene Person einzeln informiert werden müsste, was in der Praxis zu einem unverhältnismässigen Mehraufwand führen würde. Dieser Mehraufwand würde sich zudem noch zunehmen, da nach der neuen Regelung des VE-DSG die Informationspflicht auf alle Personendaten ausgeweitet werden würde. **Änderung**: Bisnode ist der Meinung, dass die betroffenen Personen auch in allgemeiner Weise, beispielsweise über AGB, informiert werden können müssen. **Alternativ**: Eventualiter ist Bisnode der Meinung, dass analog der aktuellen Regelung von Art. 14 Abs. 3 DSG eine aktive Informationspflicht bei der Beschaffung von besonders schützenswerten Personendaten eingefügt werden sollte.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	13	3		Die Offenlegung der Empfänger und Empfängerinnen würde dazu führen, dass Unternehmen den betroffenen Personen heikle Geschäftsgeheimnisse mitteilen müssten. Die Bestimmung ist grundsätzlich sehr unklar formuliert, da insbesondere die Begriffe „Dritte“ und „Empfänger“ nicht definiert werden. **Änderung**: Bisnode ist der Meinung, dass Art. 13 Abs. 3 VE-DSG ersatzlos gestrichen werden sollte.
Bisnode **Fehler! Verweisquelle konnte nicht**	DSG	13	4		Eine Informationspflicht bei der Auftragsdatenbearbeitung ist absolut unverhältnismässig und daher abzulehnen. **Änderung**: Bisnode ist der Meinung, dass Art. 13 Abs. 4 VE-DSG ersatzlos gestrichen werden sollte.

gefunden werden.					
Bisnode **Fehler! Verweisquelle konnte nicht gefunden werden.**	DSG	13	5		**Änderung**: Bisnode ist der Meinung, dass Art. 13 Abs. 5 VE-DSG ersatzlos gestrichen werden sollte. **Alternativ**: Eventualiter ist Bisnode der Meinung, dass analog der aktuellen Regelung von Art. 14 Abs. 3 DSG eine aktive Informationspflicht bei der Bearbeitung von besonders schützenswerten Personendaten eingefügt werden sollte.
Bisnode	DSG	14	1		**Änderung**: Bisnode ist der Meinung, dass die Informationspflicht zudem entfallen sollte, wenn die datenbearbeitende Stelle an der Datenbearbeitung ein überwiegendes Interesse hat sowie wenn die Datenbearbeitung in den betroffenen Verkehrskreisen als bekannt gilt oder aus den Umständen ersichtlich ist.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	14	2		**Änderung**: Bisnode ist der Meinung, dass der Ausnahmenkatalog so erweitert werden soll, dass die Informationspflicht auch entfällt, wenn keine besonders schützenswerte Personendaten bei Dritten beschafft werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	14	4	a	Die Voraussetzung der Datenbekanntgabe würde zu einer unnötigen Erschwerung der Datenbekanntgabe innerhalb eines Konzerns führen. **Änderung**: Bisnode ist der Meinung, dass der Teilsatz *„[…] und er die Personendaten nicht Dritten bekannt gibt“* gelöscht werden sollte.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	15	1		Die Informationspflicht von Art. 15 Abs. 1 VE-DSG kommt dann zur Anwendung, wenn eine automatisierte Einzelentscheidung rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat. Sie unterscheidet sich damit im Wortlaut von Art. 22 DSGVO bzw. Art. 8 Abs. 1 lit. a E-SEV 108, denn diese zwei Bestimmungen lassen darauf schliessen, dass auch die rechtliche Wirkung auf für die betroffene Person eine gewisse Intensität erreichen muss, um eine Pflicht des Verantwortlichen auszulösen. **Änderung**: Bisnode ist der Meinung, dass das Kriterium der „rechtlichen Wirkung“ insofern ergänzt werden

					sollte, dass die betroffene Person nur dann informiert werden muss, wenn eine gewisse Intensität der Auswirkung vorliegt.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	15	2		Ein Anhörungsrecht der betroffenen Person würde für die datenbearbeitenden Stellen zu einem Mehraufwand führen, der dem Effizienzgewinn durch eine automatisierte Datenbearbeitung zuwiderlaufen würde. Zudem ist nicht klar, ob eine Äusserung der betroffenen Person im Rahmen der Anhörung überhaupt Folgen hätte. **Änderung**: Bisnode ist der Meinung, dass Art. 15 Abs. 2 VE-DSG gestrichen werden sollte. **Alternativ**: Bisnode ist eventualiter der Meinung, dass die Rahmenbedingungen der Anhörung konkretisiert werden sollten (namentlich der Inhalt und auch der Zeitpunkt) und zwar so, dass der Mehraufwand für die datenbearbeitende Stellen möglichst gering gehalten wird.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	15	3		**Änderung**: Bisnode ist der Meinung, dass Art. 15 Abs. 3 VE-DSG gelöscht werde sollte, da hiermit vorwiegend staatliche Organe einseitig entlastet werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	16			Eine Datenschutzfolgenabschätzung würde in der Praxis ausschliesslich zu einem unverhältnismässigen Mehraufwand führen. Bisnode ist der Meinung, dass ein solches Vorgehen weder Persönlichkeitsverletzungen verhindern noch dem Datenschutz in irgendeiner anderen Weise zuträglich sein kann. Die Bearbeitungsfrist von drei Monaten ist zudem zu lang und würde in der Praxis zu unverhältnismässigen Verzögerungen von Projekten führen. **Änderung**: Bisnode ist der Meinung, dass Art. 16 VE-DSG ersatzlos gestrichen werden sollte. **Alternativ**: Bisnode ist eventualiter der Meinung, dass die Pflicht, den Beauftragten über das Ergebnis der Datenschutz-Folgeabschätzung zu informieren sowie das Widerspruchsrecht des Beauftragten gestrichen werden sollten. Zudem muss der Auftragsbearbeiter aus der Bestimmung gestrichen werden (vgl. Ausführungen zu Art. 3 lit. h und i VE-DSG). Auch die Frist von drei Monaten ist zu lang und sollte angemessen gekürzt werden.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	17			Die Meldepflicht in Art. 17 VE-DSG geht über diejenige der DSGVO und E-SEV 108 hinaus, da sie auf jede Datenschutzverletzung Anwendung findet. Diese ausgedehnte Meldepflicht ist nicht verhältnismässig und verletzt zudem den Grundsatz, sich nicht selbst belasten zu müssen. **Änderung**: Bisnode ist der Meinung, dass die Meldepflicht in Art. 17 VE-DSG ersatzlos gestrichen werden sollte.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	18			Die Pflicht in Art. 18 VE-DSG ist eine unnötige Wiederholung des Prinzips der Datensicherheit sowie des Verhältnimässigkeitsgrundsatzes. Diese Doppelspurigkeit und der unklare Wortlaut von Art. 18 VE-DSG werden in der Praxis zu Unsicherheiten führen. **Änderung**: Bisnode ist der Meinung, dass Art. 18 VE-DSG ersatzlos gestrichen werden sollte.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	19		a	Die Dokumentationspflicht in Art. 19 lit. a VE-DSG würde für die datenbearbeitenden Stellen zu einem erheblichen Mehraufwand führen und geht zudem über die Dokumentationspflicht gemäss Art. 30 DSGVO hinaus. Die vorgesehene breite Dokumentationspflicht bringt zudem keinerlei Mehrwert, weshalb sie abzulehnen ist. **Änderung**: Bisnode ist der Meinung, dass die Dokumentationspflicht in Art. 19 lit. a VE-DSG ersatzlos gestrichen werden sollte.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	19		b	Die Informationspflicht in Art. 19 lit. b VE-DSG geht zu weit, da Berichtigungen, Löschungen usw. andauernd stattfinden. Nicht bei einer jeden solchen Änderung der Personendaten macht eine Mitteilung allerdings Sinn und kann zudem dazu führen, dass die Empfänger Personendaten erhalten, für deren Erhalt sie nicht berechtigt sind. Zusammenfassend führt die Informationspflicht von Art. 19 lit. b VE-DSG ausschliesslich zu einem unverhältnismässigen Mehraufwand. **Änderung**: Bisnode ist der Meinung, dass die Dokumentationspflicht in Art. 19 lit. b VE-DSG ersatzlos gestrichen werden sollte.
Fehler! Verweisquelle konnte nicht	DSG	20	2	e	**Änderung**: Bisnode ist der Meinung, dass die Dokumentationspflicht in Art. 20 Abs. 2 lit. e VE-DSG ersatzlos gestrichen werden sollte, da eine automatisierte Einzelentscheidung für die betroffene Person in

gefunden werden.					der Regel aus den Umständen ersichtlich ist.
Bisnode **Fehler! Verweisquelle konnte nicht gefunden werden.**	DSG	20	2	f	Die Pflicht, die Herkunft der Personendaten bekanntzugeben, kann dazu führen, dass Geschäftsgeheimnisse offenbart werden müssen. **Änderung**: Bisnode ist der Meinung, dass Art. 20 Abs. 2 lit. f VE-DSG gestrichen werden sollte. **Alternativ**: Bisnode ist eventualiter der Meinung, dass die Datenherkunft nicht bekanntgegeben werden muss, wenn ein überwiegendes eigenes oder ein Interesse Dritter vorliegt.
Bisnode	DSG	20	3		Die Bestimmung in Art. 20 Abs. 3 VE-DSG würde dazu führen, dass jede Entscheidung, die auf einer Bearbeitung von Personendaten basiert, eine Pflicht zur Benachrichtigung auslöst. Die Informationspflicht wäre nicht mehr auf automatisierte Einzelentscheidungen beschränkt, was im Ergebnis nicht sinnvoll und unbefriedigend ist und zudem über die Bestimmungen der DSGVO hinausgeht. **Änderung**: Bisnode ist der Meinung, dass die Benachrichtigungspflicht in Art. 20 Abs. 3 VE-DSG ersatzlos gestrichen werden sollte. **Alternativ**: Bisnode ist eventualiter der Meinung, dass die Benachrichtigungspflicht auf den Umstand, dass ein Entscheid getroffen wird, beschränkt werden sollte.
Bisnode **Fehler! Verweisquelle konnte nicht gefunden werden.**	DSG	23	2	d	Die breite Begriffsdefinition von Profiling in Art. 3 lit. f VE-DSG in Verbindung mit der Bestimmung in Art. 23 Abs. 2 lit. d VE-DSG würde dazu führen, dass für jede Entscheidung, die auf einer Bearbeitung von Personendaten basiert, eine ausdrückliche Einwilligung eingeholt werden müsste. Dies ist vollkommen unverhältnismässig und in der Praxis nicht umsetzbar. **Änderung**: Bisnode ist der Meinung dass Art. 23 Abs. 2 lit. d VE-DSG ersatzlos gestrichen werden sollte (vgl. Ausführungen zu Art. 3 lit. f VE-DSG).
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	24	2		Art. 24 Abs. 2 VE-DSG spricht davon, dass ein überwiegendes Interesse in den aufgezählten Fällen *möglicherweise* gegeben ist. Hier ist der aktuelle Wortlaut des Art. 13 Abs. 2 DSG vorzuziehen, der anstatt „möglicherweise“ den Begriff „insbesondere“ verwendet. Es ist in der Praxis unbestritten, dass in den aufgezählten Fällen ein überwiegendes Interesse bejaht werden muss, wovon ein Gericht ausschliesslich

					in begründeten Fällen abweichen darf. **Änderung**: Bisnode ist der Meinung, dass der aktuelle Wortlaut des Art. 13 Abs. 2 DSG *„Ein überwiegendes Interesse der bearbeitenden Person fällt insbesondere in Betracht, wenn diese: […]"* belassen werden sollte.
Bisnode	DSG	24	2	a	**Änderung**: Bisnode ist der Meinung, dass das Wort „unmittelbar" gestrichen werden sollte.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	24	2	c	Das Alter und somit die Volljährigkeit einer betroffenen Person kann häufig nicht festgestellt werden, da der datenbearbeitenden Stelle regelmässig die entsprechenden Informationen fehlen. **Änderung**: Bisnode ist der Meinung, dass Art. 24 Abs. 2 lit. c Ziff. 3 VE-DSG ersatzlos gestrichen werden sollte.
Bisnode	DSG	25		a-c	Die Bestimmung ist sehr offen formuliert, da sie sich im Wortlaut nicht auf eine bestimmte Datenbearbeitung bezieht. **Änderung**: Bisnode ist der Meinung, dass Art. 25 lit. a-c VE-DSG folgendermassen geändert werden sollten: *„[…] Die klagende Partei kann insbesondere verlangen, dass* *a. Eine bestimmte Datenbearbeitung verboten wird;* *b. Die Bekanntgabe von bestimmten Personendaten an Dritte untersagt wird;* *c. Bestimmte Personendaten berichtigt, gelöscht oder vernichtet werden."*
Bisnode **Fehler! Verweisquelle konnte nicht gefunden werden.**	DSG	25	2		**Änderung**: Bisnode ist der Meinung, dass das Recht zur Anbringung eines Bestreitungsvermerks gestrichen werden sollte. **Alternativ**: Bisnode ist eventualiter der Meinung, dass der Bestreitungsvermerk ersetzt werden soll mit dem Recht, einen Hinweis anzubringen, dass eine Information auf einer Behauptung der datenbearbeitenden Stelle basiert.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	25	3		**Änderung**: Bisnode ist der Meinung, dass Art. 25 Abs. 3 VE-DSG ersatzlos gestrichen werden sollte, da die Regelung für den Schutz der Persönlichkeit der betroffenen Person keinerlei Mehrwert bringt.
Bisnode	DSG	28	1-2		**Änderung**: Bisnode ist der Meinung, dass Art. 28 Abs. 1 und 2 VE-DSG ersatzlos gestrichen werden sollten. **Alternativ**: Bisnode ist eventualiter der Meinung, dass auch datenbearbeitende Private in den Geltungsbereich des Art. 28 VE-DSG genommen werden sollten.
Bisnode	DSG	37	1		**Änderung**: Bisnode ist der Meinung, dass der Beauftragte durch die Bundesversammlung gewählt werden sollte. Der Bundesrat wiederum soll der Bundesversammlung den Beauftragten zur Wahl vorschlagen können.
Bisnode	DSG	37	4		**Änderung**: Bisnode ist der Meinung, dass das Budget einer Genehmigung durch die Bundesversammlung bedarf.
Bisnode	DSG	38	2		**Änderung**: Bisnode ist der Meinung, dass eine automatische Wiederwahl gestrichen werden sollte.
Bisnode	DSG	39	2		**Änderung**: Bisnode ist der Meinung, dass jede genehmigte Nebenbeschäftigung öffentlich gemacht werden sollte.
Bisnode	DSG	41	4		Eine Überwachungsmöglichkeit des Beauftragten, ohne dass konkrete Anzeichen für eine Gefährdung der Rechte der betroffenen Personen bestehen, ist unverhältnismässig und kann zudem aus Kostensicht nicht vertreten werden. **Änderung**: Bisnode ist der Meinung, dass Art. 41 Abs. 4 gestrichen werden sollte.
Bisnode	DSG	42			Vorsorgliche Massnahmen können durch Gerichte erlassen werden. Wird nun dem Beauftragten dieselbe Kompetenz zugesprochen, ist dies aus rechtsstaatlicher Sicht bedenklich und wird zu

					Rechtsunsicherheiten führen. **Änderung**: Bisnode ist der Meinung, dass Art. 42 VE-DSG gestrichen werden sollte.
Bisnode	DSG	43	1		Die Ausweitung der Kompetenzen des Beauftragten auf den Erlass von Verfügungen ist unverhältnismässig und nicht notwendig. **Änderung**: Bisnode ist der Meinung, dass Art. 43 Abs. 1 VE-DSG gestrichen werden sollte.
Bisnode	DSG	44	3		**Änderung**: Bisnode ist der Meinung, dass Art. 44 Abs. 3 VE-DSG gestrichen werden sollte. Vielmehr hat ein Gericht darüber zu entscheiden, ob eine aufschiebende Wirkung entzogen werden soll.
Bisnode	DSG	45			Eine Anzeigepflicht des Beauftragten ist unverhältnismässig. Vielmehr sollte er das Recht haben, Anzeige zu erstatten. **Änderung**: Bisnode ist der Meinung, dass Art. 45 VE-DSG anstatt eine Anzeigepflicht ein Anzeigerecht beinhalten sollte.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	49		b	**Änderung**: Bisnode ist der Meinung, dass Art. 49 lit. b VE-DSG ersatzlos gestrichen werden sollte. Ausländische Behörden sollen nicht über den Beauftragten Einfluss auf dem Schweizer Territorium gewinnen.
Bisnode	DSG	50 ff.			Die Strafbestimmungen des VE-DSG sind aus den folgenden Gründen abzulehnen: • Strafrechtliche Sanktionierungen sind grundsätzlich nicht nötig. **Änderung**: Bisnode ist der Meinung, dass Verwaltungsbussen gegenüber strafrechtlichen Sanktionen vorzuziehen sind. • Die Sanktionierung von fahrlässigen Verstössen gegen das Datenschutzgesetz ist nicht sachgerecht. Änderung: Bisnode ist der Meinung, dass fahrlässiges Handeln aus den Tatbeständen gestrichen werden sollte. • Die Bussen sind unverhältnismässig hoch gesetzt. **Änderung**: Bisnode ist der Meinung, dass die maximalen Bussen auf eine angemessene Höhe reduziert werden sollten. Bussen können sich im

					Wiederholungsfall erhöhen. • Im Gegensatz zur DSGVO basiert die Höhe der Bussen nicht auf dem Umsatz eines verurteilten Unternehmens bzw. auf dem steuerbaren Einkommen einer verurteilten natürlichen Person. Die kann dazu führen, dass dem Unternehmen bzw. der natürlichen Person Bussen auferlegt werden, welche sie aufgrund fehlender Mittel nicht zahlen kann. **Änderung**: Bisnode ist der Meinung, dass die Höhe der Bussen von den finanziellen Möglichkeiten des verurteilten Unternehmens bzw. der verurteilten natürlichen Person abhängig gemacht werden sollte.
Bisnode	DSG	51	2		**Änderung**: Bisnode ist der Meinung, dass die fahrlässige Begehung nicht strafbar sein und Art. 51 Abs. 2 VE-DSG daher ersatzlos gestrichen werden sollte (vgl. Anmerkungen zu Art. 50 VE-DSG).
Bisnode	DSG	52			Art. 52 VE-DSG sieht eine Verschärfung des aktuell gültigen Art. 35 DSG vor. Eine solche Änderung ist unverhältnismässig, da sie eine grosse Anzahl von Datenbearbeitern zu einem verschärften Berufsgeheimnis führen würde, ohne dass hierfür ein Grund ersichtlich ist. **Änderung**: Bisnode ist der Meinung, dass der bisherige Wortlaut des Art. 35 DSG beibehalten werden sollte.
Bisnode	DSG	54			**Änderung**: Bisnode ist der Meinung, dass die Verfahren auf dem bundesrechtlichen Verwaltungsweg zu führen sind, weshalb Art. 54 VE-DSG ersatzlos gestrichen werden sollte.
Bisnode	DSG	55			Die Ausdehnung der Verfolgungsverjährung auf fünf Jahre ist unverhältnismässig und nicht nachvollziehbar. **Änderung**: Bisnode ist der Meinung, dass die dreijährige Verjährungsfrist gemäss Art. 109 StGB zur Anwendung kommen und Art. 55 VE-DSG daher gestrichen werden sollte.
Bisnode	DSG	56			**Änderung**: Bisnode ist der Meinung, dass die bundesrätlichen Staatsverträge vom Parlament genehmigt werden müssen.
Bisnode	DSG				**Anhang Art. 58, Ziff. 11. Zivilprozessordnung**

					Es bestehen keine sachlichen Gründe für zivilprozessuale Sonderregelungen für datenschutzrechtliche Verfahren. **Änderung**: Bisnode ist der Meinung, dass die angestrebten Änderungen der ZPO gestrichen werden sollten.
Bisnode	DSG				
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.		

Bundespatentgericht
Tribunal fédéral des brevets
Tribunale federale dei brevetti
Tribunal federalda patentas

Erste Gerichtsschreiberin

Postfach, 9023 St. Gallen
Telefon +41 (0)58 465 21 10
susanne.anderhalden@bpatger.ch
Registratur-Nummer: 021

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

St. Gallen, 30. März 2017 / ans

Vernehmlassungsverfahren zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes, zum Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der EU, zum Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die E-Mail vom 22. Dezember 2016 betreffend das obige Vernehmlassungsverfahren und danken Ihnen für die Gelegenheit zur Stellungnahme.

Es wurde uns bereits im Rahmen der Ämterkonsultation vom Juli 2016 die Möglichkeit zur Stellungnahme eingeräumt und die damaligen Anliegen des Bundespatentgerichts wurden in der Folge allesamt berücksichtigt.

Im Auftrag des Präsidenten teilen wir Ihnen daher nach Durchsicht der Unterlagen mit, dass wir auf eine Stellungnahme verzichten.

Freundliche Grüsse

lic. iur. Susanne Anderhalden

Kopie per E-Mail an:

- Bundesgericht
- Bundesstrafgericht
- Bundesverwaltungsgericht

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

DIE PRÄSIDENTENKONFERENZ
CH - 1000 Lausanne 14
Tel. 021 318 91 11
Fax 021 323 37 00
Korrespondenznummer 10.9

An die Vorsteherin des
Eidg. Justiz- und Polizeidepartements
Frau Bundesrätin
Simonetta Sommaruga
Bundeshaus West
3003 Bern

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

Lausanne, 30. März 2017/lza

Vernehmlassungsverfahren zur Totalrevision des Datenschutzgesetzes sowie

- **zum Bundesbeschluss über die Genehmigung des Notenaustausches mit der EU betreffend den Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen**
- **zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten**

Sehr geehrte Frau Bundesrätin

Wir danken Ihnen für die Gelegenheit, uns zur Vorlage über die Totalrevision des Datenschutzgesetzes und damit verbundener Erlasse vernehmen zu lassen. Üblicherweise äussert sich das Bundesgericht nur zu verfahrens- und organisationsrechtlichen Aspekten, die es selbst betreffen, und nicht zu materiellrechtlichen Inhalten einer Vorlage. Wir halten das auch hier so und äussern uns nur im Rahmen der nachfolgenden Bemerkungen.

1. Ausschluss der Anwendbarkeit das Datenschutzgesetzes auf die Bearbeitung von Personendaten durch unabhängige eidgenössische Justizbehörden (Art. 2 Abs. 2 lit. c E-DSG) sowie durch die eidgenössischen Gerichte (Art. 2 Abs. 3 E-DSG)

Die Anwendbarkeit des Datenschutzgesetzes auf gerichtliche Verfahren bildete bereits ein Thema der Ämterkonsultation. Das Bundesgericht nahm dazu den Standpunkt ein, bei der institutionellen Stellung des Bundesgerichts im Verhältnis zum Datenschutzbeauftragten müsse es im Wesentlichen bei der bisherigen Regelung bleiben, das heisst insbesondere, dass das Datenschutzgesetz auf gerichtliche Verfahren keine Anwendung

findet und der Datenschutzbeauftragte keine Kontrollfunktion gegenüber den eidgenössischen Gerichten ausübt und diese selbst die Verantwortung für den Datenschutz in ihrem administrativen Zuständigkeitsbereich übernehmen. Dieser Standpunkt des Bundesgerichts ist in den Entwurf des Datenschutzgesetzes eingeflossen. Artikel 2 Absatz 3 Entwurf des Datenschutzgesetzes nimmt weiterhin Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechung bearbeitet werden, von der Anwendbarkeit des Gesetzes aus und bestimmt weiter, dass die Gerichte für die Bearbeitung der übrigen Daten von der Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten ausgenommen sind. Damit entfallen auch die vom Bundesgericht in der Ämterkonsultation angesprochenen Folgeprobleme wie Meldepflichten und Untersuchungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten im Bereich des Bundesgerichts. Darüber hinaus schliesst Artikel 2 Absatz 2 lit. c Entwurf des Datenschutzgesetzes folgerichtig auch die Bearbeitung von Personendaten im Rahmen der Rechtsprechung durch unabhängige eidgenössische Justizbehörden (wie die ETH-Beschwerdekommission, vgl. Art. 47 Abs. 1 lit. c VwVG i.V.m. Art. 37 Abs. 3 ETH-G) von der Anwendbarkeit des Datenschutzgesetzes, nicht aber im übrigen Zuständigkeitsbereich ausdrücklich von der Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten aus. Die Unterscheidung der Zuständigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten im Administrativbereich bei den eidgenössischen Gerichten (Ausschluss) einerseits von den unabhängigen eidgenössischen Justizbehörden (kein Ausschluss) andererseits erscheint uns inkonsequent. Im Übrigen begrüssen wir die nunmehr vorgeschlagene Gesetzesfassung und halten vollumfänglich an unserem bereits in der Ämterkonsultation geäusserten Standpunkt fest. Insbesondere darf das Datenschutzgesetz auch künftig nicht auf abgeschlossene Gerichtsverfahren anwendbar sein, da es dadurch nachträglich auf dem Weg des Datenschutzes zu Änderungen gerichtlicher Entscheide kommen könnte; dafür sollen weiterhin einzig die entsprechenden prozessualen Rechtsmittel (wie Revision oder Berichtigung usw.) zur Verfügung stehen. Aus Gründen der Gewaltenteilung müssen sodann die eidgenössischen Gerichte auch in Zukunft allein und vollumfänglich für den Datenschutz in ihrem Zuständigkeitsbereich unter Einschluss der Justizverwaltung verantwortlich bleiben.

2. Kostenlosigkeit in zivilrechtlichen Verfahren

Der Entwurf sieht vor, dass für zivilrechtliche Streitigkeiten im Bereich des Datenschutzes keine Sicherstellungen und Gerichtskosten mehr erhoben werden sollen (Anpassung von Art. 99 Abs. 3 lit. d, Art. 113 Abs. 2 lit. g und Art. 114 lit. f ZPO). Wir möchten dazu klarstellen, dass für das Bundesgericht analog zu anderen Fällen der Kostenlosigkeit die Bestimmungen des Bundesgerichtsgesetzes (insbes. Art. 65 f. BGG) weiterhin vorgehen. Für das bundesgerichtliche Verfahren sieht der Entwurf zu Recht weder Kostenlosigkeit noch einen reduzierten Tarif vor. Im Privatrecht sind auch in solchen Fällen mitunter erhebliche finanzielle Interessen im Spiel.

Genehmigen Sie, sehr geehrte Frau Bundesrätin, den Ausdruck unserer ausgezeichneten Hochschätzung.

Freundliche Grüsse

SCHWEIZERISCHES BUNDESGERICHT

Die Präsidentenkonferenz

Der Vorsitzende	Der Generalsekretär
Nicolas von Werdt	Paul Tschümperlin

Kopie (per E-Mail)
- Bundesstrafgericht
- Bundesverwaltungsgericht
- Bundespatentgericht

Bundesverwaltungsgericht
Tribunal administratif fédéral
Tribunale amministrativo federale
Tribunal administrativ federal

Der Präsident / Die Präsidentenkonferenz

Postfach, 9023 St. Gallen
Telefon +41 58 70 52626
Registratur-Nummer: 024.1

A-Post

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Frau Bundesrätin S. Sommaruga
Bundeshaus West
3003 Bern

PDF- und Word-Version per E-Mail an:

Jonas.amstutz@bj.admin.ch

St. Gallen, 31. März 2017 / bro

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 Frau Bundesrätin

Für Ihre Einladung vom 21. Dezember 2016 zur Stellungnahme im oben erwähnten Vernehmlassungsverfahren danken wir Ihnen bestens. Wir haben den Entwurf mit Interesse zur Kenntnis genommen und begrüssen die vorgesehene Regelung für die eidgenössischen Gerichte und deren Aufsicht. Zudem erlauben wir uns, einige Hinweise auf dem entsprechenden Formular einzureichen.

Im Übrigen verzichtet das Bundesverwaltungsgericht in dieser Angelegenheit auf eine Stellungnahme. Wir bitten Sie, bei der Auswertung der Vernehmlassung die Antwort des Bundesverwaltungsgerichts als Enthaltung und nicht als Zustimmung auszuweisen.

Mit vorzüglicher Hochachtung

Der Präsident des
Bundesverwaltungsgerichts

Jean-Luc Baechler

Der Vorsitzende der
Präsidentenkonferenz

Vito Valenti

Beilage:

- Formular für die Stellungnahme (nur per E-mail)

Kopie an:

- Bundesgericht
- Bundesstrafgericht
- Bundespatentgericht

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 : Bundesverwaltungsgericht

Abkürzung der Firma / Organisation : BVGer

Adresse : Kreuzackerstrasse 12

Kontaktperson : Barraud Jérôme

Telefon : 058 465 28 69

E-Mail : jerome.barraud@bvger.admin.ch

Datum :

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 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 3

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 4

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten 4

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") 5

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" 5

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.	
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	VGG	35		b	Aufheben, da obsolet. Der EDÖB kann jetzt verfügen und muss/kann bei Ablehnung seiner Empfehlung nicht mehr Klage beim BVGer erheben.

gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.	BGÖ	9	2		Diese Bestimmung verweist bezüglich Schutz von Personendaten auf Art. 19 des bisherigen DSG. Im revidierten DSG ist die entsprechende Bestimmung in Art. 29 zu finden, der Verweis sollte daher angepasst werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	BGA	11	1		Diese Bestimmung verwendet den Begriff „Persönlichkeitsprofil“, der im neuen DSG nicht mehr verwendet wird. Allenfalls ist die Bestimmung anzupassen.
Fehler! Verweisquelle konnte nicht gefunden werden.	BGA	15	1		Diese Bestimmung verweist auf das DSG vom 19. Juni 1992. Der Verweis sollte auf das neue DSG lauten.
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: Raphael.Raetzo@billag.com
Gesendet: Mittwoch, 5. April 2017 12:34
An: _BAG-DM; Amstutz Jonas BJ
Betreff: Stellungsnahme Vernehmlassung DSG
Anlagen: Revision DSG_Stellungsnahme CallNet.ch.doc

Sehr geehrte Damen und Herren

Gerne möchten wir vom Branchenverband CallNet.ch (Verband der schweizerischen Contact Center für Kundendialogmanagement) unsere Stellungsnahme überreichen. Leider wurde diese infolge eines Missverständnisses im Sekretariat gestern nicht geschickt, ich hoffe dass Sie unsere Stellungsnahme trotz der kleinen Verspätung trotzdem annehmen.

Herzlichen Dank und freundliche Grüsse
Raphael Raetzo
CallNet.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 : CallNet.ch

Abkürzung der Firma / Organisation : Schweizerischer Branchenverband für Kundendialog Management

Adresse : Pfadacher 5, Postfach, 8623 Wetzikon

Kontaktperson : Raphael Raetzo

Telefon : 079 708 29 20

E-Mail : raphael.raetzo@callnet.ch

Datum : 4.4.17

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 _____ 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) _____ 4

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. CallNet.ch	CallNet.ch ist der Verband der schweizerischen Contact Center. Die Mitglieder setzen sich zusammen aus Firmen mit Kundenkontaktcentern (Versicherungen, Banken, Telekomunternehmungen), externen Dienstleistern für Kundenkontakt sowie Suppliern aus diesem Bereich. Der Verband begrüsst grundsätzlich die Modernisierung des Datenschutzgesetzes und die damit einhergehende Annäherung an die Rechtslage der EU. In der jetzigen Form jedoch müssen wir den vorliegenden Entwurf ablehnen bzw. bitten um eine Überarbeitung. Dies ausfolgenden Gründen: • Sanktionssystem: Dieses sieht eine Kriminalisierung von natürlichen Personen vor anstelle einer Disziplinierung der Unternehmung. Dies ist vor allem für schweizerische KMU's problematisch – bei Grosskonzernen mit internationalem Sitz ist Verfolgung praktisch unmöglich. • Vergleich EU: Das Datenschutzgesetz soll nicht über die Bestimmungen der EU hinausgehen. Das benachteiligt den Standort Schweiz, insbesondere bei Berücksichtigung, dass Datenbearbeitungen heute und vermehrt zukünftig nicht an der Schweizer Grenze haltmacht. • Dokumentationspflichten: Die vorgesehenen Massnahmen führen zu hohen administrativen Dokumentationspflichten ohne Mehrwert. Grundsätzlich soll das DSG die Betroffenen schützen und gleichzeitig kein Standortnachteil Schweiz ergeben. Aus unserer Sicht geht der vorgeschlagene Entwurf in vielen Punkten deutlich zu weit, schränkt die in der Schweiz ansässigen Firmen ein in dem es weit über europäische Regelungen hinausgeht. Dies lehnen wir ab.

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. CallNet.ch	DSG	3		a	Es ist zu begrüssen dass der Begriff Personendaten beibehalten wird.Im erläuternden Bericht ist die Regelung jedoch unklar und teilweise widersprüchlich. Insbesondere bei Online-Aktivitäten (Einsatz von Cookies) zur Auslierferung von individualisierter Werbung auf Webseiten besteht kein Interesse an der Identifikation des Nutzers, sondern lediglich an der Kategorisierung. Es besteht keine Notwendigkeit über die Gesetzeslage der EU hinauszugehen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	3		f	Die vorgeschlagene Definiton des Profilings lehnen wir ab. Die Definition geht ohne Not weit über diejenige der EU hinaus.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	3		c	Der Begriff biometrische Daten soll präzisiert werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	7			Es ist zu begrüssen, dass die Rechtslage hinsichtlich der Auftragsdatenbearbeitung grundsätzlich gleichbleibt. Ablehnend stehen wir der Ausdehnung der Vergewisserungspflicht gegenüber. Diese ist unklar und kann zu einem wirtschaftlich schädigenden Mehraufwand für Outsourcing bedeuten. Auch auf die unbeschränkte Delegation an den Bundesrat zur Festlegung weiterer Pflichten ist soll verzichtet werden.
Fehler! Verweisquelle konnte nicht	DSG	8			Die Einführung von Empfehlungen der guten Praxis begrüssen wir. Jedoch kann das Genehmigungsverfahren nicht dem EDÖB alleine unterliegen. Es soll definiert werden, wer zu den

gefunden werden.					interessierten Kreisen gehört.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	8	1		Die dem EDÖB zugesprochene Kompetenz eigenständige Empfehlungen zu erlassen ist problematisch und deshalb zu streichen. Es muss sichergestellt werden, dass branchenübliche Bedürfnisse berücksichtigt werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	8	2		Es muss rechtlich sichergestellt werden, dass Empfehlungen von den betroffenen Unternehmen bzw. Verbänden bei Ablehnung gerichtlich anzufechten sind.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	13			Diverse Punkte gehen in der vorgeschlagenen Regelung deutlich zu weit. Nachfolgend werden einige Punkte aufgenommen welche wir ablehnen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	13	2		Es soll klar und abschliessend definiert werden welche die mitzuteilenden Informationen sind. Dies auch im Sinne des betroffenen Konsumenten.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	13	4		Diese Vorgabe geht klar über die europäische Regelung hinaus und ist deshalb ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden	DSG	13	5		Mit der Ausdehnung der Pflicht auf die indirekte Datenbeschaffung wird in der Praxis jegliche Beschaffung von Daten bei Drittanbietern verunmöglichen. Deshalb ist die Bestimmung ersatzlos zu streichen. Die Regelung geht über die europäischen Vorgaben hinaus.

werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	14			Die enge Fassung der Ausnahmen geht über E-SEV 108 hinaus. Der Zusatz "und er die Personendaten nicht Dritten bekannt gibt" ist zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	16			Auch hier geht der Entwurf unverständlicherweise über die europäischen Vorgaben hinaus. Der Begriff "erhöhte Risiken" führt zu einem unverständlich weit gefassten Anwendungsbereich. Der Begriff soll zu "sehr hohem Risiko" umbenennt werden. Die Bezugnahme auf die Risiken der Grundrechte von Betroffenen ist unpassend und zu streichen. Durch die vorgeschlagene Lösung würde ein nicht zu bewältigender Aufwand entstehen. Auch die Frist von drei Monaten zur Beurteilung durch den EDÖB ist zu lange und muss massiv verkürzt werden, um durch die Frist nicht die Unternehmung/Wirtschaft zu lähmen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	17			Auch hier geht die vorgeschlagene Regelung weit über die europäischen Regelungen hinaus. Die Regelung geht viel zu weit und schützt den Betroffenen nicht zusätzlich. Es soll auf schwerwiegende Rechteverletzungen, die zu einem Bruch oder Verlust des Gewahrsams an Daten führen, beschränkt werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	19			Die Auftragsdatenbearbeiter sind in Bezug auf die vorgesehene Informationspflicht aus der Pflicht zu nehmen. Der Entwurf geht auch hier unverständlich über die EU-DSGVO hinaus.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	19		a	Damit ein solches Verzeichnis seinen Zweck erfüllen kann muss es auf regelmässige Datenbearbeitungen beschränkt werden. Ansonsten müsste jegliche Korrespondenz erfasst werden. Die Regelung darf deshalb nicht über das in der EU-DSGVO vorgeschriebene Verzeichnis hinausgehen sowie sind Ausnahmen wie in der EU-DSGVO vorzusehen.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	19		b	Diese Mitteilungspflicht ist im E-SEV 108 nicht vorgesehen und deshalb ersatzlos zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	20	1		Die Kostenlosigkeit des Auskunftsrechts ist im E-SEV 108 nicht ersichtlich und ist deshalb zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	20	3		Hinsichtlich von Entscheidungen aufgrund einer automatisierten Datenbearbeitung ist das Auskunftsrecht deutlich zu weit gefasst, wenn nicht sogar uferlos. Die Regelung schiesst über das Ziel hinaus und ist deshalb einzuschränken.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	23			Wird diese Vorschrift Gesetz wird praktisch jede Form von personalisierter Werbung für in der Schweiz ansässige Firmen verunmöglicht und ist deshalb eine Bedrohung für den Wirtschaftsstandort Schweiz. Deshalb ist die generelle Erfordernis der ausdrücklichen Einwilligung für das Profiling zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	50ff			Das Sanktionssystem welches primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen wird von uns strikt abgelehnt. Es hemmt Innovationen und steht der digitalen Strategie der Schweiz entgegen. Eine Kultur des Denunziantentums wird sich etablieren. Es führt zu einer gewichtigen Benachteiligung des Standorts Schweiz, da Rechtsmittel gegenüber ausländischen Firmen praktisch nicht durchsetzbar sind. Die Schweiz würde hier einen Sonderweg einschlagen. Die Sanktionierung von natürlichen Personen ist nicht zielführend und unverhältnismässig. Die Schärfe des Sanktionssystems ist absurd. Anstelle von strafrechtlichen Sanktionen empfehlen wir die Einführung von verwaltungsrechtlichen Bussen. Weiter soll der Strafkatalog nicht über europäische Regelung hinausgehen.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	52			Der Ausbau der geltenden Regeln lehnen wir ab da keine Notwendigkeit besteht.

Amstutz Jonas BJ

Von: Pascal KOTTE (CloudReady) <pascal.kotte@cloudready.ch>
Gesendet: Dienstag, 4. April 2017 11:33
An: Amstutz Jonas BJ
Betreff: consultation avant-projet LPD
Anlagen: 2017-04-04, CloudReady, Lettre pour consultation publique sur la révision de la LPD.pdf

Bonjour,
veuillez avoir l'amabilité de me confirmer la bonne réception de notre courrier joint.
Avec nos plus cordiales salutations.
Pascal

Pascal KOTTÉ *Conseiller numérique, éthicien digital* +41 79 309 28 86 MeetMe: meet.cloudready.ch Pascal.KOTTE@cloudReady.ch Président de **CloudReady.ch** association art.60 CH *Observatoire et Projets durables pour le Cloud*	LesEnfantsDu.Net De "digital naïf" à "digital natif" ? INTERGEN.digital Les juniors au secours des seniors !	Formation/Veille **CloudReady.ch**

CloudReady.ch
Observatoire Suisse Romand du Cloud Computing

Courrier public

La Culture Numérique, c'est une nécessité pour tous !

Date: 04/04/2017
REF LPD2017

Sujet Avant-projet LPD

À jonas.amstutz@bj.admin.ch
Département Fédéral de
Justice et Police
3003 BERN

Madame la Conseillère fédérale,
Madame, Monsieur,

L'association Suisse romande pour des transitions numériques responsables, comprend une soixantaine de conseillers numériques expérimentés, dont les membres de l'association ICT-a.ch, déontologiquement engagée dans le conseil indépendant et la défense des intérêts des PME/PMI suisses romandes. Nous vous livrons ici quelques conclusions de réflexions informelles échangées entre nous, mais que nous ne pouvons laisser sous silence.

Le contenu de la dernière LRENS a déjà fait beaucoup de dégât quand à la réputation de la Suisse en termes de protection et de respect des données. Mais ce n'est pas le sujet pour cette révision de la LPD. Nous ne disposons pas des juristes nécessaires pour vous proposer des modifications éclairées, mais nous pouvons vous partager nos inquiétudes concernant l'évolution de la LPD.

Nous ne voyons pas d'un bon œil l'abandon total de la protection des personnes morales. Le fait de conserver un certain protectionisme des entreprises et organisations morales, permet de maintenir la Suisse en position d'acceuil International priviliégié pour un grand nombre d'organisations, que ce soit par des ONG ou bien des entreprises privées, de multiples nations qui aiment la discrétion et le respect de leurs affaires. Bien entendu, cela ne doit pas servir à couvrir des activités douteuses, voir répréhensibles et nous sommes des fervents défenseurs des principes de transparence, d'Opendata ; mais dans le respect du droit à la vie privée des personnes morales, comme des personnes physiques.

Il est tout à fait possible de mettre en place une LPD qui conserve un caractère plus protecteur que nos voisins, même de peu, et d'autoriser les exports de données vers des pays légèrement inférieurs en termes de protection, puis en instituant des nuances : C'est-à-dire des directives de contrats types complémentaires, par groupes de pays selon leurs manques en termes de protections.

Cela positionnerait ainsi un focus fort sur la Suisse comme régulateur d'une déontologie numérique de référence, et observateur neutre des pratiques internationales à ce sujet, sans être moralisateur.

En vous remerciant de votre attention, veuillez agréer, Madame la Conseillère fédérale, Madame, Monsieur, nos salutations distinguées.

Pascal Kotté
+41 79 309 28 86, Pascal.KOTTE@CloudReady.ch
Président de CloudReady.ch, administrateur de LIN (Léman Innovation Numérique)
Porteur du projet http://Responsibility.digital
(membre du comité SISR.ch et Social-IN3.coop)

Amstutz Jonas BJ

Von: Isabelle Dubois <id@adhocresolution.ch>
Gesendet: Freitag, 31. März 2017 10:39
An: Amstutz Jonas BJ
Cc: enrico.vigano@clusis.ch
Betreff: avis conslutatif LPD du CLUSIS
Anlagen: Revision-totale-de-la-loi-sur-la-protection-des-donnees_Formulaire-pour-prise-de-position_fr.doc

Monsieur,
Au nom de l'association suisse de la sécurité de l'information, je vous transmets son avis sur l'avant-projet de loi LPD.
Je vous en souhaite bonne réception,
Bonne journée

Avec mes meilleurs messages,

Isabelle Dubois
Expert en protection des données

+41 22 552 05 60
+41 79 519 04 25

AD HOC RESOLUTION
Rue du Simplon 50
1800 Vevey

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 : Association suisse de la sécurité de l'information

Abréviation de la société / de l'organisation : CLUSIS

Adresse : c/O Fiduciaire Roubaty, Passage du Pécos 5, 1005 Lausanne

Personne de référence : Enrico Vigano, Président

Téléphone : 079.217.07.07

Courriel : enrico.vigano@clusis.ch

Date : 1er 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

Remarques générales 3

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 4

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 6

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel 6

Rapport explicatif (excepté chap. 8 « Commentaire des dispositions») 7

Rapport explicatif : chap. 8 « Commentaire des dispositions » 7

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.CLUSIS	Le CLUSIS approuve de manière générale les modifications prévues de la LPD, et de la Convention STE 108
Fehler! Verweisquelle konnte nicht gefunden werden.	Ces modifications sont indispensables pour que la Suisse conserve, en sa qualité de pays tiers de l'Union européenne, son niveau adéquat de législation reconnu aujourd'hui par décision de la Commission européenne
Fehler! Verweisquelle konnte nicht gefunden werden.	Les nouvelles dispositions de la LPD qui harmonisent certaines définitions, notions et concepts avec l'UE sont saluées, de même que le renforcement du rôle et des compétences du PFPDT
Fehler! Verweisquelle konnte	A ce propos devrait être ajoutée une compétence d'amende administrative, d'une part pour rejoindre les compétences des autorités européennes, d'autre part pour créer deux niveaux de sanctions.

nicht gefunden werden.	
Fehler! Verweisquelle konnte nicht gefunden werden.	L'exigence de Privacy by design and by default est saluée.
Fehler! Verweisquelle konnte nicht gefunden werden.	L'introduction d'une obligation d'évaluation de l'impact lorsqu'un traitement est susceptible d'enfreindre les droits de la personnalité est saluée. Un ajout relatif au recours à de nouvelles technologies, par analogie au texte européen serait bienvenu (voir ci-dessous)
Fehler! Verweisquelle konnte nicht gefunden werden.	**Le CLUSIS déplore et s'inquiète de la disparition pure et simple de la fonction de conseiller en protection des données personnelles en entreprise, qui doit au contraire être renforcée, et surtout ancrée dans la loi, à titre obligatoire lorsque des traitements de grandes ampleurs et volumes ont lieu ou que des données sensibles sont traitées, ainsi que pour les institutions publiques, et à titre facultatif dans les autres cas. Le CLUSIS juge que l'absence de cette fonction risque de conduire purement et simplement à l'impossibilité pour les organismes concernés de se mettre en conformité, et de garantir aux personnes concernées un traitement conforme.** **Pour les règles relatives à la fonction de DPO, et aux conditions d'exercices de celle-ci, le CLUSIS souhaite que les règles existante dans le règlement européen soit purement et simplement reprises.** **Cette fonction est d'autant plus importante que de nouvelles obligations apparaissent auxquelles les organismes auront de la peine à faire face sans une aide expérimentée et bienveillante mais neutre et indépendante, et que en revanche l'obligation de déclarer les fichiers disparaît, ce qui est cohérent si une personne de référence tient le registre des traitements. En outre le droit absolu d'accès à ses données personnelles ne sera pas mis en oeuvre de manière efficiente sans un tel relai.**

Fehler! Verweisquelle konnte nicht gefunden werden.	Le CLUSIS regrette l'absence d'une disposition sur la portabilité des données liées directement au droit d'accès à ses données personnelles, puisque celles-ci doivent pouvoir être reçues par la personne concernée dans un format structuré, clair et lisible.
Fehler! Verweisquelle konnte nicht gefunden werden.	Le CLUSIS regrette de la même manière l'absence d'une disposition prévoyant l'exercice collectif des droits, en cas de violation. Aujourd'hui l'exercice concret de ses droits est laborieux et long. Il apparaît que si un groupe d'individus concernés par une violation de leurs droits de la personnalité par le biais d'un traitement non conforme de leurs données personnelles pouvaient agir de concert, les entreprises seraient davantage motivées à se conformer aux règles.
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.	LPD	2			La renonciation à l'applicabilité aux personnes morales est de nature à uniformiser le droit avec le droit européen sans nuire aux entreprises qui peuvent faire valoir leur droit par d'autres lois.
Fehler! Verweisquelle konnte nicht gefunden werden.		3		c	Les ajouts données biométriques et données génétiques sont à conserver
Fehler! Verweisquelle konnte nicht gefunden werden.		7	2		Cette exigence relative aux sous-traitants est indispensable pour garantir un traitement conforme
Fehler! Verweisquelle konnte nicht gefunden werden.		12			Ajout bienvenu s'agissant des droits d'une personne décédée en lien notamment avec les réseaux sociaux

Fehler! Verweisquelle konnte nicht gefunden werden.		15			Ajout bienvenu car les décisions automatisées sont fréquentes et pour l'instant prises à l'insu de la personne concernée
Fehler! Verweisquelle konnte nicht gefunden werden.		16	1		Ajouter „par exemple par l'utilisation de nouvelles technologies"
Fehler! Verweisquelle konnte nicht gefunden werden.		17			Ajout bienvenu
Fehler! Verweisquelle konnte nicht gefunden werden.		25			Ajouter un article 25a:exercice collectif du droit
Fehler! Verweisquelle konnte nicht gefunden werden.		43			Ajouter la possibilité pour le PFPDT de notifier des amendes administratives en cas de traitement non conforme

Fehler! Verweisquelle konnte nicht gefunden werden.					**Ajouter une section Délégué à la protection des données, prévoyant l'obligation d'une telle fonction pour les institutions publiques et les entreprises qui traitent beaucoup de données personnelles ou des données sensibles, et facultatives dans les autres cas, mais encouragée. Sur la base des règles européenne en la matière : indépendance, neutralité, missions d'accompagnement à la conformité, de sensibilisation interne et de rapport annuel à la gouvernance, exercice centralisé du droit d'accès et tenue des registres de fichiers**
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

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

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

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

Eidgenössisches Justiz- und
Polizeidepartement EJPD
CH-3003 Bern

7. April 2017

Referenz: Thomas Mahrer

Vernehmlassung zum neuen Datenschutzrecht: Stellungnahme Coop

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit der Stellungnahme zum Datenschutzrecht. Die Coop-Gruppe, ihre Divisionen und ihre Tochtergesellschaften sind auf vielfältige Weise mit der Thematik des Datenschutzes konfrontiert.

Der Werkplatz Schweiz hat sich in den vergangenen Jahrzehnten auch dank eines hohen Digitalisierungsgrads unserer Wirtschaft erfolgreich positionieren können. Alle sind sich einig, dass wir heute erst am Anfang einer noch viel weitergehenden Entwicklung stehen: Es steht uns ein fundamentaler Wandel der künftigen (Welt-)Wirtschaft bevor. Dabei sind die Daten und die Datenbewirtschaftung der wertvollste Rohstoff. Wenn nun in der Schweiz mit einer restriktiven Regulierung des Datenhandlings neue Geschäftsmodelle verhindert werden, so gelangt der Werkplatz Schweiz schnell ins Hintertreffen. Die digitale Wirtschaft findet global statt und spielt sich dort ab, wo auch ein optimaler Regulierungsrahmen besteht. So zeigen z.B. Google, Apple, Cisco, Alibaba auf, wohin es in Zukunft geht: Die Wirtschaft wird immer enger verknüpft mit einem tiefgreifenden Einsatz der Informations- und Kommunikationstechnik. Von dieser Entwicklung profitieren diejenigen Wirtschaftsstandorte, welche massvolle, aber zurückhaltende Regulierungen i.S. Datenschutz haben.

Das neue DSG ist daher ganz grundsätzlich zu überarbeiten und zu entschlacken. Alleine die europäischen verbindlichen Vorschriften i.S. Datenschutz gehen eigentlich schon zu weit, wenn man den weltweiten Markt der digitalen Wirtschaft betrachtet. Dass darüber hinaus noch zusätzliche schweizerische Regulierungen vorgeschlagen werden, geht eindeutig zu weit. Coop lehnt daher dezidiert sämtliche Regulierungen ab, welche über die EU-Regulierungen hinausgehen. Diese vorgeschlagene Swiss Finish-Gesetzgebung gefährdet die Wettbewerbsfähigkeit des digitalen Wirtschaftsstandorts Schweiz.

Zur Vernehmlassung zum neuen Datenschutzrecht äussert sich Coop zusammenfassend wie folgt:

Coop Genossenschaft
Wirtschaftspolitik
Hauptsitz

Thiersteinerallee 14
Postfach 2550
4002 Basel
Schweiz

Tel. +41 61 336 72 52
Mobile +41 79 255 51 35
Fax +41 61 335 80 31
CHE-116.311.185 MWST

wirtschaftspolitik@coop.ch
www.coop.ch

JA zur Übernahme der Richtlinie (EU) 2016/680 im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen
Die Übernahme ist im Rahmen des Schengen-Abkommens verpflichtend und steht deshalb für Coop ausser Frage.

JA zur Ratifizierung des revidierten Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108)
Die Ratifizierung ist massgebend für den Angemessenheitsentscheid der EU-Kommission zum Datenschutzniveau in der Schweiz. Aus der Sicht von Coop ist sie ebenfalls unbestritten.

Totalrevision des Datenschutzgesetzes
Die EU-Kompatibilität des neuen DSG ist im Rahmen der Totalrevision zu gewährleisten. Darüber hinausgehende Regelungen (Swiss Finish) sind strikte zu vermeiden. Die künftig möglichen Datenbewirtschaftungsformen sind eine Chance für den schweizerischen Werkplatz. Das angedachte DSG verunmöglicht jedoch einen liberalen und gleichzeitig sicheren Umgang mit Daten. Dies gefährdet die Wettbewerbsfähigkeit der Schweiz im Bereich digitale Wirtschaft.

Allgemeine Forderungen zur Totalrevision DSG

Zur Totalrevision des DSG finden Sie im Folgenden unsere allgemeinen Forderungen sowie im beiliegenden Formular die konkreten Anträge für den Gesetzestext.

1. Änderungen auf das beschränken, was im internationalen Kontext zwingend nötig ist

- Das EU-Recht muss für das neue Schweizer DSG massgebend sein. Viele Schweizer Unternehmen sind heute in irgendeiner Weise international tätig oder bearbeiten zumindest Daten in einem internationalen Kontext. Somit ist die europäische Datenschutzgrundverordnung (DSG-VO) für viele Unternehmen ohnehin operativ relevant. Die Schweizer Gesetzgebung muss deshalb grundsätzlich gleichwertig ausgestaltet werden.
- Dabei gilt es auch den von der DSGVO gegebenen Handlungsspielraum auszunutzen und dort liberalere Regeln vorzusehen, wo dies im Schweizer Kontext sinnvoll und der Sache dienlich ist. Dies ist insbesondere bei den aufsichtsrechtlichen Bestimmungen (Kompetenzen des Beauftragten) nicht der Fall.

2. Interpretationsspielraum in der Folgeregulierung klären

- Die hohe Ambivalenz des Gesetzestextes verunsichert. Zum jetzigen Zeitpunkt ist es insgesamt sehr schwierig, die betrieblichen Auswirkungen der Vernehmlassungsvorlage detailliert abzuschätzen, da das vorliegende Gesetz dem Verordnungsgeber und dem Beauftragten zu viel Spielraum einräumt.
- Die risikobasierte, prinzipienorientierte Ausgestaltung des neuen DSG wird seitens Coop begrüsst. Es gilt jedoch im Botschaftstext, im parlamentarischen Prozess, bei der Ausarbeitung der Verordnungen und in zukünftigen Empfehlungen der guten Praxis des Beauftragten auf eine klare Linie zu achten. Der vorliegende Gesetzesentwurf grenzt insbesondere noch zu unklar das Pflichtenheft von "Verantwortlichem" und "Auftragsbearbeiter" ab.
- Die Rechtssicherheit für die betroffenen Unternehmen muss letztlich gewährleistet sein. Die Folgeregulierungen dürfen für die betroffenen Unternehmen nicht plötzlich unverhältnismässige Investitions- und Betriebskosten nach sich ziehen. Gegebenenfalls sind zu einzelnen Massnahmen auch vertiefende Regulierungsfolgeabschätzungen erforderlich.

3. Bedarfsgerechte, konsumentenfreundliche Auskunfts- und Informationspflichten

- Coop befürwortet es, dass die Transparenz und Rückverfolgbarkeit einzelner Bearbeitungsvorgänge für die Konsumentinnen und Konsumenten verbessert wird. Aus Sicht von Coop wird dieses Ziel jedoch verfehlt, wenn ihnen öfters und immer mehr Informationen zu einzelnen Datenbearbeitungsvorgängen zur Verfügung gestellt werden. Es ist sogar davon auszugehen, dass dies

zu einer Überforderung und Desensibilisierung der betroffenen Personen führt. Mit dem neuen DSG würden die Menge und die Komplexität der zu prüfenden Informationen nochmals massiv zunehmen. Im Verhältnis zum erwarteten Nutzen stellt dies einen unverhältnismässigen administrativen Mehraufwand dar.

- Stattdessen hat das neue DSG auf eine verbesserte allgemeine und prinzipielle Information abzuzielen, so dass sich eine betroffene Person vorab der Konsequenzen einer Datenpreisgabe bewusst wird. Die vorgesehenen Informations- und Auskunftspflichten sind entsprechend sinnvoll einzugrenzen. Der Katalog der mitzuteilenden Informationen muss sich dabei zwingend eins zu eins an den Anforderungen in der EU orientieren.

4. Wirtschaftsfreundliche und pragmatische Mitwirkungspflichten

- Coop fordert, dass der Umfang einer Datenschutzfolgeabschätzung auf ein sinnvolles, sachgerechtes Mass beschränkt wird (z.B. als vorgelagertes Datenbearbeitungsreglement). Was für die Pflichten der Unternehmen gegenüber den Konsumentinnen und Konsumenten gilt, muss auch für den Beauftragten gelten: Weniger ist mehr. Ausserdem gilt es, kurze, wirtschaftsfreundliche Ordnungsfristen für die Bearbeitung durch den Beauftragten im Rahmen der Folgeregulierung festzusetzen.
- Die vorgesehene unverzügliche Meldepflicht im Falle sämtlicher Datenschutzverstösse an den Beauftragten ist sodann stark einzuschränken. Sie erfasst weit mehr Fälle als die DSGVO. Die Pflicht ist daher auf Verstösse mit gravierenden Folgen zu beschränken. Im Sinne einer modernen Compliance-Gesetzgebung muss die Meldung beim Beauftragten den Schutz vor Sanktionen zur Folge haben.
- Der Beauftragte seinerseits soll seine neuen Aufgaben und Kompetenzen unter den gleichen personellen und finanziellen Voraussetzungen wie bis anhin erfüllen. Zusätzliche Mittel führen aus der Sicht von Coop tendenziell dazu, dass die Behörde zur eigenen Legitimation in Aktionismus verfällt.

5. Freiwillige branchenspezifische Regeln vorsehen

- Die kommerzielle Auswirkung der Datenbearbeitung, der Aufwand der Information und des Einholens einer Einwilligung sind je nach Branche sehr unterschiedlich. Coop begrüsst es daher, dass mittels Empfehlungen der guten Praxis eine verstärkte Selbstregulierung stattfinden soll. So gilt es sicher zu stellen, dass das neue DSG nicht zu einer "one size fits all"-Lösung wird.
- Z.B. sind Kundenbindungsprogramme wie die Supercard oder andere im Detailhandel übliche Modelle derzeit noch vorwiegend "offline". Eine Änderung der Datenschutzbestimmungen (in den AGB) und das folglich notwendige Einholen des Einverständnisses der betroffenen Personen sind mit einem sehr grossen Aufwand verbunden (u.a. Medienmitteilung, Postversand, E-Mail-Versand). Demgegenüber kann etwa ein Social-Media-Anbieter Änderungen an den AGB und das Einholen des Einverständnisses sehr viel schneller, einfacher und kostengünstiger durchführen.
- Soll der Ansatz der Selbstregulierung konsequent umgesetzt werden, müssen die Empfehlungen der guten Praxis als freiwillige Branchenvereinbarungen ausgestaltet werden. Die Ausarbeitung der Branchenstandards muss von den betroffenen Unternehmen und Branchen selbst erarbeitet werden. Dem Beauftragten soll dabei ein Mitwirkungsrecht eingeräumt werden. Dieser praxisgerechte, effiziente Lösungsansatz hat sich verschiedenerorts bereits sehr bewährt (Swiss Pledge (Werbeverhalten gegenüber Kindern); Plastiksackverbot usw.).

6. Geschäftsgeheimnisse schützen

- Die Vernehmlassungsvorlage schützt Geschäftsgeheimnisse nicht ausreichend. Zwar sind Bestimmungen vorgesehen, die das Aufschieben, Einschränken oder den Verzicht der Information oder Auskunft zulassen, wenn "eigene überwiegende Interessen" vorliegen. Der erläuternde Bericht zur Vorlage lässt darauf schliessen, dass dem Bund hier eine Handhabung vorschwebt, die in der Praxis nicht umsetzbar wäre, ohne dass sensitive Informationen bekannt gegeben werden müssten. Auch wäre wiederum der Informationsmehrwert für die betroffenen Personen aus der

Sicht von Coop sehr gering. Umgekehrt wird das Missbrauchspotenzial (Verwendung für datenschutzfremde Zwecke) als hoch eingeschätzt.

- Coop fordert deshalb, dass geschäftlich sensitive Bearbeitungsvorgänge von vornherein von einer etwaigen Information oder Auskunft ausgenommen werden können.

7. Alleinige Aufsicht des Beauftragten in der Schweiz sicherstellen

- Die DSGVO tritt im Mai 2018 in Kraft, das revidierte DSG wird zu gegebenem Zeitpunkt folgen. Die Parallelität der beiden gesetzlichen Regelungen wirft die Frage der aufsichtsrechtlichen Zuständigkeit auf: Es muss gewährleistet werden, dass der Beauftragte in der Schweiz die alleinige aufsichtsrechtliche Hoheit hat, unabhängig davon, ob in einem bestimmten Fall das Schweizer DSG oder die DSGVO zur Anwendung kommt.
- Coop begrüsst es, dass sich Bundesrat und Parlament im Rahmen der Motion 16.3752 mit dieser Problematik befassen und auch ihre Bereitschaft signalisiert haben, in dieser Sache Sondierungsgespräche mit der EU zu führen.

8. Umfassende Überarbeitung der strafrechtlichen Bestimmungen nötig

Coop fordert aufgrund der folgenden Erwägungen eine umfassende Überarbeitung der vorgesehenen Strafbestimmungen:

- **Grundsätzliches:** Die Strafbestimmungen verstossen gegen strafrechtliche Grundprinzipien. Die vorgesehenen Mitwirkungspflichten (insbesondere die Meldepflicht bei Datenschutzverstössen) kämen faktisch einer Selbstanzeige gleich, was mit Blick auf das Selbstbelastungsverbot besonders stossend ist.
- **Persönliche Strafbarkeit von Mitarbeitenden:** Coop lehnt die vorgesehenen individualstrafrechtlichen Sanktionen ab. Sie führen zu einer Kriminalisierung der mit dem Datenschutz betrauten Mitarbeiter. Die gesetzlich gegebenen Spielräume bei der Datenbearbeitung werden dann aus Angst vor persönlicher Bestrafung nicht ausgenutzt und es wird ein Denunziantentum innerhalb der Unternehmen gefördert. Ausserdem geraten Mitarbeitende in einen nicht hinnehmbaren Zielkonflikt, wenn sie zwischen der Wahrung von Geschäftsgeheimnissen und der Einhaltung ihrer Pflichten aus dem Datenschutzrecht abwägen müssen.
- **Verwaltungssanktionen gegen Unternehmen:** Im Gegenzug sind die Möglichkeiten zu Verwaltungssanktionen gegen Unternehmen auf verhältnismässige Art und Weise zu erweitern. Dieser Ansatz ist auch in der EU üblich, steht im Einklang mit anderen Gesetzen (KG, UWG, FMG und BEHG) und ist sachgerecht. Dabei ist darauf zu achten, dass die Sanktion zwar wirksam und abschreckend, aber auch angemessen ist. Als angemessen erachtet Coop dabei eine Busse von höchstens CHF 500'000.- resp. höchstens 250'000.- bei leichtem Verschulden.

Wir danken Ihnen für die Berücksichtigung unserer Argumente und stehen Ihnen für Rückfragen jederzeit zur Verfügung.

Freundliche Grüsse

Joos Sutter
Vorsitz der Geschäftsleitung
Coop Genossenschaft

Thomas Mahrer
Leiter Wirtschaftspolitik
Coop Genossenschaft

Beilagen: erwähnt

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 : Coop Genossenschaft

Abkürzung der Firma / Organisation : Coop

Adresse : Thiersteinerallee 14

Kontaktperson : Lukas Federer, Fachmitarbeiter Wirtschaftspolitik

Telefon : +41 61 336 72 04

E-Mail : lukas.federer@coop.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 ____ 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ 4

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 ____ 17

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ____ 17

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") ____ 18

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" ____ 18

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
Coop	Wir verweisen an dieser Stelle auf unser Begleitschreiben zur vorliegenden Stellungnahme.

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Coop	VE-DSG	2	2		**Antrag Coop:** Die Nichtanwendbarkeit des DSG auf hängige Verfahren gemäss Art. 2 Abs. 1 lit. c DSG fehlt und ist ins neue Recht zu übernehmen. **Begründung:** Es kann nicht angehen, dass die gegnerische Partei während hängiger Verfahren Auskunftsbegehren stellen kann. Dies hätte zur Folge, dass die so zur Auskunft verpflichtete Partei sich selbst belasten müsste (Verstoss gegen den nemo tenetur-Grundsatz).
Coop	VE-DSG	3		lit. f	**Antrag Coop:** *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 über das EU-Recht hinaus und soll jener der DSGVO angeglichen werden. Die Formulierung "um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen" muss in der Folgeregulierung eng eingegrenzt und sinnvoll konkretisiert werden.
Coop	VE-DSG	4	3		**Antrag Coop:** *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 zu streichen, da er ambivalent ist. Die Interpretationshoheit des Verwendungszwecks muss beim Verantwortlichen liegen und darf nicht von vornherein durch das Gesetz zu eng abgesteckt sein.
Coop	VE-DSG	4	6		**Antrag 1 Coop:** *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 geht über die EU-Regelung hinaus und ist deshalb zu streichen. **Antrag 2 Coop:** Die Einholung der Einwilligung muss einmalig und in allgemeiner Weise möglich sein (z.B. durch Ankreuzen eines Feldes, gem. Hinweis im Erläuternden Bericht), mindestens solange die gleiche Datengrundlage für die Bearbeitung verwendet wird. Dies ist auf Verordnungsebene zu gewährleisten. **Begründung 2:** Das häufigere Einholen einer Einwilligung (besonders einer ausdrücklichen) ist für die betroffenen Unternehmen sehr aufwändig und verbessert die Transparenz für die Konsumentinnen und Konsumenten nicht. Zudem ist die Massnahme besonders kostenintensiv für Angebote, die nicht rein Web-basiert sind (z.B. ist das Einholen der Einwilligung zu einer AGB-Änderung bei einer Kundenkarte massiv teurer als bei einer Suchmaschine oder einem Social-Media-Account). Dies ist diskriminierend für einzelne Wirtschaftszweige.
Coop	VE-DSG	5	5		**Antrag Coop:** *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, die zudem durch die Nachforderung von Informationen durch den Beauftragten beliebig verlängerbar ist, macht ein Genehmigungsverfahren nicht sinnvoll umsetzbar und führt zu unzumutbaren Verzögerungen bei Auslandtransfers. Eine Frist von dreissig Tagen (wie bisher) genügt.
Coop	VE-DSG	5	6		**Antrag Coop:** Bestimmung ersatzlos streichen. **Begründung:** Die Pflicht zur Information des Beauftragten geht über die Anforderungen der EU-Gesetzgebung (DSGVO) hinaus und wird deshalb abgelehnt. Sie bedeutet eine nicht akzeptable Mehrbelastung für alle Unternehmen und generiert zudem eine für den Beauftragten (zeitlich und inhaltlich) nicht sinnvoll zu bewältigende Informationsflut – ohne dass dabei ein Mehrwert für den Datenschutz und die betroffenen Personen geschaffen wird.
Coop	VE-DSG	6	1	lit. a	**Antrag Coop:** *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;* **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.
Coop	VE-DSG	6	2		**Antrag Coop:** Bestimmung ersatzlos streichen.

					Begründung: Die Meldepflicht von Datentransfers geht zu weit und ist nicht sinnvoll. Es kann nicht sein, dass der Beauftragte über solche Geschäftsgeheimnisse, welche wohl nicht einmal datenschutzrelevant sind, informiert werden muss. Er wird zudem kaum über die Kapazitäten verfügen, um die Meldungen zielführend zu verarbeiten. Zudem ist eine solche Bestimmung im EU-Recht (DSGVO) nicht vorgesehen. Entgegen den Ausführungen im Erläuternden Bericht (S. 51/52) wird dies auch vom Entwurf zur Revision des Übereinkommens SEV 108 nicht zwingend verlangt.
Coop	VE-DSG	7	2		**Bemerkung:** Bei der Präzisierung durch den Bundesrat muss die Rechtssicherheit für den Verantwortlichen gewahrt werden. Insbesondere ist darauf zu achten, dass der Auftragsbearbeiter sich nicht hinter seinem Auftraggeber verstecken kann. Es muss ein Gleichgewicht bestehen zwischen der Kontrollpflicht des Verantwortlichen und der Eigenverantwortung des Auftragsbearbeiters. Die Gewährleistung der Datensicherheit bei einem Drittanbieter darf nicht alleine Pflicht des Verantwortlichen sein. **Antrag Coop:** *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. Es ist völlig unrealistisch und unverhältnismässig, wenn der Auftragsbearbeiter sämtliche Rechte der betroffenen Person gewährleisten muss.
Coop	VE-DSG	8			**Bemerkung:** Coop begrüsst es, dass gemäss VE-DSG mittels Empfehlungen der guten Praxis eine verstärkte Selbstregulierung stattfinden soll. Die konkret vorgeschlagene Bestimmung läuft diesem Zweck jedoch gerade zuwider. Es kann nicht angehen, dass dem Beauftragten ein Genehmigungsvorbehalt zukommt – sonst handelt es sich letztlich um eine einseitige Auslegung des DSG durch den Beauftragten. Damit die Konkre-

					tisierung der datenschutzrechtlichen Pflichten sich als praxistauglich erweist, müssen Formulierungsvorschläge von den betroffenen Unternehmen und Branchen selbst erarbeitet werden. Soll der Ansatz der Selbstregulierung konsequent umgesetzt werden, muss die Initiative für Empfehlungen der guten Praxis daher von den interessierten Kreisen (Unternehmen und Branchen) selbst ausgehen. In anderen Rechtsgebieten haben sich Branchenvereinbarungen auf freiwilliger Basis als zielführend erwiesen (vgl. etwa die Branchenvereinbarung Plastiksäcke). Die Bestimmung ist dahingehend anzupassen, dass Unternehmen und Branchen das Recht haben, selbständig Branchenvereinbarungen auszuarbeiten. Statt einem Genehmigungsvorbehalt kommt dem Beauftragten ein Mitwirkungsrecht zu.
Coop	VE-DSG	9			**Antrag Coop:** Die Empfehlungen sollen lediglich die Vermutung begründen, dass das Gesetz eingehalten wird (keine Fiktion). **Begründung:** Eine Fiktion, welche von der Einhaltung der Empfehlungen auf die Einhaltung der Datenschutzvorschriften schliesst, ist nicht zielführend und wäre rechtsstaatlich problematisch. Es sind Konstellationen denkbar, die von den Empfehlungen nur unvollständig oder unzureichend geregelt sind. Die Fiktion ist auf eine Vermutung der Richtigkeit zu reduzieren. Diese muss ebenfalls für den Auftragsdatenbearbeiter gelten.
Coop	VE-DSG	13			**Bemerkung:** Aus der vorgeschlagenen Formulierung von Art. 13 VE-DSG geht zu wenig eindeutig hervor, welche Beschaffungsvorgänge von der Informationspflicht betroffen sind. In der Botschaft ist klar festzuhalten, dass nicht jede einzelne Datenbeschaffung eine Informationspflicht auslösen kann. Insbesondere dürfen die in Art. 13 Abs. 2 lit. b VE-DSG genannten Kategorien von Personendaten nicht zu eng gefasst werden.
Coop	VE-DSG	13	1		**Antrag Coop:** *Der Verantwortliche informiert die betroffene Person über die Beschaffung von besonders schützenswerten Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden.* **Begründung:**

					Die Gesetzesformulierung gemäss Vernehmlassungsvorlage hätte zur Folge, dass KundInnen regelrecht mit Informationen überflutet würden. Eine Informationspflicht ist daher nur bei der Beschaffung von besonders schützenswerten Personendaten angezeigt.
Coop	VE-DSG	13	3		**Antrag Coop:** *Werden Personendaten Dritten für deren eigene Verwendung bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.* **Begründung:** Die Weitergabe von Personendaten an Dritte im Rahmen von Art. 7 VE-DSG soll, wie im geltenden Recht (Art. 10*a* DSG), nicht der Informationspflicht unterliegen. Andernfalls müsste der Verantwortliche über den Beizug sämtlicher Hilfspersonen informieren.
Coop	VE-DSG	13	4		**Antrag Coop:** Bestimmung ersatzlos streichen. **Begründung:** Die Bekanntgabe der Identität des Auftragsbearbeiters stellt gegenüber dem EU-Recht eine Besonderheit dar und wird deshalb von Coop abgelehnt (Swiss Finish).
Coop	VE-DSG	14	4	lit. a	**Antrag Coop:** *a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht konzernfremden Dritten bekannt gibt;* **Begründung:** Die Berufung auf ein überwiegendes privates Interesse muss bei der Datenweitergabe unter Konzerngesellschaften möglich sein, ansonsten mit einem enormen administrativen Mehraufwand zu rechnen wäre,

					der nicht zur Transparenz beiträgt.
Coop	VE-DSG	15	1		**Antrag Coop:** *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 Voraussetzung für eine Information soll sich auf erhebliche Auswirkungen beschränken, so wie dies in der EU (DSGVO) auch der Fall ist. 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, wenn dies tatsächlich dem Datenschutz dient. In diesem Sinne ist der Begriff "rechtliche Wirkungen" zu streichen.
Coop	VE-DSG	15	2		**Antrag Coop:** Bestimmung ersatzlos streichen. **Begründung:** Es ist zu befürchten, dass ein Recht zur "Äusserung" faktisch zu einer Begründungspflicht führt und damit die Vertragsfreiheit einschränkt (Kontrahierungszwang). Das ist ein Anliegen des Konsumentenschutzes, das nicht ins Datenschutzrecht gehört.
Coop	VE-DSG	16	1		**Antrag Coop:** *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.* **Begründung:**

					Wie auch im EU-Recht, soll die Folgeabschätzung nur bei einem hohen Risiko notwendig werden. Auch ist der Verweis auf die Grundrechte zu entfernen – Es ist (wie gemäss geltendem Recht) nicht die Aufgabe eines privaten Verantwortlichen, die Grundrechte betroffener Personen zu schützen, sofern diese Grundrechte nicht in einzelnen Anforderungen des DSG Ausdruck gefunden haben. Coop investiert bereits heute viel in den Datenschutz – dies wurde seitens EDÖB mehrfach gewürdigt. Trotz diesen guten Voraussetzungen hätte die vorgesehene Vorschrift der Datenschutz-Folgenabschätzung erhebliche Kostenauswirkungen, sofern die genannte Einschränkung nicht erfolgt. Die Bestimmung darf nicht dazu führen, dass beispielsweise jedes Mal eine Datenschutz-Folgenabschätzung notwendig wird, wenn Coop eine neue Verkaufsstelle eröffnet (z.B. weil aufgrund der Sicherheitsaufzeichnungen ein "erhöhtes Risiko" bestünde). Die Datenschutzfolgeabschätzung darf (dem EU-Recht entsprechend!) nicht mehr als ein zeitlich vorgelagertes Datenbearbeitungsreglement sein.
Coop	VE-DSG	16	3-4		**Antrag Coop:** Beide Bestimmungen ersatzlos streichen. **Begründung:** Beide Bestimmungen gehen über die Regelungen des EU-Rechts hinaus und führen zu einem hohen Mehraufwand mit geringem Zusatznutzen für die Konsumentinnen und Konsumenten. Die Frist von drei Monaten zur Erhebung von Einwänden kann zudem eine unnötige Verzögerung bei Einführung neuer Geschäftsmodelle bewirken.
Coop	VE-DSG	17			**Antrag Coop:** Der Begriff der Unverzüglichkeit in Abs. 1 genau zu klären. Ebenso sind die Pflichten des Auftragsbearbeiters mit jenen des Verantwortlichen abzustimmen. **Begründung:** Auch hier fordert Coop eine massvolle Regulierung, so dass nicht jede Kleinigkeit eine Meldung nach sich zieht. Dies wäre aus Sicht der betroffenen Personen, der Unternehmen und letztlich auch des Beauftragten nicht zweckmässig aufgrund der resultierenden Informationsflut. Denkbar wäre ein analoger Prozess wie bei einem Produkt-Rückruf durch das BLV oder das BAG – in diesem Bereich hat sich ein risikobasierter

					Ansatz (da abgestuft für verschiedene Situationen!) und ein funktionierender Austausch zwischen Bundesorganen und Wirtschaft etabliert.
Coop	VE-DSG	18	1		**Antrag 1 Coop:** Der Begriff "angemessene Massnahmen" ist in der Verordnung zu konkretisieren, so dass die betroffenen Unternehmen einerseits Rechtssicherheit haben und andererseits keine unverhältnismässigen Massnahmen umzusetzen sind. **Begründung 1:** Coop befürwortet einen besseren Datenschutz "ex ante", jedoch nicht ohne eindeutige Definition der "Angemessenheit". Die Marktbearbeitung muss weiterhin unter stabilen Rahmenbedingungen stattfinden können. **Antrag 2 Coop:** *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.* **Begründung 2:** Der Einbezug der Auftragsbearbeiter in die vorliegende Bestimmung geht über die Regelung im EU-Recht hinaus. Er wird deshalb von Coop abgelehnt.
Coop	VE-DSG	18	2		**Bemerkung:** "Privacy by Default" muss so praxisnah wie möglich umgesetzt werden. Dies beinhaltet auch die Sicherstellung der Planungs- und Rechtssicherheit für Unternehmen, die beispielsweise in Kundenbindungsprogramme investieren.
Coop	VE-DSG	19		lit. a-b	**Antrag Coop:** *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 Benachrichtigung, 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.~~* **Begründung:** Inhalt und Ausmass der Pflicht zur Dokumentation der Datenbearbeitung gemäss lit. a soll auf das Führen eines Verzeichnisses aller Datenbearbeitungen, für die der Verantwortliche direkt zuständig ist, beschränkt werden. Es wäre absolut unverhältnismässig, eine umfassende und detaillierte Dokumentation der Datenbearbeitung zu verlangen, insbesondere auch vor dem Hintergrund, dass ein Verstoss gegen die Dokumentationspflicht nach dem VE-DSG sanktioniert werden kann. Ausserdem sieht das EU-Recht keine derart weitgehende Informationspflicht vor.
Coop	VE-DSG	20	1		**Bemerkung** Es fehlt eine Bestimmung zur Bekämpfung des Missbrauchs des Auskunftsrechts, insbesondere für die zweckentfremdete Nutzung zur Beweismittelausforschung. Dies ist umso stossender, da Auskunftsbegehren de lege nie unverhältnismässig sein können, sprich auch untergeordnete Datenschutzinteressen für einen Auskunftsanspruch ausreichen. Es sind daher weitere Mechanismen zur Verhinderung des Auskunftsrechts bei offensichtlich nicht datenschutzrechtlichen Zwecken vorzusehen (z.B. durch die Ergänzung von Art. 21 VE-DSG um einen weiteren Ausnahmetatbestand). **Antrag Coop:** *Jede Person kann vom Verantwortlichen ~~kostenlos~~ Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.* **Begründung:** Die Möglichkeit einer Kostenbeteiligungspauschale soll gemäss geltendem Recht weitergeführt werden (Art. 2 VDSG).

Coop	VE-DSG	20	2	lit. b-f	**Antrag Coop:** *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: (…)* *f. die verfügbaren Angaben über die Herkunft der Personendaten, sofern diese nicht direkt bei der betroffenen Person beschafft wurden; (…)* **Begründung:** Wenn die Personendaten bei der betroffenen Person selbst beschafft wurden, ist ein zusätzliches Auskunftsrecht über die Datenherkunft redundant.
Coop	VE-DSG	20	3		**Antrag Coop:** Die Bestimmung ist ersatzlos zu streichen. **Begründung:** Die Pflicht zur Begründung jeglicher Entscheide (nicht nur automatisierte Einzelentscheide) greift massiv in die Freiheit eines Unternehmens ein und geht über die Erfordernisse der DSGVO hinaus.
Coop	VE-DSG	21			**Antrag Coop:** Die Berufung auf überwiegende private Interessen muss zulässig sein. Dies gilt insbesondere für die Datenweitergabe innerhalb des Konzerns. **Begründung:** Siehe Begründung Antrag Coop zu Art. 14 Abs. 4 lit. a VE-DSG.
Coop	VE-DSG	23	2	lit. d	**Antrag Coop:** Bestimmung ersatzlos streichen. **Begründung:**

					Das Erfordernis der Einwilligung geht über die EU-Regelung hinaus und ist deshalb zu streichen.
Coop	VE-DSG	23	3		**Bemerkung:** Das Opt-out-Recht darf nicht zu einer Verunmöglichung oder Einschränkung des mitgeteilten Zweckes führen. Beispielsweise kann eine Kundenkarte nicht sinnvoll genutzt werden, wenn die betroffene Person die Zustimmung für die in den Geschäftsbedingungen vorgesehene Datenbearbeitung entzieht. Wer den in den AGB vorab beschriebenen Datenerhebungen und –bearbeitungen zustimmt, soll daher nachträglich diese Zustimmung nicht teilweise entziehen können. Es soll nur ein vollständiger Rücktritt möglich sein, da sonst das entsprechende Angebot nicht mehr sinnvoll genutzt werden kann.
Coop	VE-DSG	24	2	a	**Bemerkung:** Der Rechtfertigungsgrund des Abschlusses und der Abwicklung des Vertrags sollte auch die Bearbeitung von Daten weiterer in den Vertrag involvierter Personen umfassen (z.B. Kontaktpersonen für Rückfragen).
Coop	VE-DSG	41	5		**Antrag Coop:** Bestimmung ersatzlos streichen. **Begründung:** Es verletzt die Geheim- und Privatsphäre des Unternehmens, wenn die Anzeige erstattende Privatperson über das Ergebnis einer allfälligen Untersuchung informiert wird.
Coop	VE-DSG	44	3		**Antrag Coop:** Bestimmung ersatzlos streichen. **Begründung:** Vorsorgliche Massnahmen im Bereich der Datenbearbeitung können massive Konsequenzen für Unternehmen haben. Die Erfahrungen haben gezeigt, dass der Beauftragte vorsorgliche Massnahmen auch ohne vertieftes Abwägen der Folgen beantragt. Eine unabhängige Überprüfungsmöglichkeit ist daher entscheidend. Bis diese stattfindet, muss eine aufschiebende Wirkung bestehen.

Coop	VE-DSG	50-55			**Antrag Coop:** Es sind primär verwaltungsrechtliche Sanktionen für Unternehmen vorzusehen. Lediglich subsidiär soll eine strafrechtliche Verfolgung der Mitarbeitenden bei Vorsatz möglich sein. Die maximale Bussenhöhe für Unternehmen ist auf CHF 500'000.- resp. bei leichtem Verschulden auf CHF 250'000.- zu begrenzen. Der Strafenkatalog ist mit jenem der DSGVO abzugleichen. **Begründung:** Die vorgesehene persönliche Strafbarkeit ist weder verhältnismässig noch zielführend und führt in Unternehmen zu einer Denunziationskultur. Dem Ziel – einem hohen Datenschutzniveau – ist in einem verwaltungsrechtlichen Sanktionssystem besser gedient. Ferner müssen die in Art. 50-55 zitierten Pflichten genauer umschrieben werden, um dem strafrechtlichen Bestimmtheitsgebot gerecht zu werden. Durch die primäre Strafbarkeit der Unternehmen mit maximalen Bussen von CHF 500'000.- resp. CHF 250'000.- kannsichergestellt werden, dass Sanktionen wirksam und abschreckend, aber auch angemessen sind.
Coop	VE-DSG	52			**Antrag Coop:** Die Bestimmungen zur Schweigepflicht sollen gemäss geltendem DSG belassen werden. **Begründung:** Für die Verschärfung der heute in Art. 35 DSG beschriebenen Schweigepflicht besteht kein Anlass. Es ist nicht nachvollziehbar, wieso z.B. der Onlinehandel den gleich weitreichenden Geheimhaltungspflichten wie etwa ein Arzt unterliegen soll. Ausserdem stellt Art. 52 VE-DSG mit der Bezugnahme auf "geheime Personendaten" auf einen Begriff ab, ohne diesen näher zu definieren.
Coop	VE-DSG	59			**Antrag Coop:** Die Übergangsfrist von zwei Jahren ist generell zu gewähren. **Begründung:** Eine generelle Übergangsfrist von zwei Jahren ist angemessen und EU-konform (DSGVO).

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

Centre Patronal

Département fédéral de justice et police
DFJP
3003 Berne

Par courrier électronique :
M. Jonas Amstutz
jonas.amstutz@bj.admin.ch

Paudex, le 24 mars 2017
PGB

Consultation: révision de la loi fédérale sur la protection des données

Madame, Monsieur,

Nous avons pris connaissance du dossier de consultation mentionné en titre, qui comprend un avant-projet de révision totale de la loi fédérale sur la protection des données, ainsi que des modifications liées à ce thème dans plusieurs autres lois fédérales. Ce dossier intéresse l'économie privée. Par la présente, nous souhaitons vous communiquer notre position.

Objectif de la révision

Nous avons pris note de ce que la présente révision est motivée essentiellement par un double souci 1) d'adapter la loi de 1992 aux circonstances actuelles (utilisation facile, intensive et multiforme de très nombreuses données, méfiance croissante des citoyens) et 2) de suivre l'évolution de la législation européenne (reprise de développements Schengen, maintien de la possibilité d'échanger des données avec l'UE). Nous comprenons et approuvons ces objectifs.

Contenu et conséquences de la révision, remarques générales

Charge administrative pour les entreprises

Concrètement, la révision amène à préciser et à accroître les obligations des responsables de traitements de données (organisations, entreprises) et à élargir simultanément les droits des personnes dont les données sont utilisées (citoyens, clients). Fondamentalement, cette évolution peut apparaître légitime face aux vastes possibilités offertes par les techniques modernes de communication: il importe que l'usage des données soit cadré et que les citoyens puissent avoir confiance dans l'usage qui en est fait.

Toutefois, l'analyse des dispositions de la nouvelle loi, de même que les échos que nous recevons, montrent que ces dispositions peuvent entraîner des charges administratives substantielles pour certaines entreprises, en particulier pour les PME – qui ont pourtant, dans leur grande majorité, un comportement prudent et respectueux en matière de traitement de données. Il est important que les autorités – l'administration fédérale, le législateur, le Préposé fédéral à la protection des données – soient conscientes de l'importance de ces charges, ce qui ne ressort pas toujours clairement de la lecture du rapport explicatif. Ce dernier affirme, sur un ton quelque peu désinvolte, que «les coûts nécessaires au respect des nouvelles obligations […] devraient ainsi être compensés, notamment par les avantages découlant du libre transfert des données avec l'Union européenne»; pour notre part, nous ne croyons pas qu'une telle «compensation» puisse concerner toutes les entreprises.

Route du Lac 2
1094 Paudex
Case postale 1215
1001 Lausanne
T +41 58 796 33 00
F +41 58 796 33 11
info@centrepatronal.ch

Kapellenstrasse 14
Postfach 5236
3001 Bern
T +41 58 796 99 09
F +41 58 796 99 03
cpbern@centrepatronal.ch

www.centrepatronal.ch

Considérant cela, nous ne pouvons pas nous réjouir d'un renforcement de la législation dans ce domaine. Nous pouvons toutefois l'accepter dans la mesure où 1) ce renforcement permettra le maintien des échanges de données avec d'autres pays européens, ce qui est dans l'intérêt de nombreuses entreprises, et 2) les contraintes imposées aux responsables de données, bien qu'importantes, n'apparaissent pas a priori exagérées ou déraisonnables.

Futures «recommandations de bonnes pratiques»

Nous constatons que la mise en œuvre concrète de certaines dispositions n'est, au stade actuel, pas aisée à concevoir. Nous nous prononçons aujourd'hui sur des principes qui peuvent paraître légitimes mais dont nous ne savons pas encore comment il faudra les appliquer, ni à quelles conditions leur mise en œuvre sera considérée comme conforme à la loi. Tout reposera sur les futures «recommandations de bonnes pratiques» qui seront édictées par le Préposé et qui constitueront des «standards» d'application de la nouvelle loi.

Nous comprenons certes l'intérêt de ne pas intégrer trop de détails dans la loi elle-même, s'agissant d'un domaine où les pratiques évoluent vite. Mais nous souhaitons tout de même insister sur les attentes du monde économique face à ces futures «recommandations»: non seulement elles ne devront évidemment pas aller plus loin que la loi elle-même, mais elles devront aussi être conçues de manière à aider toutes les entreprises, y compris les PME, à remplir leur obligations légales d'une manière pragmatique et proportionnelle aux intérêts en jeu. Idéalement, ces futures «recommandations» pourraient faire l'objet, le moment venu, d'une nouvelle procédure de consultation.

Préposé fédéral à la protection des données

La révision renforce les pouvoirs et compétences du Préposé fédéral à la protection des données, qui pourra désormais ouvrir des enquêtes d'office et prendre des décisions contraignantes. Cette évolution ne va pas dans un sens positif et représentera une source d'inquiétude pour des entreprises qui se trouveront peut-être confrontées à des enquêtes ouvertes d'office, sans même qu'elles aient fait l'objet d'une plainte.

Nous pouvons toutefois l'accepter dans la mesure où cela apparaît nettement comme une condition posée par l'UE pour le maintien du libre transfert de données avec la Suisse. Mais nous insistons pour que le Préposé à la protection des données exerce ces pouvoirs avec modération et maintienne un dialogue régulier avec le monde économique.

Gratuité des frais

Enfin, le seul point qui appelle un refus catégorique de notre part est la modification du Code de procédure civile, qui accorderait l'absence de frais justice pour les actions civiles en matière de protection des données (comme c'est déjà le cas, par exemple, en matière d'égalité entre hommes et femmes ou en matière de droit du travail). La gratuité de ces procédures est censée encourager les personnes concernées à faire valoir leurs droits devant la justice civile. Or un tel encouragement apparaît totalement inopportun et inutilement chicanier, ce d'autant plus qu'il ne résulte apparemment d'aucune nécessité ni d'aucune revendication de l'UE.

Conclusions

En conclusion de ce qui précède, et sous réserve de la prise en compte de nos diverses remarques, nous ne nous opposons pas à la révision projetée, excepté en ce qui concerne la gratuité des procédures civiles en matière de protection des données.

Nous vous remercions de l'attention que vous porterez à ce qui précède et vous prions d'agréer, Madame, Monsieur, nos salutations les meilleures.

Centre Patronal

Pierre-Gabriel Bieri

Annexe: formulaire officiel pour la prise de position

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 : Centre Patronal

Abréviation de la société / de l'organisation : CP

Adresse : 2, route du Lac, 1094 Paudex

Personne de référence : Pierre-Gabriel Bieri

Téléphone : 058 796 33 70

Courriel : pgbieri@centrepatronal.ch

Date : 24 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

Remarques générales 3

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 4

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 5

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel 6

Rapport explicatif (excepté chap. 8 « Commentaire des dispositions») 6

Rapport explicatif : chap. 8 « Commentaire des dispositions » 7

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 :**
CP	D'une manière générale, les nouvelles contraintes imposées aux responsables de traitements de données pourront entraîner des charges supplémentaires parfois importantes pour certaines entreprises. Le rapport explicatif est un peu léger sur cet aspect.
CP	L'impact exact de ces nouvelles contraintes reste difficile à évaluer, dès lors que la mise en œuvre concrète de certaines dispositions dépendra largement des futures «recommandations de bonnes pratiques» qui seront édictées par le Préposé fédéral à la protection des données. Il importe que ces futures «recommandations» non seulement ne dépassent pas le sens de la loi, mais soient en outre élaborées de manière à permettre à toutes les entreprises, y compris les PME, de remplir leur obligations légales d'une manière pragmatique et proportionnée aux intérêts en jeu. Ces futures recommandations pourraient idéalement faire l'objet d'une procédure de consultation.
CP	Le renforcement des pouvoirs et des compétences du Préposé fédéral à la protection des données pourra représenter une source d'inquiétude pour des entreprises qui se trouveront peut-être confrontées à des enquêtes ouvertes d'office, sans même qu'elles aient fait l'objet d'une plainte. Nous souhaitons que le Préposé à la protection des données exerce ces pouvoirs avec modération et maintienne un dialogue régulier avec le monde économique.
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

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 :
CP	LPD	3	h + i		L'expression "personne privée" laisse supposer qu'un travailleur employé par une entreprise pourrait être tenu pour personnellement responsable des traitements de données qu'il effectue dans le cadre de son activité professionnelle, ce qui ne paraît pas adéquat.
CP	LPD	5	5		Un délai de six mois pour obtenir l'approbation du préposé paraît excessivement long.
CP	LPD	10	2		Nous nous interrogeons fortement sur l'utilité d'un "label de qualité de protection des données" réglementé par le Conseil fédéral. Le rapport explicatif ne donne aucune justification à ce sujet. Si tant est qu'un label soit véritablement utile, il n'a pas besoin d'une réglementation étatique.
CP	LPD	11	2		Nous nous interrogeons sur l'utilité d'une réglementation supplémentaire relative à des "exigences minimales en matière de sécurité des données". Les exigences formulées à l'alinéa 1 de cet article nous paraissent suffisantes.
CP	CPC	113 + 114			Nous refusons catégoriquement la suppression des frais de justice pour les actions civiles en matière de protection des données.
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.		

Rapport explicatif : chap. 8 « Commentaire des dispositions »

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

CREDIT SUISSE AG
Paradeplatz 8
Postfach
CH-8070 Zurich

Telefon 044 333 3389
Telefax 044 334 8600
www.credit-suisse.com

Eidg. Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

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

Zürich, 4. April 2017

Vorentwurf zu einer Totalrevision des Datenschutzgesetzes

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Am 21. Dezember 2016 wurde der Vorentwurf zur Totalrevision des Datenschutzgesetzes in die Vernehmlassung gegeben. Gerne unterbreiten wir Ihnen hiermit unsere Stellungnahme zum Revisionsvorentwurf.

Vorgängig verweisen wir auf die Kommentierungen der Schweizerischen Bankiervereinigung, des Wirtschaftsdachverbandes economiesuisse und des Verein Unternehmens-Datenschutz VUD, die Sie mit separatem Schreiben erhalten haben. An allen dreien haben wir massgeblich mitgewirkt, und wir unterstützen diese. In unserer Stellungnahme möchten wir darüber hinaus die aus Sicht der Credit Suisse wichtigsten Aspekte hervorheben und nachstehend kommentieren.

Anpassung der Vorlage notwendig, um Ziele der Reform und Praktikabilität für Wirtschaft sicherzustellen

Die Credit Suisse begrüsst die grundsätzliche Stossrichtung des Vorentwurfs zur Totalrevision des Datenschutzgesetzes. Die neu erlassene Datenschutzverordnung der EU macht eine Anpassung der Schweizer Gesetzgebung notwendig, um zu gewährleisten, dass Personendaten zwischen der Schweiz und EU-Staaten unkompliziert fliessen können. Zudem ist es wichtig für unsere exportorientierte Wirtschaft, dass die Datenschutzgesetzgebungen in der EU und in der Schweiz in allen Prinzipien sehr ähnlich sind. Wäre dies nicht der Fall, müssten Firmen je nach Kunden unterschiedliche Regelungen einführen.

Die Anpassungen im Rahmen der Revision müssen sorgfältig austariert werden. Einerseits muss mit der Revision die Gleichwertigkeit mit der EU-Regelung erzielt werden, andererseits dürfen die Anpassungen auch nicht über das Ziel hinausschiessen, da ansonsten Standortvorteile verloren gingen.

In vielen Punkten stimmt der Vorentwurf zur Revision des Datenschutzgesetzes (VE-DSG) mit den Grundprinzipien der EU-Regelung überein. Dies ist für die Anerkennung der Gleichwertigkeit zentral. Ausdrücklich begrüsst wird, dass sie sich auf natürliche Personen beschränkt und juristische Personen von der Anwendbarkeit ausnimmt.

In verschiedenen Punkten nimmt sie allerdings nicht ausreichend Rücksicht auf die Bedürfnisse der Wirtschaft und kann in ihrer aktuellen Form somit nicht unterstützt werden. Wir sind jedoch der Ansicht, dass durch zielgerichtete Anpassungen eine Vorlage geschaffen werden kann, welche die Ziele der Reform erreicht und für die umsetzenden Unternehmen praktikabel ist.

Unseres Erachtens besteht insbesondere Anpassungsbedarf bei den nachfolgenden Aspekten:

Swiss Finish im Vergleich zur Datenschutzverordnung der EU vermeiden

Die folgenden Artikel charakterisieren sich dadurch, dass sie striktere Regelungen als die EU-Verordnung vorsehen. Diese zusätzlichen Einschränkungen stellen einen für die Gleichwertigkeit mit der EU-Regelung unnötigen „Swiss Finish" dar und schaffen wesentliche Wettbewerbsnachteile für Schweizerische Unternehmen.

- Profiling (Art. 3 lit. f und Art. 23 Abs. 2 lit. d VE-DSG)

  Die Definition von Profiling geht über die Vorgaben der Datenschutz-Grundverordnung der EU (EU-DSGVO) hinaus. Das Konzept sollte mit der europäischen Idee übereinstimmen. Hier wird speziell für die Schweiz eine weitergehende, aufwändige Lösung kreiert, die in der Praxis viel Aufwand verursachen würde und aufgrund der Strafbestimmungen und Bussen zu erheblichen Risiken für die Unternehmen führt. Deshalb ist die Definition von Profiling auf die automatisierte Auswertung von Personendaten einzuschränken. Art. 23 Abs. 2 lit. d VE-DSG ist zudem zu streichen.

- Bekanntgabe ins Ausland in Ausnahmefällen (Art. 5 Abs. 6 und Art. 6 Abs. 2 VE-DSG)

  Art. 5 Abs. 6 und Art. Art. 6 Abs. 2 VE-DSG sind zu streichen. Die Pflicht zur Information des Beauftragen ist der EU-DSGVO fremd sowie in dieser Breite in der Schweizer Gesetzgebung neu. Sie verursacht eine sehr hohe administrative Bürde für die Unternehmen. Zudem würde der Beauftragte mit einem hohen Volumen an Informationen konfrontiert werden mit dem Risiko, dass deren ordentliche Bearbeitung nicht mehr geleistet werden kann.

- Bekanntgabe ins Ausland in Ausnahmefällen (Art. 6 Abs. 1 VE-DSG)

  Die Beschränkung Abs.1 lit.c auf „unerlässlich" hat sich als unpraktikabel erwiesen, womit diese gesetzliche Ausnahme faktisch gar nicht ausgeübt werden konnte. Eine Anpassung auf „massgeblich" ist deshalb notwendig, damit diese Bestimmung in der Praxis überhaupt verwendet werden kann.

  In Abs. 1 lit. c. Ziff.2 sollte sodann in Analogie zu Art. 42c FINMAG der Kreis auch um „andere ausländische Stellen" erweitert werden, die mit Aufsichtsaufgaben betraut sind. Diese Wahrnehmung von Aufsichtsaufgaben in delegierter Form hat sich aus Effizienzgründen in vielen Staaten verbreitet und muss vom Schweizerischen Gesetzgeber berücksichtigt werden.

- Informationspflicht bei der Beschaffung von Personendaten (Art. 13 Abs. 4 und 5 VE-DSG)

  Diese Vorschrift geht über die Regelung der EU-DSGVO hinaus. Sie führt zu einem erheblichen Mehraufwand, stellt einen wesentlichen Wettbewerbsnachteil für die Schweizerische Wirtschaft dar und verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Art. 13 Abs. 4 VE-DSG ist zu streichen und Art. 13 Abs. 5 VE-DSG ist mit einer Regelung in Anlehnung an die EU-DSGVO (Art. 14.3.(a)-(c)) zu ersetzen. Dort ist der Anknüpfungspunkt nicht die „Speicherung", sondern die „Beschaffung".

- Ausnahmen von der Informationspflicht und Einschränkungen (Art. 14 Abs. 2 und Abs. 4 VE-DSG)

  Die EU-DSGVO kennt mehr Ausnahmen von der Informationspflicht als der Schweizer VE-DSG. Deshalb sollte die Schweizer Vorlage um weitere Ausnahmen ergänzt werden. Beispielsweise entfällt die Informationspflicht in der EU-DSGVO, wenn die Daten dem Berufsgeheimnis unterliegen – ein Punkt, der auch in der Schweizer Gesetzgebung zu ergänzen ist.

- Datenschutz-Folgeabschätzung, und Meldung von Verletzungen des Datenschutzes (Art. 16 und Art. 17 VE-DSG)

  In Art. 16 und 17 VE-DSG ist unklar, was der Unterschied zwischen «Risiko für die Persönlichkeit» und «Risiko einer Verletzung der Persönlichkeit» ist. Letzterer ist ein auch in der übrigen Rechtsordnung verwendeter Begriff; ersterer hingegen ist unklar.

  Art. 16 VE-DSG ist nicht logisch stringent formuliert und hat erhebliche administrative Aufwendungen zur Folge, welche bei Unterlassen mit Strafe belegt werden.

  Aufgrund der Verpflichtung des Auftragsbearbeiters zusätzlich zum Verantwortlichen sieht Art. 16 VE-DSG unnötig einen kleineren Spielraum als die EU-DSGVO vor. Richtigerweise ist in Art. 16 VE-DSG nur der Verantwortliche in die Pflicht zu nehmen und die Nennung des Auftragsbearbeiters zu streichen.

  Die in Art. 16 Abs. 1 und 2 VE-DSG erwähnte direkte Drittwirkung von Grundrechten für Private gibt es nicht (mit Ausnahme von Art. 8 Abs.3 BV, die aber auf den Bereich des DSG nicht direkt Anwendung findet). Private müssen bei ihrem Handeln die Grundrechte nicht beachten. Art. 16 VE-DSG ist entsprechend anzupassen.

  Die bisherige Frist von 3 Monaten in Art. 16 Abs. 4 VE-DSG hat sich bei Fällen mit Auslandsbezug als äusserst nachteilig erwiesen, weshalb eine wesentliche Verkürzung nötig ist. Es kann nicht sein, dass Schweizerischen Unternehmen im Ausland Nachteile drohen, weil die inländischen Verfahren sich zu lange hinziehen. Es ist neu eine Beschleunigung auf 2 Wochen vorzusehen.

  Zudem ist in einem neuen Abs. 5 explizit festzuhalten, dass die Datenschutz-Folgeabschätzung als genehmigt gilt, wenn innert Frist keine Einwände geltend gemacht werden (Klärung der Folgen und Beschleunigung des sonst überlangen Verfahrens).

  Gemäss Art. 17 VE-DSG müsste jede «unbefugte Datenbearbeitung» dem Beauftragten gemeldet werden. Die Verletzung dieser Bestimmung steht unter Strafe. Damit wird gegen das Prinzip von «nemo tenetur se ipsum accusare» («niemand ist verpflichtet, sich selbst zu belasten») verstossen. Die Strafandrohung ist zu streichen.

  Des Weiteren sprechen die Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarats (SEV 108) und die EU-DSGVO nur von «Verstoss gegen die Datensicherheit». Art. 17 VE-DSG geht darüber hinaus. Ohne eine Einschränkung ist eine Flut von Meldungen zu erwarten. Deshalb ist die Meldepflicht auf den Verlust der Daten in Kombination mit einem hohen Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person einzuschränken.

- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 18 Abs. 1 VE-DSG)

  Aufgrund der Verpflichtung des Auftragsbearbeiters zusätzlich zum Verantwortlichen sieht der Artikel einen kleineren Spielraum als die EU-DSGVO vor. In Art. 18 Abs. 1 VE-DSG ist nur der Verantwortliche in die Pflicht zu nehmen und die Nennung des Auftragsbearbeiters zu streichen.

- Auskunftsrecht (Art. 20 Abs. 3 VE-DSG)

Art. 20 Abs. 3 VE-DSG enthält einen operativ sehr aufwendigen Swiss Finish. Die Ausweitung auf jede Datenbearbeitung ist ein Eingriff in die operative Führung eines jeden Unternehmens und zwingt das Unternehmen, jede Entscheidung zu begründen. Im Sinne der Verhältnismässigkeit ist Art. 20 Abs. 3 VE-DSG auf *automatisierte* Einzelentscheidungen zu beschränken.

- Untersuchung (Art. 41 Abs. 3 VE-DSG)

  Dem Beauftragten werden polizeiliche Befugnisse eingeräumt, welche in der EU-DSGVO nicht vorgesehen sind. Art. 41 Abs. 3 VE-DSG ist deshalb dahingehend zu ergänzen, dass der Beauftragte, um von den erwähnten Befugnissen Gebrauch zu machen, vorgängig eine anfechtbare Verfügung vorzulegen hat.

Strafbestimmungen müssen eigeschränkt werden

Der Schweizer VE-DSG beinhaltet strenge Strafbestimmungen, welche zu entschärfen sind. Die Bussenhöhe steht in keinem Verhältnis zum potentiellen Unrechtsgehalt bzw. zur übrigen Rechtsordnung. Vergleichbare Sachverhalte sanktioniert Art. 150 FINFRAG mit höchstens Fr. 100 000. Dieser Rahmen trifft einen Privaten empfindlich und sollte auch hier Anwendung finden. Hier wurde gegenüber der EU «vorauseilender Gehorsam» betrieben. Die SEV 108 schreibt keine derart hohen Bussen vor. Zudem darf bezweifelt werden, ob die Gleichwertigkeitsanerkennung der EU-Kommission tatsächlich von der Bussenhöhe abhängt.

Die Geldstrafen sind damit generell zu senken. Es ist nicht vertretbar, dass Private für Lappalien, d.h. Verletzung von Formvorschriften oder die Verletzung von Meldepflichten, mit Bussen bis zu CHF 500'000.- bestraft werden. Darüber hinaus, unterscheidet der Entwurf hinsichtlich der maximalen Bussbeträge nicht zwischen formellen und materiellen Pflichtverletzungen. Die Maximalbussen für formelle Pflichtverletzungen (Art. 50 VE-DSG) sind im Vergleich zu den materiellen Pflichtverletzungen (Art. 51 VE-DSG) erheblich tiefer anzusetzen.

Das DSG gilt auch für alle Unternehmen in der Schweiz. Diese müssten gemäss VE-DSG einen enormen Aufwand betreiben, um sicherzustellen, dass sie sich nicht strafbar machen. Bussen für fahrlässiges Handeln öffnen Tür und Tor für unzählige Verfahren. In keinem Tätigkeitsbereich ist die Schwelle für Bussen vergleichbar niedrig. Deshalb ist eine explizite Beschränkung auf direkt vorsätzliches Handeln vorzusehen („Wer wider besseres Wissen….“), was aufgrund der Komplexität des Datenschutzgesetzes durchaus angebracht ist. Die Bestimmungen würden sonst zu einer Kriminalisierung der verantwortlichen Personen in den Unternehmen führen. Es wäre daher in Zukunft deutlich schwieriger, überhaupt noch geeignetes Personal für die entsprechenden Stellen zu finden.

Schliesslich ist die Kompetenzregelung (Ausfällung der Strafen von den jeweiligen Strafverfolgungsbehörden in den Kantonen) unbefriedigend. Um eine einheitliche Handhabung zu gewährleisten, ist eine Regelung der Strafkompetenz im Verwaltungsrecht vorzuziehen.

- Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten (Art. 50 Abs. 3 lit. b und Abs. 4 VE-DSG)

  Der Tatbestand ist auf direkten Vorsatz zu beschränken. Eine mögliche Strafe aufgrund einer fahrlässigen oder eventualvorsätzlichen Handlung führt nur dazu, dass jeder Verantwortliche bei jedem Entscheid, der sich als nicht richtig herausstellt, bereits gebüsst werden kann. Dies endet in einer Kriminalisierung aller Verantwortlichen.

- Verletzung der Sorgfaltspflichten (Art. 51 Abs. 1 lit. f und Abs. 2 VE-DSG)

  Wie in der EU-DSGVO sollte bei der Dokumentation der Datenverarbeitung in Art. 51 Abs. 1 lit. f VE-DSG auf die Führung eines Verzeichnisses verwiesen werden. Aus bereits genannten

Gründen ist der Tatbestand auf direkten Vorsatz zu beschränken und deshalb Art. 51 Abs. 2 VE-DSG zu streichen.

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

  Art. 52 VE-DSG ist zu streichen. Die berufliche Schweigepflicht ist spezialgesetzlich geregelt und sollte nicht wiederholt werden. Eine Wiederholung führt zu unnötigen Komplikationen und stellt einen Swiss Finish gegenüber der EU-DSGVO dar.

- Anwendbares Recht und Verfahren, und Verfolgungsverjährung für Übertretungen (Art. 54 und Art. 55 VE-DSG)

  Art. 54 und Art. 55 VE-DSG sind zu streichen, da die Sachverhalte bereits in der Strafprozessordnung geregelt sind.

Übergangsbestimmungen (Art. 59 VE-DSG) sind auszuweiten

Die Übergangsregelung ist von zentraler Bedeutung. Im VE-DSG sollte eine umfassende Übergangsfrist von zwei Jahren eingeräumt werden. Die Übergangsbestimmungen dürfen sich nicht nur auf einzelne Aspekte des Gesetztes beschränken. Auch die EU-DSGVO sieht eine Umsetzungsfrist von zwei Jahren für alle ihre Bereiche vor.

Sonstige zu berücksichtigende Anliegen

- Amtshilfe zwischen schweizerischen und ausländischen Behörden (Art. 47 Abs. 2 VE-DSG)

  Der Beauftragte kann ausländische Behörden, die für den Datenschutz zuständig sind, um die Bekanntgabe von Information ersuchen, und zu diesem Zweck mehrere Angaben zur Verfügung stellen. Es ist aber sicherzustellen, dass der Beauftragte dabei existierende Geheimhaltungsbestimmungen anderer Gesetze einhält und für den adäquaten Schutz der Daten verantwortlich ist. So sollten grundsätzlich Personendaten, die dem Bankgeheimnis unterstellt sind, nicht vom Beauftragten ausgehändigt werden können. Um dies zu gewährleisten, ist in Art. 47 Abs. 2 VE-DSG ein Buchstabe f mit der entsprechenden Pflicht zu ergänzen.

- Geldwäschereigesetz, Datenbanken und Akten in Zusammenhang mit der Meldepflicht (Art. 34 und Art. 34bis VE-GwG)

  Die FINMA konkretisiert das per anfangs 2016 in Kraft getretene revidierte Geldwäschereigesetz in ihrer gleichzeitig in Kraft getretenen Verordnung 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, 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 Präambel (19) der EU-DSGVO festgehaltenen Bestimmung, dass die Mitgliedstaaten Erlasse beschliessen können, welche die in der EU-DSGVO festgehaltenen Pflichten und Rechte beschränken, soweit dies zur Bekämpfung der Geldwäsche erforderlich und verhältnismässig ist.

Wir bedanken uns für die Gelegenheit zur Teilnahme an der Vernehmlassung und ersuchen Sie um wohlwollende Berücksichtigung. Detailliertere Kommentare zu einzelnen Artikeln des Entwurfs finden Sie im Anhang. Für weitergehende Erläuterungen und für Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Credit Suisse AG

Alberto Job
Head Data Management Switzerland

Dr. Andrae Lamprecht
Head Legislative Developments

ANHANG

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

Vorentwurf

Anmerkungen zum Vernehmlassungsentwurf

mit konkreten Änderungsvorschlägen

Zürich, 4. April 2017

Art.	Text	Änderungsvorschläge	Kommentare
	1. Abschnitt: Zweck, Geltungsbereich und Begriffe		
1	Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.		
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[3], 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 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. Fussnote: [3] SR 192.12		Hauptänderung ist die **Beschränkung des der Anwendbarkeit auf natürliche Personen. Juristische Personen** sind ausgenommen. Dies entspricht dem Konzept der EU-DSGVO und dem allgemeinen Wunsch der Wirtschaft, somit ist dies zu begrüssen. Die weiteren Änderungen betreffen die öffentliche Hand.
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;	[…]	Die meisten Änderungen können als Präzisierungen verstanden werden und sind zu begrüssen.

Art.	Text	Änderungsvorschläge	Kommentare
	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, 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; 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; i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	f. *Profiling*: jede automatisierte Auswertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale zu ~~analysieren~~ bewerten ~~oder Entwicklungen vorherzusagen~~, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder ~~Mobilität~~ Ortswechsel; […]	Abs. 1 lit. f: Wesentlich ist jedoch eine Schweizer Eigenheit: Die Definition von **Profiling** geht über die Vorgaben von der EU-DSGVO hinaus. Hier sollten wir uns an die Europäische Idee halten, ansonsten wir speziell für die **Schweiz eine weitergehende, aufwändige Lösung** haben, die in der Praxis viel Aufwand bedeutet und – aufgrund der Strafbestimmungen und Bussen – zu erheblichen Risiken für die Unternehmen führen. Deshalb wird empfohlen, die Anwendung auf „automatisierte“ Auswertungen einzuschränken. Das Inkludieren von «Daten», d.h. nicht personenbezogenen Daten, ist zu streichen. Der VE-DSG Begriff geht über die SEV 108 und die EU-DSGVO hinaus. Über eine Hintertür fallen nicht-personenbezogene Daten (z.B. technische Daten) plötzlich unter den VE-DSG. Das ist systemfremd. Die Bemerkung im Bericht, wonach «Daten, welche aufgrund eines Profilings entstehen, grundsätzlich Personendaten sind», ist falsch. Deshalb müssen «Daten» ersatzlos gestrichen werden. «Analysieren» ist mit «bewerten» zu ersetzen. Zu streichen – weil zu unbestimmt – ist

Art.	Text	Änderungsvorschläge	Kommentare
			«Entwicklungen» vorauszusagen. Schliesslich ist der Begriff «Mobilität» durch «Ortwechsel» zu ersetzen (analog EU-DSGVO).
	2. Abschnitt: Allgemeine Datenschutzbestimmungen		
4	Grundsätze [1] Personendaten müssen rechtmässig bearbeitet werden. [2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. [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. [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. [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 besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.	[…] [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. [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, ausser es bestehen gesetzliche oder regulatorische Aufbewahrungspflichten. [5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind ~~und wenn nötig nachgeführt wurden~~. Diese Pflicht entfällt, wenn der diesbezügliche Aufwand für den Verantwortlichen erheblich und die Persönlichkeit nicht gefährdet ist. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten, ausser es bestehen gesetzliche oder regulatorische Aufbewahrungsvorschriften. [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 besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen.	Abs. 3: Wurde angepasst, um den Vorgaben der EU-DSGVO nachzukommen. Jedoch werden in der Schweiz nicht in der Gesetzgebung übliche Begriffe verwendet, die die Anwendung in der Praxis verkomplizieren. Abs. 4: Einführung einer Löschungsverpflichtung. Diese Pflicht sollte jedoch bezüglich gesetzlichen oder regulatorischen Aufbewahrungsverpflichtungen ergänzt werden. Unklar, was mit «in einer Form» gemeint ist. Franz. Text ist zudem anders formuliert. Abs. 5 Neue Pflicht zur Korrektur der Daten. Diese Pflicht kann sehr aufwändig sein, insbesondere wenn die Daten von der Person aufgrund eines Vertrages selbst zur Verfügung gestellt worden sind. Sie sollte eingeschränkt werden, damit aufwändige Massnahmen unterbleiben können. Ein Auftragsdatenbearbeiter kann nicht prüfen und sicherstellen, ob Personendaten richtig sind. Der Verantwortliche hat diese Pflicht. Abs. 5 VE-DSG ist durch die Formulierung des geltenden Art. 5 DSG ersetzen. Diese Bestimmung berücksichtigt mit «angemessenen Massnahmen» das Verhältnismässigkeitsprinzip. Abs. 6: Wieder verwendet der Gesetzestext neue Begriffe, die das Schweizer Recht nicht kennt. Hier sollte wiederum die übliche Schweizer Gesetzessprache verwendet werden. Zudem ist es fraglich ob der Schutzbedürfins bei Profiling wirklich eine Ausdrücklichkeit erfordert.
5	Bekanntgabe ins Ausland		Abs. 1 und Abs. 2 wurden getrennt, was nur

Art.	Text	Änderungsvorschläge	Kommentare
	[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 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.	~~[1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde.~~ […] [5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens 30 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. ~~[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.~~ […]	**Unklarheiten zum Anwendungsbereich** aufwirft (zum Beispiel, ob Abs. 1 unabhängig von Abs. 2 gilt). Abs. 1 führt nur zu Unklarheiten und sollte deshalb ersatzlos gestrichen werden. Es wurde ja nicht beabsichtigt, dass bei nicht schwerwiegender Gefährdung eine Bekanntgabe ins Ausland erlaubt ist. Abs. 3 Bst. c steht im Widerspruch zu Abs. 5: Warum muss der EDÖB über die Verwendung von standardisierten Garantien informiert werden, wenn er sie vorgängig genehmigt hat? Abs. 5: Der EDÖB soll nach 30 Tagen informieren. 6 Monate sind viel zu lang für Unternehmen. Abs. 6: Diese Pflicht zur Information des Beauftragten ist neu und bedeutet eine sehr hohe administrative Bürde für alle Unternehmen. Der Beauftragte wird mit solchen Informationen überhäuft werden, und nicht in der Lage sein, diese zu bearbeiten. Zudem ist diese Pflicht dem EU Recht fremd, somit ein **Swiss Finish**. Sie ist ersatzlos zu streichen. Zudem ist Abs. 6 unlogisch. Warum muss der

Art.	Text	Änderungsvorschläge	Kommentare
			EDÖB nur über die Verwendung von standardisieren Garantieren informiert werden, nicht aber über die Verwendung von spezifischen?
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.	[…] a. die betroffene Person ~~im Einzelfall~~ eingewilligt hat; […] c. die Bekanntgabe im Einzelfall ~~unerlässlich~~ massgeblich ist für: […] 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht, ~~oder~~ einer ~~Verwaltungsb~~ Behörde oder einer anderen mit der Aufsicht betrauten ausländischen Stelle; 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; […] ~~[2] Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.~~	Abs. 1 lit. a: Das Wort Einzelfall hat in der Praxis zu Unklarheiten in der Anwendung geführt. Meistens wird die Einwilligung für einen Zweck eingeholt und nicht für eine einzelne Übermittlung. Deshalb sollte es hier gestrichen werden. Abs.1 lit.c.: Die Beschränkung auf „unerlässlich“ hat sich als unpraktikabel erwiesen, womit diese Ausnahme faktisch nicht zur Verfügung stand. Eine Anpassung auf „massgeblich“ ist deshalb notwendig. Abs. 1 lit. c. Ziff.2: Besser sollte allgemein von einer „Behörde“ gesprochen werden, damit neben Verwaltungsbehörden z.B. auch Strafbehörden umfasst sind. Sodann sollte in Analogie zu Art. 42c FINMAG der Kreis auch um anderen ausländische Stellen erweitert werden, die mit Aufsichtsaufgaben betraut sind. Abs. 1 lit. d: «im Einzelfall» streichen Abs. 1 lit. f: Der Satz ist unklar und sollte deshalb verständlicher ausformuliert werden. Abs. 2: Diese Pflicht zur Information des Beauftragten ist neu und bedeutet eine sehr hohe administrative Bürde für alle Unternehmen. Der Beauftragte wird mit solchen Informationen überhäuft werden, und nicht in der Lage sein, diese zu bearbeiten. Zudem ist diese Pflicht dem EU Recht fremd, somit ein **Swiss Finish**. Sie ist ersatzlos zu streichen.
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	[…]	

Art.	Text	Änderungsvorschläge	Kommentare
	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.	[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. […]	Abs. 2: Streichen, da «weitere Pflichten» zu unbestimmt und potentiell zu weit. Präzisierung der Datensicherheit in der VO, wie bis anhin. Der Auftragsdatenbearbeiter kann nicht im Mass wie der Verantwortliche die Rechte der betroffenen gewährleisten. Er kann z.B. nicht dafür garantieren, dass die Daten richtig sind. Diese Pflicht hat der Verantwortliche. Abs. 3 geht über die Regelung in der EU-DSGVO hinaus. In der heutigen arbeitsteiligen Welt ist das Verlangen nach einer „vorgängigen schriftlichen Zustimmung“ nicht umsetzbar und führt zu einem Verbot einer Unterakkordanz. Dies kann nicht im Sinne des Gesetzgebers sein. Sollte diesem Ersuchen nicht Folge geleistet werden, ist es noch immer nicht klar, ob die Subakkordanz blanco von Anfang an zuggestimmt werden kann oder ob Fall zu Fall das Einverständnis eingeholt werden muss.
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.	~~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.~~	Dieser Artikel ist gut gemeint, aber schlecht in der Umsetzung. Das Ganze führt zu einer Parallel-Gesetzgebung durch den EDÖB. Gemäss Bericht sind die «Empfehlungen der guten Praxis» materielles Gesetz. Der EDÖB bekommt damit Rechtsetzungskompetenzen, die demokratisch nicht legitimiert sind. Er bekommt zu viel Macht. Ferner ist unklar, ob man die Empfehlungen anfechten kann.

Art.	Text	Änderungsvorschläge	Kommentare
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.	~~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.~~	Der deutsche und französische Gesetzestext stimmen nicht überein.
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.		
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.		
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. [4] Jeder Erbe kann verlangen, dass der Verantwortliche Daten des	[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	Abs. 1: Es stellt sich auch die Frage, was diese Einsichtsrecht beinhaltet. Dies kann unter Umständen mit sehr viel Aufwand verbunden sein. Ein solches Recht kostenlos anzubieten stellt eine erhebliche Belastung der Wirtschaft dar. Abs. 1 lit. a ist in der Praxis schwer umsetzbar. Wie soll der Verantwortliche feststellen ob die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat? Ist dies an der ersuchenden Person zu beweisen? Lit. a ist ersatzlos zu streichen. Abs. 2. Wie soll der Verantwortliche feststellen ob die die Person in einer faktischen Lebensgemeinschaft mit der verstorbenen Person lebte? Ist dies von der ersuchenden Person zu

Art.	Text	Änderungsvorschläge	Kommentare
	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.	eingetragener Partnerschaft lebten ~~oder mit ihr eine faktische Lebensgemeinschaft führten~~. [3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden. Entsprechende Strafbestimmungen finden keine Anwendung. [4] ~~Jeder Erbe~~ Die Erbgemeinschaft bzw. der alleinig Erbberechtigte kann verlangen, dass der Verantwortliche Daten 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; oder c. es bestehen gesetzliche oder regulatorische Aufbewahrungspflichten. […]	beweisen? Vorschlag: ersatzlos zu streichen oder aber präzisieren, wie der Verantwortliche solches kontrollieren kann. Abs. 3: Es stellt sich die Frage wie dieser Abschnitt sich im Verhältnis zu Art. 47 Bankengesetz stellt. Führt dies zu einer Straflosigkeit? Dies ist zu präzisieren. Abs. 4: Der Artikel schafft eine neue erbrechtliche Bestimmung die zu den Bestimmungen des ZGB in Widerspruch stehen können. So kommen alle direkten Nachfahren Einsichtsgesuche stellen, auch wenn der Erblasser eine andere Erbschaftsregelung erlassen hat. Es wäre zu begrüssen, wenn die erbrechtlichen Bestimmungen zur Anwendung kommen. Schliesslich müssen gesetzliche oder regulatorische Aufbewahrungspflichten dem Vernichtungswunsch entgegengehalten werden können. Und was macht man, wenn diverse Erben unterschiedliche Wünsche haben?
	3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters		Genereller Kommentar: Die Verwendung der Begriffe “Daten” und “Personendaten” ist nicht konsistent.
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. [3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.	[…] d. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger der	Neue Pflicht zur Information der betroffenen Person, jedoch kongruent zu den Bestimmungen der EU-DSGVO. Die Begriffe sind unklar. Es wird «Beschaffung» und «Bearbeitung» verwendet. Das Ganze ist nicht stringent formuliert. Ferner kann das Ziel, die Gesellschaft für den Datenschutz zu sensibilisieren (vgl. Bericht S. 56), nicht mittels solchen Informationspflichten, welche mit Strafe belegt sind, erreicht werden.

Art.	Text	Änderungsvorschläge	Kommentare
	[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. [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.	Personendaten. ~~[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.~~ ~~[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.~~ [5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person innerhalb von 3 Monaten ~~spätestens bei der Speicherung der Daten~~ informiert werden; oder werden die Daten beschafft, um mit der betroffenen Person zu kommunizieren, so muss die betroffene Person bei dem ersten Kontakt informiert werden; oder werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.	Abs. 3 ist eine weitere Pflicht im Fall von Abs. 2. Sollte deshalb dort integriert werden. Im Gesetzestext taucht mehrmals ein neuer Begriff «Empfänger» auf. Es ist nicht klar, was der Unterschied zw. «Empfänger» und «Dritten» ist. Ferner ist der ganze Absatz unklar formuliert. Er ist auch nicht klar, ob der Verantwortliche oder der Auftragsdatenbearbeiter informieren müssen. Abs. 4: Diese Vorschrift geht über die Regelung der EU-DSGVO hinaus und ist als **Swiss Finish** abzulehnen. Deshalb sollte der Absatz gestrichen werden. Im Übrigen führ dies zu einem erheblichen Mehraufwand. Der Absatz ist unklar formuliert sowie nicht kongruent mit dem franz. Text. Abs. 5. Diese Regelung ist viel strenger als die Regelung der EU-DSGVO und 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 EU-DSGVO ersetzt werden. In der EU-DSGVO ist der Anknüpfungspunkt nicht die „Speicherung“, sondern die „Beschaffung“. Zudem sieht GPDR 3 unterschiedliche Fälle vor, was zur Verbesserung der Verständlichkeit führt. Wir empfehlen deshalb die Regelung der EU-DSGVO (Art. 14.3.(a)-(c) EU-DSGVO) zu übernehmen. Unklar ist auch, wer informieren muss. Ferner ist Abs. 5 nicht praktikabel, Daten werden immer «gespeichert».
14	Ausnahmen von der Informationspflicht und Einschränkungen [1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt. [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	[…] [2] Zudem, werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, auch wenn: a. die ~~Speicherung~~ Beschaffung oder die Bekanntgabe der Daten ~~ausdrücklich~~	Neuer Artikel. Abs. 1 und Abs. 2 entsprechen EU-DSGVO. Abs. 2: In der EU-DSGVO, entfällt die Informationspflicht, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt auch wenn die Daten nicht bei der betroffenen Person beschafft werden. Wegen der separaten Behandlung in

Art.	Text	Änderungsvorschläge	Kommentare
	b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist. [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. [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.	im Gesetz oder in Regulierungen vorgesehen ist; oder […] c. die Daten dem [Amts- oder] Berufsgeheimnis unterliegen. [3] Der Verantwortliche kann die ~~Übermittlung der~~ Information~~en~~ einschränken, aufschieben oder darauf verzichten, wenn: […] c. die Information wurde von der betroffenen Person veröffentlicht oder ist allgemein zugänglich. [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;~~ […] [5] Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information gemäss Abs. 3 oder 4 wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen. [6] Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Massnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.	Abs. 2 von Fällen, in denen die Daten nicht von der betroffenen Person beschafft werden, ist es nicht klar, dass diese Ausnahme von der Informationspflicht im VE-DSG fehlt. Sollte präzisiert werden. Abs. 2 lit. a: "Speicherung" mit "Beschaffung" ersetzen. Zudem stehen zum Beispiel Banken 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. Abs. 2 lit. c: In der EU-DSGVO entfällt die Informationspflicht, wenn die Daten das Berufsgeheimnis unterliegen. Dies sollte zur Wahrung des Schweizer [Amts- und] Berufsgeheimnisses eingefügt werden. So werden zum Beispiel Banken von der FINMA angehalten, Hintergrundinformationen zu wirtschaftlich Berechtigten und Kunden zu sammeln. Sie dürfen diese Information jedoch nur eingeschränkt diesen Personen weiterleiten. Abs. 3 ist unklar formuliert und sollte präzisiert werden, insbesondere der Begriff «Übermittlung». Zudem sollte Abs. 3 ergänzt werden mit einem Absatz bezüglich bereits öffentlichen Daten. Abs. 1 ist diesbezüglich unklar. Abs. 4 lit. a. Swiss Finish betreffend Einbezug von Dritten. Dies sieht die EU-DSGVO nicht vor und sollte gestrichen werden. Abs. 5: Präzisieren, dass es sich auf Abs. 3 und 4 bezieht. Unter Art. 12 Abs. 5 EU-DSGVO können bei offenkundig unbegründeten oder exzessiven Anträgen Kosten verrechnen oder eine Antwort verweigern. Eine solche Möglichkeit sollte auch geschaffen werden.
15	Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung		Abs. 1. Formulierung «rechtliche Wirkungen oder

Art.	Text	Änderungsvorschläge	Kommentare
	[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. [2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern. [3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.		erhebliche Auswirkungen» ist zu unbestimmt und geht zu weit. Die Beispiele im Bericht überzeugen nicht, insbesondere nicht das Beispiel mit den Verkehrsbussen. Deshalb sind die Begriffe enger zu fassen. Abs. 2: Unklar, was der Verantwortliche dann mit der «Äusserung» der betroffenen Person machen muss bzw. soll.
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. [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.	[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 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. [3] 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 oder die Grundrechte der betroffenen Person besteht. [4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen ~~oder dem Auftragsbearbeiter~~ innerhalb von ~~drei Monaten~~ zwei Wochen nach Erhalt aller erforderlichen Informationen mit. Der Beauftrage hat dem Verantwortlichen schriftlich mitzuteilen, welche Massnahmen zu ergreifen ist. [5]Meldet der Beauftragte innert Frist keine Einwände an, so gilt die Datenschutz-Abschätzung ohne weiteres als genehmigt.	Es ist unklar, was ein erhöhtes Risiko für die Persönlichkeit darstellt. Somit ist der Anwendungsbereich offen. Er sollte eingegrenzt werden. Abs. 3 und 4 EU-DSGVO verlangt diese Anforderung nur von den Verantwortlichen und nicht von Auftragsdatenbearbeiter. Dieser Swiss Finish ist zu streichen. Zudem ist der Beauftrage im Gegensatz zur EU-DSGVO immer zu informieren statt nur bei hohen Risiken. Dies ist ein Swiss Finish das gestrichen werden soll. Der Beauftrage würde auch durch die Flut von Meldungen nicht in der Lage sein, seinen gesetzlichen Verpflichtungen nachzukommen. Abs. 4 Die bisherige Frist von 3 Monaten hat sich bei Fällen mit Auslandsbezug als äusserst nachteilig erwiesen, weshalb eine wesentliche Verkürzung nötig ist. Abs. 5 (neu) Es ist explizit festzuhalten, dass die Abschätzung als genehmigt gilt, wenn innert Frist keine Einwände geltend gemacht werden (Klärung der Folgen und Beschleunigung des sonst überlangen Verfahrens).

Art.	Text	Änderungsvorschläge	Kommentare
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. [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.	[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 hohen Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person. [4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über ~~eine unbefugte Datenbearbeitung oder~~ einen Verlust von Daten.	Neue Regelung. Grundsätzlich ähnlich wie EU-DSGVO, aber nicht gleich. Abs. 1 Die Pflicht sollte auf hohe Risiken eingeschränkt werden, ansonsten eine Flut von Meldungen zu erwarten sind. Abs. 4 ist nicht kongruent mit Abs. 1.
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.	[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 oder äquivalenter Methoden sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.	Geht weiter als EU-DSGVO. Auch der Auftragsbearbeiter ist verpflichtet, nicht nur der Verantwortliche. Sollte EU-DSGVO angepasst werden. Der Artikel ist zudem undeutlich formuliert.
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.	Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet: a. Sie führen ein Verzeichnis aller Verarbeitungsaktivitäten die ihrer Zuständigkeit unterliegen. ~~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,	Art. 19 Abs. 1 lit a: Anwendungsbereich unklar. Sollte wenn schon an Art. 30 EU-DSGVO angeglichen werden. Art. 19 Abs. 1 lit. b In der EU-DSGVO ist klar, dass diese Notifizierungen nur gemacht werden müssen, wenn die betroffene Person danach ersucht. Die referenzierten Artikel müssen sich somit auf alle Tatbestände referenzieren. Die Bedeutung des Begriffs «Empfängerinnen und Empfänger» ist unklar. Dem Auftragsdatenbearbeiter werden Pflichten auferlegt, die er von vornherein nicht erfüllen kann, weil er die erforderlichen Informationen gar nicht

Art.	Text	Änderungsvorschläge	Kommentare
		jeweils nach Artikel 25 Absatz 2 oder 34 Absatz 2, es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.	besitzt (z.B. Richtigkeit der Daten).
	4. Abschnitt: Rechte der betroffenen Person		
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. 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.	[…] b. die Kategorien der bearbeiteten Personendaten; […] f. wenn die Personendaten nicht bei der betroffenen Person erhoben werden, die verfügbaren Informationen 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~~ Bei automatisierten Einzelentscheidungen ~~,~~ erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung, soweit ihr dies nicht bereits mitgeteilt wurde. […] 7 Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern,	Abs. 2 lit. b: Unklare Formulierung. Es sollte präzisiert werden, dass die Information nur die Kategorien der bearbeiteten Personendaten beinhalten sollte. Dies wäre in Line mit Art. 15 lit. b EU-DSGVO Abs. 2 lit. f: Die Herkunft soll nur dann angegeben werden müssen, falls die Daten nicht bei der betroffenen Person erhoben wurden. Dies entspricht Art. 15 Abs. 1 lit. g EU-DSGVO. Abs. 2 lit. 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). Abs. 3: Diese Absatz geht weit über die Vorgaben der EU-DSGVO hinaus und enthält einen operativ sehr aufwendigen **Swiss Finish**. Die Ausweitung auf jede Datenbearbeitung ist ein Eingriff in die operative Führung eines jeden Unternehmens und zwingt das Unternehmen jede Entscheidung zu begründen. Alle Entscheidungen in einer Unternehmung sind schlussendlich immer auf Daten basierend, die auf Systemen gespeichert sind. Somit ist der Absatz der Vorgabe der EU-DSGVO anzugleichen. Unter Art. 12 Abs. 5 EU-DSGVO können bei offenkundig unbegründeten oder exzessiven Anträgen Kosten verrechnen oder eine Antwort verweigern. Eine solche Möglichkeit sollte auch

Art.	Text	Änderungsvorschläge	Kommentare
		aufgrund des Antrags tätig zu werden. Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.	geschaffen werden.
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.		Abs. 2: Der Unterschied zwischen den Begriffen Übermittlung und Bekanntgabe ist unklar.
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.		
	5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen		
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	[…] [2] Eine Persönlichkeitsverletzung liegt insbesondere vor: […] ~~d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.~~ […]	Art. 23 Abs. 2 lit. d ist eine Schweizer Spezialität (**Swiss Finish**). Die Relevanz von Profiling sollte wie in der EU-DSGVO auf automatisierte Einzelentscheidungen limitiert werden. Deshalb ist Art. 23 Abs. 2 lit. d ersatzlos zu streichen.

Art.	Text	Änderungsvorschläge	Kommentare
	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.	[3] ~~In der Regel~~ Es liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.	Abs. 3 «In der Regel» lässt eine Hintertür offen, dass ein Persönlichkeitsverletzung vorliegen kann.
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	[…] [2] Ein überwiegendes Interesse der bearbeitenden Person ist ~~möglicherweise~~ gegeben, wenn dieser insbesondere: […]	Abs. 2: Der Einleitungssatz des franz. Textes lautet anders.

Art.	Text	Änderungsvorschläge	Kommentare
	Öffentlichkeit beziehen.		
25	Rechtsansprüche [1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs[4]. 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. Fussnote:[4] SR 210		
	6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane		
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.		
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.		

Art.	Text	Änderungsvorschläge	Kommentare
	[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; 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.		
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.		
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:		

Art.	Text	Änderungsvorschläge	Kommentare
	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. [3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004[5] 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.	Text	Änderungsvorschläge	Kommentare
	Fussnote: [5] SR 152.3		
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.		
31	Angebot von Unterlagen an das Bundesarchiv [1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998[6] 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. Fussnote: [6] SR 152.1		
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; 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		

Art.	Text	Änderungsvorschläge	Kommentare
	sind nicht anwendbar.		
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.		
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[7]. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.		

Art.	Text	Änderungsvorschläge	Kommentare
	Fussnote: [7] SR 172.021		
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[8] 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. Fussnote: [8] SR 152.3		
36	Register [1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [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		
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)[9]. [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. Fussnote: [9] SR 172.220.1		
38	Wiederwahl und Beendigung der Amtsdauer		Abs. 1 Neu: Die/der Beauftragte darf nur zwei Mal wiedergewählt werden. Es ist fraglich was diese für

Art.	Text	Änderungsvorschläge	Kommentare
	[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.	~~[1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden.~~ […]	die Schweiz fremde Bestimmung für einen Nutzen hat. Ersatzlos streichen.
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.		
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.		
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	[…]	Der Beauftragte hat gegenüber heute breitere Ermittlungsbefugnisse in der Fall von Privaten Personen.

Art.	Text	Änderungsvorschläge	Kommentare
	notwendigen Unterlagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes[10]. [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. [4] Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten. [5] Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung. Fussnote: [10] SR 172.021	[3]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; […] [5] 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 Beauftrage auch die angezeigte Person über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung zu informieren.	Abs. 3: Im Gegensatz zur EU-DSGVO werden hier dem Beauftragten polizeiliche Befugnisse eingeräumt. Dieser **Swiss Finish** ist abzulehnen, bringt sie doch in der Praxis kaum mehr Erkenntnisse. Unklar ist auch, ob man z.B. die Versiegelung der Unterlagen verlangen kann (vgl. Kartellgesetz). Abs. 5 sollte die Interessen der angezeigten Person berücksichtigen. Zudem sollte die angezeigte Person auch das Recht haben, diese Informationen zu erhalten.
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.	Vorsorgliche Massnahmen [1] Der Beauftragte kann vorsorgliche Massnahmen ~~verfügen~~ beim zuständigen Zivilrichter beantragen, 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.~~	Zu Art.42 und 43 VE-DSG: Es ist unangebracht, dass der Beauftragte selbständig vorsorgliche Massnahmen im Verfahren nach VwVG verhängen kann. Ein Beauftragter könnte also u.a. Unternehmen die Kooperation mit ausländischen Behörden auf Jahre hin unterbinden – diese überschiessende Machtfülle ist befremdend und wäre eine schwere Bürde für die Wettbewerbsfähigkeit der hiesigen Wirtschaft. Beim DSG geht es nicht um Verwaltungsrecht, sondern um den Schutz der Persönlichkeit von natürlichen Personen, also letztlich um Privatrecht. Entsprechend sollte der Beauftragte seine Massnahmen vor dem Zivilrichter beantragen, wie die Privaten auch, wenn sie ihre DSG-Rechte durchsetzen möchten. Das Gleiche gilt ja auch für

Art.	Text	Änderungsvorschläge	Kommentare
			das SECO, wenn es mit einer AGB-Klausel nicht einverstanden ist. Auch hier muss der Zivilgerichtsweg beschritten werden. Es ist kein Grund ersichtlich, weshalb im DSG anderes gelten müsste.
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.	~~Verwaltungsm~~ Massnahmen [1] Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte ~~verfügen~~ dem zuständigen Gericht beantragen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden. [2] Der Beauftragte kann dem Gericht zudem beantragen, es sei ~~-~~die Bekanntgabe ins Ausland aufschieben oder zu 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.	Vgl. Bemerkungen zu Art. 42 und 43 vorstehend.
44	Verfahren [1] Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz[11]. [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. [4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten. Fussnote: [11] SR 172.021	Verfahren [1] Das Untersuchungsverfahren ~~sowie Verfügungen nach den Artikeln 42 und 43~~ richte~~n~~t sich nach dem Verwaltungsverfahrensgesetz[11]. [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. […]	Abs. 3: Der EDÖB erhält im Verfahren bereits sehr viel Macht. Der Entzug der aufschiebenden Wirkung ist nicht gerechtfertigt.
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.		Der Satz ist unverständlich. Geht es um die Anzeigepflicht von Bundesbehörden bei Kenntnisnahme von strafbaren Handlungen? Dann besteht diese Pflicht bereits und muss hier nicht wiederholt werden.
46	Amtshilfe zwischen schweizerischen Behörden [1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses		

Art.	Text	Änderungsvorschläge	Kommentare
	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.		
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;		Abs. 1 lit. f: Es ist nicht klar, was der Unterschied zw. «Empfänger» und «Dritten» ist. Abs. 2: Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Information ersuchen, und zu diesem Zweck, mehrere Angaben zur Verfügung stellen. Es ist aber sicherzustellen, dass er existierende Geheimhaltungsbestimmungen andere Gesetze einhält und für den adäquaten Schutz der Daten verantwortlich ist. So sollten grundsätzlich Personendaten, die dem Bankgeheimnis unterstellt

Art.	Text	Änderungsvorschläge	Kommentare
	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.	f. Der Beauftragte beurteilt, dass die Datenschutzgesetzgebung im Ausland, ein angemessener Schutz gewährleistet; oder der ausländische Behörde verpflichtet sich, durch andere Garantien und Datenschutzregeln, ein angemessener Datenschutz zu beachten, und der Beauftragte beurteilt diese als angemessen. Zudem muss der Beauftragte die Interessen der Personen, deren Informationen ausgehändigt werden sollen, berücksichtigen, insbesondere Verbleib der Daten in der Schweiz (z.B. der Wahrung eins Berufsgeheimnisses).	sind, nicht vom Beauftragten ausgehändigt werden können.
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.		Abs. 2: Es ist unklar, was mit «Feststellungen» gemeint ist.
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.		

Art.	Text	Änderungsvorschläge	Kommentare
	e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen. f. Er nimmt die ihm durch das Öffentlichkeitsgesetz[12] übertragenen Aufgaben wahr. Fussnote: [12] SR 152.3		
	8. Abschnitt: Strafbestimmungen		
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; 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. c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3). [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); 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, dies vorsätzlich unterlassen: a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren; b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach	Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten [1] Mit Busse bis zu ~~5~~100 000 Franken werden private Personen auf Antrag bestraft: […] b. die es ~~vorsätzlich~~ wider besseres Wissen 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 Absatz ~~Absätze~~ 2~~, 3 und 4~~ zu liefern. […] d. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 vorsätzlich zu informieren. [2] Mit Busse bis zu ~~5~~100 000 Franken werden private Personen bestraft, ~~wer~~ die ~~vorsätzlich~~ wider besseres Wissen: 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); […]	Art.50. Abs.1-3: Die Bussenhöhe steht in keinem Verhältnis zum potentiellen Unrechtsgehalt bzw. zur übrigen Rechtsordnung. Vergleichbare Sachverhalte sanktioniert Art. 150 FINFRAG mit höchstens Fr. 100 000. Dieser Rahmen trifft einen Privaten empfindlich und sollte auch hier Anwendung finden. Art. 50 Abs. 1 lit. b Ziffer 1: Art. 13 Abs. 1 und 2 sind zu integrieren (s. Kommentar unter diesem Artikel). Deshalb sollte der Verweis auch korrigiert werden. Art. 50 Abs. 1 lit. b Ziffer 2: Art. 13 Abs. 4 ist zu streichen (s. Kommentar unter diesem Artikel) Art. 50 Abs. 1 neue lit. d: Art. 50 Abs. 3 lit. b VE-DSG sollte hier integriert werden, da es keinen Grund gibt, diese Strafbestimmung in einem separaten Artikel aufzuführen. Zudem muss dieser Tatbestand wiederum auf Vorsätzlichkeit beschränken. Art. 50 Abs. 2 lit. a: Verweis auf Abs. 6 ist zu streichen (s. Kommentar unter diesem Artikel) Art. 50 Abs. 2: lit. d fehlt

Art.	Text	Änderungsvorschläge	Kommentare
	Artikel 17 Absatz 4 zu informieren. [4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	~~f. einer Verfügung des Beauftragten nicht Folge leistet.~~ [3] Mit Busse bis zu ~~5~~100 000 Franken werden private Personen auf Antrag bestraft, ~~dies~~ die es ~~vorsätzlich~~ wider besseres Wissen 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.~~	Art. 50 Abs. 2 lit. f: Art. 292 StGB reicht aus. Die VE-DSG-Bestimmung ist unverhältnismässig. Art. 50 Abs. 3 lit. b: Wurde nach oben verschoben, somit hier streichen. Art. 50 Abs. 4: Abs. 4 sollte ersatzlos gestrichen werden, ansonsten jeder Verantwortliche bei jedem Entscheid der sich als nicht richtig herausstellt bereist gebüsst werden kann. Dies führt zu einer Kriminalisierung aller Verantwortlichen.
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. [2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	Verletzung der Sorgfaltspflichten [1] Mit Busse bis zu ~~5~~150'000 Franken werden private Personen auf Antrag bestraft, die ~~vorsätzlich~~ wider besseres Wissen: a. unter Verstoss gegen Artikel 5 ~~Absätze~~ Absatz 1 ~~und 2~~ und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln; […] f. nicht ein Verzeichnis ~~ihre Datenbearbeitung nicht~~ nach Artikel 19 Buchstabe a führt ~~dokumentiert~~. ~~[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.~~	Zur Busshöhe vgl. Bemerkung bei Art. 50 Art. 51 Abs. 1 lit. a: Art. 5 Abs. 1 wird gemäss unserem Vorschlag gestrichen und würde dementsprechend auch hier obsolet (s. Kommentar unter diesem Artikel) Art. 51 Abs. 1 lit. f: lit. f: Sollte auf die Führung des Verzeichnisses wie in der EU-DSGVO verweisen. Art. 51 Abs. 2 sollte ersatzlos gestrichen werden, ansonsten jeder Verantwortliche bei jedem Entscheid, der sich als nicht richtig herausstellt, bereist gebüsst werden kann. Dies führt zu einer Kriminalisierung aller Verantwortlichen.
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;	~~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~~	Die Berufliche Schweigepflicht ist spezialgesetzlich geregelt und sollte nicht wiederholt werden. Dies führt nur zu unnötigen Komplikationen. Ist zu streichen. Zudem ist es ein **Swiss Finish** gegenüber der EU-DSGVO.

Art.	Text	Änderungsvorschläge	Kommentare
	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.	~~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.~~	
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[13] über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären. Fussnote: [13] SR 313.0		
54	Anwendbares Recht und Verfahren Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.	~~Anwendbares Recht und Verfahren~~ ~~Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.~~	Ist bereits in der STPO geregelt. Sollte keine eigene Regelung enthalten.
55	Verfolgungsverjährung für Übertretungen Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.	~~Verfolgungsverjährung für Übertretungen~~ ~~Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.~~	Ist bereits im **STGB Art. 109** geregelt. Sollte keine eigene Regelung enthalten. Der Artikel ist ersatzlos zu streichen.
	9. Abschnitt: Abschluss von Staatsverträgen		
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.		
	10. Abschnitt: Schlussbestimmungen		

Art.	Text	Änderungsvorschläge	Kommentare
57	Vollzug durch die Kantone [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.		
58	Aufhebung und Änderung anderer Erlasse Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.		
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.	Übergangsbestimmung Die Übergangsfrist für das ~~Zwei Jahre nach~~ Inkrafttreten dieses Gesetzes beträgt 2 Jahre. ~~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.~~	Die Umsetzung des ganzen Gesetzes soll innerhalb 2 Jahre erfolgen, nicht nur einzelne Teile. Auch die EU-DSGVO hat eine Umsetzungsfrist von 2 Jahre für alle Punkte.
60	Referendum und Inkrafttreten [1] Dieses Gesetz untersteht dem fakultativen Referendum. [2] Der Bundesrat bestimmt das Inkrafttreten.		
	Aufhebung und Änderung anderer Erlasse I Das Bundesgesetz vom 19. Juni 1992[14] über den Datenschutz wird aufgehoben. II Die nachstehenden Bundesgesetze werden wie folgt geändert: Fussnote: [14] SR 235.1		

Art.	Text	Änderungsvorschläge	Kommentare
	1. Bürgerrechtsgesetz vom 29. September 1952[15] Fussnote: [15] SR 141.0		
Art. 49a Abs. 1	[1] Das Bundesamt kann zur Erfüllung seiner Aufgaben nach diesem Gesetz Personendaten bearbeiten, einschliesslich besonders schützenswerter Personendaten über religiöse Ansichten, politische Tätigkeiten, die Gesundheit, Massnahmen der sozialen Hilfe und verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen. Dazu kann es eine Datenbank oder Akten führen.		
	2. Ausländergesetz vom 16. Dezember 2005[16] Fussnote: [16] SR 142.20		
Art. 101	*Bearbeitung von Personendaten* Das SEM, die zuständigen Ausländerbehörden der Kantone und, in seinem Zuständigkeitsbereich, das Bundesverwaltungsgericht können Personendaten, einschliesslich besonders schützenswerter Personendaten, von Ausländerinnen und Ausländern sowie von an Verfahren nach diesem Gesetz beteiligten Dritten bearbeiten oder bearbeiten lassen, soweit sie diese Daten zur Erfüllung ihrer gesetzlichen Aufgaben benötigen.		
Art. 111d Abs. 2 Bst. a und b	[2] In Abweichung von Absatz 1 dürfen einem Drittstaat in folgenden Fällen Personendaten bekannt gegeben werden: a. die betroffene Person hat ihre Einwilligung nach Artikel 4 Absatz 6 des Datenschutzgesetzes vom ... (DSG)[17] erteilt; b. die Bekanntgabe ist erforderlich, 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; Fussnote: [17] SR ...		
Art. 111f zweiter Satz	*Aufgehoben*		
	3. Asylgesetz vom 26. Juni 1998[18] Fussnote: [18] SR 142.31		
Art. 96 Abs. 1	[1] Das SEM, die Beschwerdebehörden sowie die mit Aufgaben nach diesem Gesetz beauftragten privaten Organisationen können Personendaten,		

Art.	Text	Änderungsvorschläge	Kommentare
und 6	einschliesslich besonders schützenswerter Personendaten nach Artikel 3 Buchstabe c des Datenschutzgesetzes vom … (DSG)[19] einer asylsuchenden oder schutzbedürftigen Person und ihrer Angehörigen bearbeiten oder bearbeiten lassen, soweit sie diese zur Erfüllung ihrer gesetzlichen Aufgaben benötigen. Fussnote: [19] SR ...		
Art. 99 Abs. 6 erster Satz	[6] Ohne die Zustimmung des Verantwortlichen dürfen einem Drittstaat keine Personendaten bekanntgegeben werden, die nach Absatz 4 übermittelt wurden.		
Art. 99a Abs. 2 Bst. a	[2] MIDES dient: a. der Bearbeitung von Personendaten von Asylsuchenden und Schutzbedürftigen, einschliesslich besonders schützenswerter Personendaten nach Artikel 3 Buchstabe c DSG[20]; und Fussnote: [20] SR ...		
Art. 100 Abs. 2	[2] Diese Informationssysteme können besonders schützenswerte Personendaten enthalten, soweit dies zur Erfüllung der gesetzlichen Aufgabe notwendig ist.		
Art. 102 Abs. 1 dritter Satz und Abs. 2	[1] … Sofern es erforderlich ist, können auch in den Texten enthaltene Personendaten, namentlich Personalien, sowie besonders schützenswerte Personendaten gespeichert werden. [2] Auf Datenbanken und Akten, die besonders schützenswerte Personendaten enthalten, haben nur Mitarbeiterinnen und Mitarbeiter des SEM und des Bundesverwaltungsgerichts Zugriff.		
Art. 102c Abs. 2 Einleitungssatz und Bst. a und b	[2] Gewährleistet ein Drittstaat keinen angemessenen Schutz der Daten, so können ihm in besonderen Fällen Personendaten bekannt gegeben werden, wenn: a. die betroffene Person ihre Einwilligung nach Artikel 4 Absatz 6 des Datenschutzgesetzes vom … (DSG)[21] erteilt hat; b. die Bekanntgabe erforderlich 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; Fussnote: [21] SR		

Art.	Text	Änderungsvorschläge	Kommentare
	...		
Art. 102e zweiter Satz	*Aufgehoben*		
	4. Bundesgesetz vom 20. Juni 2003 über das Informationssystem für den Ausländer- und den Asylbereich[22] Fussnote: [22] SR 142.51		
Art. 4 Abs. 2	[2] Im Informationssystem können besonders schützenswerte Personendaten nach Artikel 3 Buchstabe c des Datenschutzgesetzes vom … (DSG)[23] bearbeitet werden, soweit dies zur Erfüllung der Aufgaben nach Artikel 3 unerlässlich ist. Fussnote: [23] SR ...		
	5. Öffentlichkeitsgesetz vom 17. Dezember 2004[24] Fussnote: [24] SR 152.3		
Art. 7 Abs. 2 und 3	[2] Der Zugang zu amtlichen Dokumenten wird eingeschränkt, aufgeschoben oder verweigert, wenn durch seine Gewährung die Privatsphäre Dritter beeinträchtigt werden kann. [3] In Abweichung von Absatz 2 kann die Behörde ausnahmsweise den Zugang zu amtlichen Dokumenten gewähren, wenn ein überwiegendes öffentliches Interesse am Zugang besteht.		
Art. 11 Abs. 1	[1] Zieht die Behörde in Erwägung, den Zugang zu Dokumenten zu gewähren, die Personendaten von Dritten enthalten, oder Artikel 7 Absatz 3 anzuwenden, gibt sie den betroffenen Dritten die Gelegenheit zur Stellungnahmen innert zehn Tagen.		
Art. 12 Abs. 3	[3] Die Behörde schiebt den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, oder den Zugang nach Artikel 7 Absatz 3 bis zur Klärung der Rechtslage auf.		
Art. 15 Abs. 2 Bst. c (neu)	[2] Im Übrigen erlässt die Behörde eine Verfügung, wenn sie in Abweichung von der Empfehlung: c. nach Artikel 7 Absatz 3 den Zugang zu einem amtlichen		

Art.	Text	Änderungsvorschläge	Kommentare
	Dokument gewähren will.		
	6. Verwaltungsverfahrensgesetz vom 20. Dezember 1968[25] *Vor dem Titel des Vierten Abschnitts einfügen* Fussnote: [25] SR 172.021		
Art. 71a	O. Schutz von Personendaten [1] Die datenschutzrechtlichen Ansprüche werden im hängigen Beschwerdeverfahren beurteilt und unterliegen den entsprechenden Rechtsmitteln. [2] Die Datenbearbeitung durch die Beschwerdeinstanz im Rahmen eines Beschwerde- oder Revisionsverfahrens ist von der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten ausgenommen.		
	7. Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997[26] Fussnote: [26] SR 172.010		
Art. 57h Abs. 1 zweiter Satz	[1] … Dieses System kann besonders schützenswerte Personendaten enthalten, die sich aus dem Schriftverkehr oder aus der Art des Geschäftes ergeben. ….		
Art. 57j Abs. 2	[2] ... Die Datenbearbeitung nach diesem Abschnitt kann auch besonders schützenswerte Personendaten umfassen.		
Art. 57l Bst. b Ziff. 4	Die Bundesorgane dürfen Personendaten, die bei der Nutzung der elektronischen Infrastruktur anfallen, zu folgenden Zwecken aufzeichnen: b. Daten über die Nutzung der elektronischen Infrastruktur: 4. zum Nachvollzug des Zugriffs auf die elektronische Infrastruktur,		
	8. Bundespersonalgesetz vom 24. März 2000[27] Fussnote: [27] SR 172.220.1		

Art.	Text	Änderungsvorschläge	Kommentare
Art. 27 Abs. 2, Einleitungssatz und Bst. b	[2] Die Ausführungsbestimmungen regeln im Rahmen des Datenschutzgesetzes vom …[28]: b. die Voraussetzungen und die Zuständigkeit für die Bearbeitung besonders schützenswerter Personendaten nach Artikel 3 Buchstabe c des Datenschutzgesetzes vom … (DSG); die Bearbeitung dieser Daten ist nur zulässig, sofern sie für die Personalentwicklung notwendig ist und die betroffene Person ihr schriftlich zugestimmt hat; Fussnote: [28] SR ...		
Art. 27d Abs. 2 und Abs. 4 Einleitungssatz	[2] Die PSB kann die folgenden für die Erfüllung ihrer Aufgaben notwendigen besonders schützenswerten Personendaten der Klientinnen und Klienten bearbeiten: [4] Die PSB kann den folgenden Personen und Stellen die in Absatz 2 genannten besonders schützenswerten Personendaten zugänglich machen, sofern sie diese für die Erfüllung ihrer Aufgaben benötigen:		
	9. Zivilgesetzbuch[29] Fussnote: [29] SR 210		
Art. 45a Abs. 3 Ziff. 3 und Abs. 4	[3] Der Bundesrat regelt im Rahmen des Gesetzes und unter Mitwirkung der Kantone: 3. die zur Sicherstellung des Datenschutzes und der Datensicherheit erforderlichen organisatorischen und technischen Massnahmen sowie die Aufsicht über die Einhaltung der Datenschutzvorschriften, [4] Der Bundesrat kann die Ansprüche der betroffenen Personen ganz oder teilweise abweichend von Artikel 34 Absätze 1-3 des Datenschutzgesetzes vom …[30] regeln, wenn der Zweck der zentralen Datenbank dies erfordert. Fussnote: [30] SR ...		
	10. Bundesgesetz vom 24. März 2000 über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten[31]		

Art.	Text	Änderungsvorschläge	Kommentare
	Fussnote: [31] SR 235.2		
Art. 1 zweiter Satz	[1]… Die Bearbeitung von besonders schützenswerten Personendaten und das Profi- ling sind zulässig.		
Art. 2 Abs. 1 und Abs. 2 erster Satz	[1] Zur Planung und Durchführung der Einsätze für die Friedensförderung, die Stärkung der Menschenrechte und die humanitäre Hilfe können die zuständigen Stellen des Departements über die an solchen Einsätzen beteiligten Personen eine Datenbank oder Akten führen. [2] Die Bearbeitung von besonders schützenswerten Personendaten und das Profiling sind für diesen Zweck zulässig.		
Art. 5 Abs. 1 Einleitungssatz	[1] Zur Erfüllung der völkerrechtlichen Verpflichtungen der Schweiz führen das Staatssekretariat und die ständige Mission der Schweiz bei den internationalen Organisationen in Genf Datenbanken und Akten über:		
Art. 6 Bst. a	Der Bundesrat erlässt Ausführungsbestimmungen über: a. Organisation und Betrieb der Datenbanken und die Aktenführung;		
	11. Zivilprozessordnung[32] Fussnote: [32] SR 272		
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 …[33], Fussnote: [33] SR ...		
Art. 99 Abs. 3 Bst. d	[3] Keine Sicherheit ist zu leisten: d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom … 3 4 .		

Art.	Text	Änderungsvorschläge	Kommentare
	Fussnote: [34] SR ...		
Art. 113 Abs. 2 Bst. g	[2] Keine Gerichtskosten werden gesprochen in Streitigkeiten: g. nach dem Datenschutzgesetz vom …[35]. Fussnote: [35] SR ...		
Art. 114 Bst. f	Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten: f. nach dem Datenschutzgesetz vom …[36]. Fussnote: [36] SR ...		
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 …[37]; Fussnote: [37] SR ...		
	12. Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht[38] Fussnote: [38] SR 291		
Art. 130 Abs. 3	Klagen zur Durchsetzung eines Auskunfts- oder Einsichtsrechts im Zusammenhang mit der Bearbeitung von Personendaten können bei den in Artikel 129 genannten Gerichten oder bei den schweizerischen Gerichten am Ort, wo der betreffende Vorgang stattfindet, eingereicht werden.		
	13. Strafgesetzbuch[39] Fussnote: [39] SR 311.0		
Art. 179novies	Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.	~~Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.~~	Diese Bestimmung ist ersatzlos zu streichen. Die ist technologiefeindlich und behindert jegliche Innovation.

Art.	Text	Änderungsvorschläge	Kommentare
Art. 179decies	*Vor dem 4. Titel einfügen* 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.		
	14. Bundesgesetz vom 22. März 1974 über das Verwaltungsstrafrecht[40] *Gliederungstitel nach Art. 18* **Dritter Abschnitt: Schutz von Personendaten** *Nach dem Gliederungstitel des 3. Abschnitts die Artikel 18a–18g einfügen* Fussnote: [40] SR 313.0		
Art. 18a	A. Schutz von Personendaten I. Beschaffung von Personendaten [1] Personendaten sind bei der betroffenen Person oder für diese erkennbar zu beschaffen, wenn dadurch das Verfahren nicht gefährdet oder unverhältnismässig aufwendig wird. [2] Erfolgte die Beschaffung von Personendaten ohne Wissen der betroffenen Person, so ist diese umgehend darüber zu informieren. Die Information kann zum Schutze überwiegender öffentlicher oder privater Interessen unterlassen oder aufgeschoben werden.		
Art. 18b	II. Bearbeitung von Personendaten Bei der Bearbeitung von Personendaten sieht die Verwaltungsbehörde des Bundes angemessene Massnahmen vor, damit so weit wie möglich unterschieden werden zwischen: a. verschiedenen Kategorien betroffener Personen; b. auf Fakten und auf persönlichen Einschätzungen beruhenden Personendaten.		
Art. 18c	III. Bekanntgabe und Verwendung von Personendaten bei hängigem Strafverfahren Die Verwaltungsbehörde des Bundes darf Personendaten aus einem hängigen Verwaltungsstrafverfahren zur Verwendung in einem anderen		

Art.	Text	Änderungsvorschläge	Kommentare
	hängigen Verfahren bekannt geben, wenn anzunehmen ist, dass die Personendaten wesentliche Aufschlüsse zum Sachverhalt geben können.		
Art. 18d	IV. Auskunftsrechte bei hängigem Verfahren Solange ein Verfahren hängig ist, haben die Parteien und die anderen Verfahrensbeteiligten nach Massgabe des ihnen zustehenden Akteneinsichtsrechts das Recht auf Auskunft über die sie betreffenden Personendaten.		
Art. 18e	V. Richtigkeit der Personendaten [1] Die Verwaltungsbehörde des Bundes berichtigt unverzüglich unrichtige Personendaten. [2] Sie benachrichtigt die Behörde, die ihr die Personendaten übermittelt oder bereitgestellt oder der sie diese bekannt gegeben hat, unverzüglich über die Berichtigung.		
Art. 18f	Ansprüche und Verfahren VI. Ansprüche und Verfahren [1] Die datenschutzrechtlichen Ansprüche werden im hängigen Verwaltungsstrafverfahren beurteilt und unterliegen den entsprechenden Rechtsmitteln. [2] Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte ist für die Aufsicht über die Datenbearbeitung durch die Verwaltungsbehörde des Bundes in diesem Verfahren nicht zuständig, bis der Endentscheid nicht in Rechtskraft erwachsen ist.		
	15. Militärstrafprozess vom 23. März 1979[41] *Gliederungstitel nach Art. 25* **Sechstes Kapitel: Schutz von Personendaten** *Nach dem Gliederungstitel des 6. Kapitels die Artikel 25a–25e einfügen* Fussnote: [41] SR 322.1		
Art. 25a	Beschaffung von Personendaten [1] Personendaten sind bei der betroffenen Person oder für diese erkennbar zu beschaffen, wenn dadurch das Verfahren nicht gefährdet oder unverhältnismässig aufwendig wird. [2] Erfolgte die Beschaffung von Personendaten ohne Wissen der		

Art.	Text	Änderungsvorschläge	Kommentare
	betroffenen Person, so ist diese umgehend darüber zu informieren. Die Information kann zum Schutze überwiegender öffentlicher oder privater Interessen unterlassen oder aufgeschoben werden.		
Art. 25b	Bearbeitung von Personendaten Bei der Bearbeitung von Personendaten sieht die militärische Strafbehörde angemessene Massnahmen vor, damit so weit wie möglich unterschieden werden kann zwischen: a. verschiedenen Kategorien betroffener Personen; b. auf Fakten und auf persönlichen Einschätzungen beruhenden Personendaten.		
Art. 25c	Bekanntgabe und Verwendung von Personendaten bei hängigem Strafverfahren Die militärische Strafbehörde darf aus einem hängigen militärischen Strafverfahren Personendaten zwecks Verwendung in einem anderen hängigen Verfahren bekannt geben, wenn anzunehmen ist, dass die Personendaten wesentliche Aufschlüsse zum Sachverhalt geben können.		
Art. 25d	Auskunftsrechte bei hängigem Verfahren Solange ein Verfahren hängig ist, haben die Parteien und die anderen Verfahrensbeteiligten nach Massgabe des ihnen zustehenden Akteneinsichtsrechts das Recht auf Auskunft über die sie betreffenden Personendaten.		
Art. 25e	Richtigkeit der Personendaten [1] Die militärische Strafbehörde berichtigt unverzüglich unrichtige Personendaten. [2] Sie benachrichtigt die Behörde, die ihr diese Personendaten übermittelt oder bereitgestellt oder der sie diese bekannt gegeben hat, unverzüglich über die Berichtigung.		
	16. Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes [42] Fussnote: [42] SR 361		
Art. 3 Abs. 2	[2] Im Rahmen dieses Gesetzes sind die Polizeibehörden des Bundes zur Bearbeitung besonders schützenswerter Personendaten sowie zum Profiling befugt und dürfen den kanonalen Polizei- und		

Art.	Text	Änderungsvorschläge	Kommentare
	Strafverfolgungsbehörden sowie anderen schweizerischen oder ausländischen Behörden solche Daten bekannt geben. Personendaten dürfen bearbeitet werden, soweit und solange es zur Erfüllung der gesetzlichen Aufgaben notwendig ist.		
Art. 5 Sachüberschrift Abs. 2	Datenbearbeitung zur internen Kontrolle *Aufgehoben*		
	17. ETH-Gesetz vom 4. Oktober 1991[43] Fussnote: [43] SR 414.110		
Art. 36a Abs. 1 erster Satz	[1] Der ETH-Rat, die ETH und die Forschungsanstalten betreiben je ein Personalinformationssystem, in welchem auch besonders schützenswerte Personendaten bearbeitet werden können.		
Art. 36b Abs. 1 und 5 zweiter Satz	[1] Jede ETH betreibt für die Verwaltung der Daten der Studienanwärter, Studierenden, Doktoranden und Hörer ein Informationssystem, in dem auch besonders schützenswerte Personendaten bearbeitet werden können. [5] ... Die Bekanntgabe besonders schützenswerter Personendaten durch ein Abrufverfahren ist nur an die für die Studienadministration zuständigen Stellen innerhalb jeder ETH gestattet.		
	18. Sportförderungsgesetz vom 17. Juni 2011[44] Fussnote: [44] SR 415.0		
Art. 21 Abs. 3 Einleitungssatz	[3] Die Dopingkontrollstellen nach Absatz 2 sind berechtigt, die im Zusammenhang mit ihrer Kontrolltätigkeit erhobenen Personendaten, einschliesslich besonders schützenswerter Personendaten, zu bearbeiten und an die zuständige Stelle weiterzuleiten für:		
Art. 25 Abs. 1 Einleitungssatz	[1] Die nach Artikel 19 für Massnahmen gegen Doping zuständige Stelle ist berechtigt, Personendaten, einschliesslich besonders schützenswerter Personendaten, zum Zweck der Dopingbekämpfung mit anerkannten ausländischen oder internationalen Dopingbekämpfungsstellen auszutauschen, wenn ein solcher Datenaustausch notwendig ist:		
	19. Bundesgesetz vom 17. Juni 2011 über die Informationssysteme des Bundes im Bereich Sport[45] Fussnote: [45] SR 415.1		

Art.	Text	Änderungsvorschläge	Kommentare
Art. 1 Einleitungssatz	Dieses Gesetz regelt die Bearbeitung von besonders schützenswerten Personendaten (Daten) in Informationssystemen des Bundesamtes für Sport (BASPO) durch:		
	20. Bundesstatistikgesetz vom 9. Oktober 1992[46] Fussnote: [46] SR 431.01		
Art. 4 Abs. 4	[2] Bei Erhebungen im Rahmen dieses Gesetzes gibt der Bund den Zweck, die Rechtsgrundlage für die Bearbeitung, die Kategorien der an der Datenbank Beteiligten und die Datenempfänger bekannt.		
Art. 7 Abs. 2 erster Satz	[2] Er kann dabei die Übernahme von Daten aus ihren Datenbanken anordnen, sofern die Rechtsgrundlage der Datenbank die Verwendung für statistische Zwecke nicht ausdrücklich ausschliesst.		
Art. 10 Abs. 4	[4] Die Verwaltungseinheiten sowie, nach Massgabe ihrer Unterstellung nach Artikel 2 Absatz 3, die übrigen Organisationen liefern dem Bundesamt zur Erfüllung seiner Aufgaben die Ergebnisse und Grundlagen ihrer Statistiktätigkeit und, falls erforderlich, Daten aus ihren Datenbanken, Akten und Erhebungen.		
Art. 12 Abs. 2	[2] Das Bundesamt wirkt auf eine Koordination mit den kantonalen Statistiken hin, insbesondere um die Erhebungsprogramme aufeinander abzustimmen und Register oder andere Bearbeitungssysteme im Hinblick auf die statistische Bearbeitung zu harmonisieren.		
	21. Bundesgesetz vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer[47] Fussnote: [47] SR 431.03		
Art. 3 Abs. 1 Bst. d	[1] In diesem Gesetz gelten als: d. Verwaltungseinheiten von Bund, Kantonen und Gemeinden, öffentlichrechtliche Anstalten sowie mit öffentlich-rechtlichen Aufgaben betraute private Einrichtungen, die Datenbanken und Akten über UID-Einheiten aufgrund von deren wirtschaftlicher Tätigkeit führen;		
Art. 5 Abs. 1	[1] Die UID-Stellen müssen die UID: b. in ihren Datenbanken und Akten führen		

Art.	Text	Änderungsvorschläge	Kommentare
Bst. b			
	22. Nationalbibliotheksgesetz vom 18. Dezember 1992[48] Fussnote: [48] SR 432.21		
Art. 2 Abs. 2	[2] Sie verzeichnet öffentlich zugängliche Datenbanken oder andere Sammlungen, die einen Bezug zur Schweiz aufweisen.		
Art. 7	*Sachüberschrift und Einleitungssatz* *Verzeichnung von Datenbanken* Die Nationalbibliothek verzeichnet die öffentlich zugänglichen Datenbanken oder andere Sammlungen, die:		
	23. Tierschutzgesetz vom 16. Dezember 2005[49] Fussnote: [49] SR 455		
Art. 20c Abs. 1 zweiter Satz	[1] Die folgenden Personen dürfen im Rahmen ihrer gesetzlichen Aufgaben Personendaten, einschliesslich besonders schützenswerter Personendaten, bearbeiten und im Abrufverfahren auf diese Daten zugreifen:		
	24. Militärgesetz vom 3. Februar 1995[50] Fussnote: [50] SR 510.10		
Art. 31 Abs. 2	[2] Der Bund unterhält die entsprechenden Dienste. Diese dürfen Personendaten, einschliesslich besonders schützenswerter Personendaten, bearbeiten, soweit und solange es ihre Aufgaben erfordern.		
Art. 99 Abs. 2 erster Satz und 3 Bst. d	[2] Er ist zur Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Personendaten, und zum Profiling befugt, gegebenenfalls ohne Wissen der betroffenen Personen, soweit und solange es seine Aufgaben erfordern. ... [3] Der Bundesrat regelt: d. die Ausnahmen von den Vorschriften über die Registrierung von Datenbearbeitungstätigkeiten, wenn diese die Informationsbeschaffung gefährden würde		
Art. 100 Abs. 2 erster Satz und	[2] Er ist zur Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Personendaten, und zum Profiling befugt, soweit und solange es seine Aufgaben erfordern. ...		

Art.	Text	Änderungsvorschläge	Kommentare
3 Bst. d	[3] Der Bundesrat regelt: d. für den Fall des Assistenz- oder des Aktivdienstes die Ausnahmen von den Vorschriften über die Registrierung der Datenbearbeitungstätigkeiten, wenn diese die Informationsbeschaffung gefährden würde;		
Art. 146	Die Bearbeitung von besonders schützenswerten Personendaten sowie das Profiling in Informationssystemen und beim Einsatz von Überwachungsmitteln der Armee und der Militärverwaltung wird im Bundesgesetz vom 3. Oktober 2008 über die militärischen Informationssysteme[51] geregelt. Fussnote: [51] SR 510.91		
	25. Bundesgesetz vom 3. Oktober 2008 über die militärischen Informationssysteme[52] Fussnote: [52] SR 510.91		
Art. 1 Abs. 1	*Einleitungssatz* [1] Dieses Gesetz regelt die Bearbeitung von besonders schützenswerten Personendaten und das Profiling in Informationssystemen und beim Einsatz von Überwachungsmitteln der Armee und der Militärverwaltung durch:		
Art. 11 Abs. 2	[2] Daten zum Profiling werden spätestens gelöscht: a. bei der Entlassung aus der Militärdienstpflicht; oder b. fünf Jahre nach Beendigung der Anstellung bei der Gruppe Verteidigung.		
	26. Kriegsmaterialgesetz vom 13. Dezember 1996[53] Fussnote: [53] SR 514.51		
Art. 30 Abs. 2 zweiter Satz	[2] ... Soweit und solange es ihre Aufgaben erfordern, ist sie zur Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Personendaten, und zum Profiling befugt.		
	27. Waffengesetz vom 20. Juni 1997[54]		

Art.	Text	Änderungsvorschläge	Kommentare
	Fussnote: [54] SR 514.54		
Art. 32e Abs. 2 Bst. a und b	[2] Gewährleistet ein Drittstaat keinen angemessenen Schutz der Daten, so können ihm in besonderen Fällen Personendaten bekannt gegeben werden, wenn: a. die betroffene Person ihre Einwilligung nach Artikel 4 Absatz 6 des Datenschutzgesetzes vom … (DSG)[55] erteilt hat; b. wenn die Bekanntgabe erforderlich 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 oder wenn ... Fussnote: [55] SR ...		
Art. 32g zweiter Satz	*Aufgehoben*		
	28. Bevölkerungs- und Zivilschutzgesetz vom 4. Oktober 2002[56] Fussnote: [56] SR 520.10		
Art. 72 Abs. 1 und 1bis	[1] Das BABS bearbeitet zur Erfüllung seiner Aufgaben nach diesem Gesetz Personendaten von Schutzdienstpflichtigen im Zentralen Zivilschutz-Informationssystem. Es ist dabei befugt: a. zur Bearbeitung von Daten über die Gesundheit; b. für Entscheide über die Zuteilung der Grundfunktion oder zur Abklärung des Kaderpotenzials zum Profiling im Sinne von Artikel 3 Buchstabe f des Datenschutzgesetzes vom …[57]. [1bis] Es bearbeitet die Personendaten von Kursteilnehmenden zur Durchführung der Ausbildungen im Veranstaltungsadministratorsystem. Es ist dabei befugt: a. zur Bearbeitung von Daten über die Gesundheit; b. zum Profiling für die Beurteilung der Eignung für eine Kader- oder Spezialistenfunktion. Fussnote: [57] SR ...		
	29. Finanzhaushaltsgesetz vom 7. Oktober 2005[58]		

Art.	Text	Änderungsvorschläge	Kommentare
	Fussnote: [58] SR 611.0		
Art. 60c Abs. 1 Einleitungssatz und Absatz 3	[1] Die SKB bearbeitet in Papierform und in einem Informationssystem die Daten, einschliesslich besonders schützenswerter Personendaten, ihrer Kundinnen und Kunden, die sie zur Erfüllung ihrer Aufgabe benötigt, namentlich um: [3] Die Angestellten der SKB können für die Erfüllung ihrer Aufgaben Personendaten, einschliesslich besonders schützenswerter Personendaten, an ihre direkten Vorgesetzten weitergeben, auch wenn diese nicht Angestellte der SKB sind.		
	30. Finanzkontrollgesetz vom 28. Juni 1967[59] Fussnote: [59] SR 614.0		
Art. 10 Abs. 3	[3] Die Verwaltungseinheiten des Bundes räumen der Eidgenössischen Finanzkontrolle das Recht ein, im Abrufverfahren auf die für die Wahrnehmung der Finanzaufsicht erforderlichen Daten zuzugreifen. Bei Bedarf erstreckt sich das Zugriffsrecht auch auf besonders schützenswerte Personendaten. Die Eidgenössische Finanzkontrolle darf die ihr derart zur Kenntnis gebrachten Personendaten nur bis zum Abschluss des Revisionsverfahrens speichern. Die Zugriffe auf die verschiedenen Systeme und die damit verfolgten Zwecke müssen protokolliert werden.		
	31. Zollgesetz vom 18. März 2005[60] Fussnote: [60] SR 631.0		
Art. 110 Abs. 1	[1] Die EZV darf Personendaten, einschliesslich besonders schützenswerter Personendaten, bearbeiten, sofern dies für den Vollzug der von ihr anzuwendenden Erlasse notwendig ist.		
Art. 110a Abs. 3 Bst. b	[3] Im Informationssystem dürfen folgende besonders schützenswerten Personendaten bearbeitet werden: b. Angaben zur Religionszugehörigkeit, falls dies ausnahmsweise für die Strafverfolgung erforderlich ist;		
Art. 112 Abs. 2 Einleitungssatz	[2] Es dürfen namentlich folgende Daten und Datenverbindungen, einschliesslich besonders schützenswerter Personendaten, bekannt gegeben werden: [4] Die EZV darf die folgenden Daten den nachfolgend genannten		

Art.	Text	Änderungsvorschläge	Kommentare
und Abs. 4 Bst. b	Behörden im Abrufverfahren zugänglich machen, sofern die Daten für den Vollzug der von diesen Behörden anzuwendenden Erlasse notwendig sind: b. *aufgehoben*		
Art. 113	*Bekanntgabe an ausländische Behörden* Die EZV darf Behörden anderer Staaten sowie supranationaler und internationaler Organisationen (ausländische Behörden) Daten, einschliesslich besonders schützenswerter Personendaten, im Einzelfall oder im Abrufverfahren nur bekannt geben, sofern ein völkerrechtlicher Vertrag dies vorsieht.		
Art. 114 Abs. 2	[2] Die inländischen Behörden geben der Zollverwaltung Daten, einschliesslich besonders schützenswerter Personendaten, bekannt, sofern dies für den Vollzug der von der Zollverwaltung anzuwendenden Erlasse notwendig ist.		
	32. Bundesgesetz vom 12. Juni 2009 über die Mehrwertsteuer[61] Fussnote: [61] SR 614.20		
Art. 76 Abs. 1 zweiter Satz	[1] ... Sie führt die dazu notwendigen Datenbanken und Akten sowie die Mittel zur Bearbeitung und Aufbewahrung.		
	33. Kernenergiegesetz vom 21. März 2003[62] Fussnote: [62] SR 732.1		
Art. 24 Abs. 2	[2] Im Rahmen dieser Prüfung können Daten über die Gesundheit und psychische Eignung sowie sicherheitsrelevante Daten über die Lebensführung der betroffenen Person bearbeitet werden; es kann darüber eine Datenbank oder Akten führen.		
	34. Strassenverkehrsgesetz vom 19. Dezember 1958[63] Fussnote: [63] SR 741.01		
Art. 76b Abs. 3 zweiter Satz	[3] ... Sie sind zur Erfüllung der ihnen übertragenen Aufgaben befugt, die dafür benötigten Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen.		

Art.	Text	Änderungsvorschläge	Kommentare
	35. Luftfahrtgesetz vom 21. Dezember 1948[64] Fussnote: [64] SR 748.0		
Art. 107a Abs. 2 Einleitungssatz, Abs. 4 und 5	[2] Die Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Daten, und das Profiling sind zulässig betreffend: [4] Die Erbringer der zivilen und der militärischen Flugsicherungsdienste können zur Untersuchung von Flugunfällen und schweren Vorfällen bei Flugverkehrsstellen Hintergrundgespräche und -geräusche aufzeichnen. Der Bundesrat regelt die Verantwortung für die Datenbeschaffung, das Auswertungsverfahren, die Datenempfänger, die Aufbewahrungsdauer und die technischen und organisatorischen Schutzmassnahmen. [5] Die Daten bearbeitenden Stellen können zum Vollzug ihrer gesetzlichen Aufgaben den mit entsprechenden Aufgaben betrauten in- und ausländischen Behörden sowie internationalen Organisationen Personendaten, einschliesslich besonders schützenswerter Daten, bekannt geben, wenn diese Behörden und Organisationen einen angemessenen Schutz der Daten gewährleisten.		
	36. Postgesetz vom 17. Dezember 2010[65] Fussnote: [65] SR 783.0		
Art. 26 Abs. 1	[1] Die PostCom sowie weitere mit dem Vollzug dieses Gesetzes betraute Behörden übermitteln anderen Behörden des Bundes und der Kantone diejenigen Daten, die diese zur Erfüllung ihrer gesetzlichen Aufgaben benötigen. Dazu gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten.		
Art. 28	*Bearbeitung von Personendaten* Die PostCom sowie die Schlichtungsstelle dürfen zur Erfüllung ihrer gesetzlichen Aufgaben Personendaten, einschliesslich besonders schützenswerter Personendaten betreffend strafrechtliche Verfolgungen und Sanktionen, bearbeiten.		
	37. Fernmeldegesetz vom 30. April 1997[66] Fussnote: [66] SR 784.10		
Art. 13a Abs. 1	[1] Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen		

Art.	Text	Änderungsvorschläge	Kommentare
erster Satz	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. ...		
	38. Betäubungsmittelgesetz vom 3. Oktober 1951[67] Fussnote: [67] SR 812.121		
Art. 3f Abs. 1	[1] Die für den Vollzug dieses Gesetzes zuständigen Behörden und Institutionen sind berechtigt, Personendaten, einschliesslich besonders schützenswerter Personendaten, zur Überprüfung der Voraussetzungen und des Verlaufs der Behandlung von betäubungsmittelabhängigen Personen zu bearbeiten.		
Art. 18c zweiter Satz	*Aufgehoben*		
	39. Arbeitsvermittlungsgesetz vom 6. Oktober 1989[68] Fussnote: [68] SR 823.11		
Art. 33a Abs. 1	*Einleitungssatz* [1] Die mit der Durchführung sowie mit der Kontrolle oder Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, Personendaten zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:		
Art. 35 Abs. 2, 3bis und	[2] In diesem Informationssystem dürfen Personendaten, einschliesslich besonders schützenswerter Personendaten nach Artikel 33*a* Absatz 2,		

Art.	Text	Änderungsvorschläge	Kommentare
5 Bst. d	bearbeitet werden. [3bis] Soweit es für den Vollzug dieses Gesetzes und des Arbeitslosenversicherungsgesetzes vom 25. Juni 1982 (AVIG)[69] notwendig ist, dürfen Personendaten, einschliesslich besonders schützenswerter Daten, zwischen den Informationssystemen der öffentlichen Arbeitsvermittlung und den Informationssystemen der Arbeitslosenversicherung (Art. 83 Abs. 1 Bst. i AVIG) ausgetauscht werden. [5] Der Bundesrat regelt: d. den Zugriff auf die Daten, namentlich, welche Benutzer des Informationssystems befugt sind, besonders schützenswerte Personendaten zu bearbeiten; Fussnote: [69] SR 837.0		
	40. Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung[70] Fussnote: [70] SR 831.10		
Art. 49a	*Einleitungssatz* Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:		
	41. Bundesgesetz vom 25. Juni 1982 über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge[71] Fussnote: [71] SR 831.40		
Art. 85a	*Einleitungssatz* Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:		
	42. Bundesgesetz vom 18. März 1994 über die Krankenversicherung[72] Fussnote: [72] SR 832.10		

Art.	Text	Änderungsvorschläge	Kommentare
Art. 84	*Einleitungssatz* Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes oder des KVAG[73] betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz oder nach dem KVAG übertragenen Aufgaben zu erfüllen, namentlich um: Fussnote: [73] SR 832.12		
	43. Bundesgesetz vom 20. März 1981 über die Unfallversicherung[74] Fussnote: [74] SR 832.20		
Art. 96	*Einleitungssatz* Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:		
	44. Bundesgesetz vom 19. Juni 1992 über die Militärversicherung[75] Fussnote: [75] SR 833.1		
Art. 94a	*Einleitungssatz* Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:		
	45. Arbeitslosenversicherungsgesetz vom 25. Juni 1982[76] Fussnote: [76] SR 837.0		
Art. 96b	*Einleitungssatz*		

Art.	Text	Änderungsvorschläge	Kommentare
	Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:		
Art. 96c Abs. 2 Einleitungssatz, Abs. 2bis	2 Sie dürfen diejenigen Personendaten, einschliesslich besonders schützenswerter Daten, abrufen, die sie benötigen, um die folgenden ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen: 2bis Soweit es für den Vollzug dieses Gesetzes und des Arbeitsvermittlungsgesetzes vom 6. Oktober 1989 (AVG)[77] notwendig ist, dürfen Personendaten, einschliesslich besonders schützenswerter Daten, zwischen den Informationssystemen der Arbeitslosenversicherung (Art. 83 Abs. 1 Bst. i) und den Informationssystemen der öffentlichen Arbeitsvermittlung (Art. 35 AVG) ausgetauscht werden. Fussnote: [77] SR 823.11		
	46. Tierseuchengesetz vom 1. Juli 1966[78] Fussnote: [78] SR 916.40		
Art. 54a Abs. 3	3 Im Rahmen ihrer gesetzlichen Aufgaben dürfen die Vollzugsbehörden besonders schützenswerte Personendaten und Betriebsprofile bearbeiten.		
	47. Jagdgesetz vom 20. Juni 1986[79] Fussnote: [79] SR 955.0		
Art. 22 Abs. 3 erster und zweiter Satz	3 Es darf diese Daten in einer Datenbank oder in Akten aufbewahren. Nach Ablauf des Entzugs der Jagdberechtigung löscht es die Daten und vernichtet die entsprechenden kantonalen Verfügungen. ...		
	48. Geldwäschereigesetz vom 10. Oktober 1997[80] Fussnote: [80] SR 955.0		
Art. 29 Abs. 2 zweiter Satz	2 …. Dazu gehören namentlich Finanzinformationen sowie andere, in Straf-, Verwaltungsstraf- und Verwaltungsverfahren beschaffte besonders schützenswerte Personendaten, einschliesslich solcher aus hängigen Verfahren.		

Art.	Text	Änderungsvorschläge	Kommentare
Art. 34	**Datenbanken und Akten im Zusammenhang mit der Meldepflicht** 1 Die Finanzintermediäre führen separate Datensammlungen, die alle im Zusammenhang mit der Meldung stehenden Unterlagen enthalten. 2 Sie dürfen Daten aus diesen Datensammlungen nur an die FINMA, die Eidgenössische Spielbankenkommission, Selbstregulierungsorganisationen, die Meldestelle und Strafverfolgungsbehörden weitergeben. 3 Das Auskunftsrecht betroffener Personen nach Artikel 8 des Bundesgesetzes vom 19. Juni 19922 über den Datenschutz ist ab Erstattung einer Meldung nach Artikel 9 Absatz 1 dieses Gesetzes oder nach Artikel 305ter Absatz 2 StGB3 bis zum Zeitpunkt, an dem die Meldestelle den Finanzintermediär nach Artikel 23 Absatz 5 oder 6 informiert, sowie während einer Vermögenssperre nach Artikel 10 ausgeschlossen.4 4 Fünf Jahre nach erfolgter Meldung sind die Daten zu vernichten.	2 Sie dürfen Daten aus diesen Datensammlungen nur an die FINMA, die Eidgenössische Spielbankenkommission, Selbstregulierungsorganisationen, die Meldestelle und Strafverfolgungsbehörden weitergeben. Vorbehalten bleibt die Weitergabe an Zweiniederlassungen und innerhalb einer Finanzgruppe gemäss Artikel 34bis.	Siehe Anmerkungen unten zum vorgeschlagenen Art. 34bis.
Art. 34bis		Art. 34bis (NEU): Weitergabe an Zweiniederlassungen 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.	Die FINMA konkretisiert das per anfangs 2016 in Kraft getretene revidierte Geldwäschereigesetz in ihrer gleichzeitig in Kraft getretenen Verordnung 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 Präambel (19) der EU-DSGVO festgehaltenen Bestimmung, dass die Mitgliedstaaten Erlasse beschliessen können, welche die in der EU-DSGVO festgehaltenen Pflichten und Rechte beschränken, soweit dies zur Bekämpfung

Art.	Text	Änderungsvorschläge	Kommentare
			der Geldwäsche erforderlich und verhältnismässig ist.
	49. Finanzmarktaufsichtsgesetz vom 22. Juni 2007[81] Fussnote: 81 SR 956.1		
Art. 23 Abs. 1 erster Satz	1 Die FINMA bearbeitet im Rahmen der Aufsicht nach diesem Gesetz und den Finanzmarktgesetzen Personendaten, einschliesslich besonders schützenswerter Personendaten. …		
	50. Bundesgesetz vom 19. März 1976 über die internationale Entwicklungszusammenarbeit und humanitäre Hilfe[82] Fussnote: 82 SR 974.0		
Art. 13a Abs. 1 Bst. g	*Aufgehoben*		
	51. Bundesgesetz vom 24. März 2006 über die Zusammenarbeit mit den Staaten Osteuropas[83] Fussnote: 83 SR 974.1		
Art. 16 Abs. 1 Bst. g	*Aufgehoben*		

Amstutz Jonas BJ

Von: Zollikofer Manuel <m.zollikofer@crif.com>
Gesendet: Montag, 3. April 2017 13:39
An: Amstutz Jonas BJ
Cc: Zollikofer Manuel
Betreff: Stellungnahme VE DSG der CRIF AG
Anlagen: Stellungnahme VE DSG der CRIF AG Zürich 20170403.pdf; Stellungnahme VE DSG der CRIF AG Zürich 20170403.docx

Sehr geehrter Herr Amstutz

Beiliegend sende ich Ihnen die Stellungnahme der CRIF AG als Word und PDF.

Darf ich Sie um eine kurz Empfangsbestätigung bitten?

Freundliche Grüsse
Manuel Zollikofer

Dr. Manuel Zollikofer
Dipl. Inf. Ing. ETH & Ph.D HEC
Vorsitzender der Geschäftsleitung
CRIF AG
Hagenholzstrasse 81
Postfach
CH-8050 Zürich

Tel +41 44 913 68 28
Mob +41 76 413 50 54
m.zollikofer@crif.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 : CRIF AG, CHE-107.708.282

Abkürzung der Firma / Organisation :

Adresse : Hagenholzstrasse 81, 8050 Zürich

Kontaktperson : Manuel Zollikofer

Telefon : +41 44 913 68 28

E-Mail : m.zollikofer@crif.com

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

Allgemeine Bemerkungen 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 4

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 17

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten 18

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") 18

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" 18

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
CRIF AG	Es ist zu begrüssen, dass im VE DSG auf eine Berechtigung des Beauftragten zum **Erlass von verbindlichen Datenschutzvorschriften** verzichtet wurde.
CRIF AG	Der Verzicht im VE DSG auf die Einführung einer **Beweislastumkehr** und von Instrumenten zur **kollektiven Rechtsdurchsetzung** wird mit der vorliegenden Vernehmlassungsantwort unterstützt.

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
CRIF AG	VE DSG	3			Der Begriff der „**Datensammlung**“ ist ohne Not vom bisherigen Art. 3 Bst. g DSG nicht ins VE DSG übernommen worden. Die Wiedereinführung dieses Begriffes könnte dafür verwendet werden, gewisse Pflichten unter dem neuen DSG einer sinnvollen Beschränkung zu unterziehen, insbesondere die Informationspflichten (VE DSG Art. 13) sowie die Auskunftspflichten (VE DSG Art. 20) des Verantwortlichen (vgl. nachstehend auch die Bemerkungen zu VE DSG Art. 20 Abs. 2). Antrag: Der Begriff der Datensammlung ist wieder in VE DSG Art. 3 zu definieren.
CRIF AG	VE DSG	3		c	**Ziffer 3**: Nur diejenigen **genetischen Daten**, die zum Zwecke der Identifikation einer natürlichen Person bearbeitet werden, sollen ein besonders schützenswertes Personendatum darstellen. Die Definition in Art. 3 Bst. c Ziffer 3 VE DSG ist insoweit einzuschränken.
CRIF AG	VE DSG	3		c	**Ziffer 4**: Der Begriff der „**biometrischen Daten, die eine natürliche Person eindeutig identifizieren**“ ist viel zu weit gefasst. Gestützt auf diese Definition wird jedes Gesichtsfoto künftig als besonders schützenswertes Personendatum gelten. Erfasst sein sollen nach Art. 3 Bst. c Ziffer 4 VE DSG jedoch nur jene biometrischen Daten, die gerade zum Zwecke der Identifikation bearbeitet werden. Mehr verlangt auch die Konvention 108 nicht.
CRIF AG	VE DSG	3		c	**Ziffer 5**: Die generelle Unterstellung von „**Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen**“ unter die besonders schützenswerten Personendaten ist für eine Auskunftei wie die CRIF AG problematisch. Der Rechtfertigungsgrund der „Prüfung der Kreditwürdigkeit“ gemäss VE DSG Art. 24 Abs. 2 Bst. c greift gemäss Ziffer 1 der betreffenden Bestimmung nicht für die Bearbeitung von besonders schützenswerten Personendaten. Werden nun generell alle „Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen“ unter die besonders schützenswerten Personendaten subsumiert, können auch **Daten zu Verurteilungen im Zusammenhang mit bestimmten Vermögensdelikten** von einer Auskunftei nicht mehr bearbeitet werden, obwohl diese von erheblicher Relevanz für die Kreditwürdigkeit

					einer Person sind. Daten über Verfolgungen im Zusammenhang mit Vermögensdelikten sind deshalb von den besonders schützenswerten Personendaten **auszunehmen** oder in VE DSG Art. 24 Abs. 2 Bst. c Ziffer 1 ist eine entsprechende **Ausnahme vorzusehen** (siehe dazu auch nachfolgend zu VE DSG Art. 24 Abs. 2 Bst. c).
CRIF AG	VE DSG	3		f	Der Begriff des „Profilings“ gemäss VE DSG Art. 3 Bst. f ist zu breit gefasst und geht deutlich über die entsprechende Regelung der EU hinaus. Im Gegensatz zur DSGVO und E-SEV 108 liegt ein Profiling nach dem VE-DSG • 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 von anderen Daten** in die Definition des Profilings ist nach Auffassung der CRIF AG 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 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 (VE DSG Art. 23 Abs. 1 Bst. d). Dies auch dann, wenn das Profiling keine unmittelbaren Auswirkungen auf die betroffene Person hat (siehe den Erläuternden Bericht zu VE DSG Art. 15, 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**.
CRIF AG	VE DSG	4	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. 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 die Bedeutung dieser Begrifflichkeit nicht klar ist. Die Umformulierung gegenüber dem geltenden Recht ist überflüssig und schafft Rechtsunsicherheit. Gemäss Erläuterndem Bericht zum Vorentwurf S. 46 hat die neue Formulierung im Vergleich zum geltenden Recht keine materiellen Änderungen zur Folge. Wenn dem so ist, erübrigt sich die Neuformulierung auch.
CRIF AG	VE DSG	4	5		Der Grundsatz der Datenrichtigkeit in VE DSG Art. 4 Abs. 5 wurde neu gefasst. Da jedoch gemäss Erläuterungen zum Vorentwurf, Seite 47, damit keine Änderung des bisherigen Rechts beabsichtigt ist, ist die **Anpassung überflüssig und schafft nur Rechtsunsicherheit**. Der Wortlaut des bestehenden Gesetzes erscheint sachgerechter und ist wieder zu übernehmen.
CRIF AG	VE DSG	4	6		Das Erfordernis der **Ausdrücklichkeit einer Einwilligung für ein Profiling** rechtfertigt sich nicht. Abgesehen davon, dass der Begriff der „Ausdrücklichkeit“ nicht klar ist, schiesst diese Bestimmung über das Ziel hinaus, indem für meist harmlose Vorgänge ein qualifiziertes Erfordernis verlangt wird. Alternativ könnte die ausdrückliche Einwilligung für ein Profiling auch nur unter dem Vorbehalt verlangt werden, dass kein überwiegendes berechtigtes Interesse eines Verantwortlichen oder eines Dritten entgegensteht.
CRIF AG	VE DSG	8			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 Beauftragte 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. Zudem besteht ein **Risiko**, dass der Beauftragte 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 Beauftragte 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.
CRIF AG	VE DSG	9			Die genauen Rechtswirkungen der 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.
CRIF AG	VE DSG		12		Der Verantwortliche muss gemäss VE DSG Art. 12 Abs. 1 Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt. Gemäss VE DSG Art. 12 Abs. 2 wird das schutzwürdige Interesse bei bestimmten Tatbeständen vermutet. Dies bedeutet für eine Auskunftei wie die CRIF AG, dass zumindest die im Gesetz genannten Vermutungstatbestände überprüft werden müssten, was mit einem **unangemessenen Mehraufwand** verbunden wäre. Verlangt werden müsste in diesem Zusammenhang ein Nachweis, z.B. über das Vorliegen einer geraden Verwandtschaft zur verstorbenen Person oder einer eingetragenen Partnerschaft mit ihr. Neben dem enormen damit verbundenen Abklärungs- und Prüfungsaufwand stellt sich auch die Frage, wie die CRIF AG als Auskunftei verifizierten soll, ob eine Person mit einer verstorbenen Person eine faktische Lebensgemeinschaft geführt hat. Dies ist

					schlicht nicht möglich. Die neue Regelung von Art. 12 DSG ist zu aufwändig, nicht praktikabel und aus Sicht des Datenschutzes überflüssig bzw. ohne Mehrwert. Sie ist daher zu streichen.
CRIF AG	VE DSG	13			Die neu gefasste Informationspflicht gemäss VE DSG Art. 13 wird zu einer unnötigen und sogar **kontraproduktiven Überinformation** der betroffenen Person führen, indem diese mit Informationen überflutet wird und sie die Informationen damit gar nicht mehr bewusst zur Kenntnis nehmen (kann). Die angestrebte Verbesserung des Datenschutzes wird damit vereitelt. Eine **risikobasierte Transparenzpflicht**, wie sie in Art. 4 DSG und Art. 4 VE DSG zum Ausdruck kommt, genügt vollständig. Auf VE DSG Art. 13 in dieser neuen Form ist zu verzichten; der bestehende Art. 14 DSG erfüllt die Anforderungen. Für eine Auskunftei wie die CRIF AG, welche ihre Daten mehrheitlich bei Dritten beschafft, wäre eine individuelle Detailinformation der betroffenen Person bei jeder einzelnen Datenbeschaffung vom zu bearbeitenden **Volumen her schlicht nicht handelbar**. Wird die neue Norm ernst genommen, würde dies bedeuten, dass bei jeder Adressänderung oder jedem Vorgang, der zu einer Anpassung der Kreditwürdigkeit führt, eine solche Information erfolgen müsste. Dies ist schlicht nicht praktikabel. Unter dem heutigen Recht hat die CRIF AG ihrer Informationspflicht in einigen wenigen Tausend Fällen nachzukommen. Mit der neuen Regelung wären über 1 Million Nachmeldungen pro Jahr informationspflichtig, ohne dass damit irgendein Mehrnutzen verbunden wäre. Es sollte damit zumindest präzisiert werden, dass bei Änderungen keine Nachinformation stattfinden muss. Statt einer Detailinformation bei jeder Datenbeschaffung sollte wenn schon die Möglichkeit vorgesehen werden, der Informationspflicht mit einer **generellen Information (z.B. auf der Website**) nachkommen zu können. Die Information bei der Beschaffung könnte auf die Identität des Datenbearbeiters und einen Hinweis für weitergehende Informationen beschränkt werden. Die Vorgaben der Konvention 108 wären auch damit erfüllt, da der Zugang zur Information gesichert wäre. Im Übrigen entspräche diese Lösung auch der geltenden Praxis des Beauftragten. Im Erläuternden Bericht zum Vorentwurf (Seite 56) wird festgehalten, dass die Information in allgemeiner Form wie AGB oder einer Datenschutzerklärung auf einer Website erfolgen kann. Im Gesetz fehlt aber eine entsprechende Bestimmung, was auf jeden Fall nachzuholen wäre.
CRIF AG	VE DSG	13	3		Art. 13 Abs. 3 VE-DSG verwendet die Begriffe «Dritter» und «Empfängerinnen und Empfänger», ohne diese

					genau zu definieren. Dies wäre nachzuholen. Im Erläuternden Bericht zum Vorentwurf (Seite 57) wird sodann festgehalten, dass die Identität des Empfängers in jedem Fall bekannt gegeben werden muss, wenn diese dem Verantwortlichen bekannt ist. Dies steht im Gegensatz zum Gesetzestext, welcher auch alternativ die Mitteilung „**der Kategorien der Empfängerinnen und Empfänger**“ vorsieht. Es ist klarzustellen, dass der Gesetzestext gilt.
CRIF AG	VE DSG	13	5		Art. 13 Abs. 5 VE DSG sieht bei indirekter Datenbeschaffung einer **Information spätestens bei Speicherung** vor. Dies ist von den Geschäftsabläufen einer Auskunftei schlicht nicht möglich, da eine Vielzahl von Daten dauernd und automatisiert geändert wird. Eine Informationsfrist von mindestens einem Monat, wie sie auch die DSGVO vorsieht, wäre hier sachgerechter.
CRIF AG	VE DSG	14			Die **typischen Ausnahmefälle** für eine Informationspflicht analog zum heutigen Art. 13 Abs. 2 DSG fehlen und sind wieder einzuführen.
CRIF AG	VE DSG	14	4	a	Die **Beschränkung der Berufung auf ein überwiegendes privates Interesse** für den Fall, dass die Personendaten nicht an Dritte bekannt gegeben werden, ist aufzuheben. Entscheidend sollte allein die Gewichtung der Interessen von Datenbearbeiter und betroffener Person sein. Dies entspricht auch der Regelung der Konvention 108.
CRIF AG	VE DSG	15	1		Die Informationspflicht bei automatisierten Einzelentscheidungen gemäss VE DSG Art. 15 Abs. 1 sollte auf den Standard gemäss Art. 22 DSGVO und Art. 8 Abs. 1 Bst. a der E-SEV 108 beschränkt werden. Beide Bestimmungen machen vom Wortlaut her klar, dass die Pflichten der Verantwortlichen nur greifen, wenn die Auswirkungen der automatisierten Entscheidung **erheblich** sind. Der Wortlaut von VE DSG Art. 15 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. Dies ist zu korrigieren. Sodann sind **Ausnahmen von der Informations- und Anhörungspflicht** vorzusehen, wie dies auch in Art. 22 Abs. 2 DSGVO der Fall ist. Es stellt sich insbesondere die Frage, ob für jeden automatisierten Vertragsabschluss (z.B. in einem Online-Shop) die Möglichkeit zum Dialog mit einem Menschen vorgesehen werden muss? Damit wird das in der Schweiz geltende Prinzip der Vertragsfreiheit tangiert. Dies ist durch

					eine entsprechende Ausnahmebestimmung zu korrigieren. Um die Vorteile, die automatisierte Entscheidungen für die Unternehmen bringen, nicht durch übermässige administrative Aufwände zunichte zu machen, müssen die Rahmenbedingungen der Information und Anhörung genauer geklärt werden. Es sollte insbesondere klargestellt werden, dass die betroffene Person nur über **die Tatsache** eines automatisierten Entscheides informiert werden muss und nicht über die bearbeiteten Daten als solche. Diesbezüglich sollte einzig darauf hingewiesen werden können, dass diese Daten auf Rückfrage zur Verfügung gestellt werden. Eine **allgemeine Klausel** z.B. auf der Website des Datenbearbeiters, in welcher darauf hingewiesen wird, in welchen Sachgebieten automatische Einzelentscheidungen erfolgen, sollte genügen, da damit genügend Angaben geliefert werden, um automatisierte Entscheide als solche erkennen zu können. Eine Rückfrage der betroffenen Person sollte sodann nur auf die **Daten zu einem spezifischen und individualisierten Entscheid** beschränkt werden. Generelle Ersuchen hinsichtlich einer „Liste der getroffenen automatisierten Entscheide" sollten klar als nicht zulässig bezeichnet werden. Die Zulässigkeit von „Listenabfragen" würde massiv in die Privatsphäre der betroffenen Datenbearbeiter eingreifen und der Schikane bzw. der Ausforschung Vorschub leisten. Gemäss Erläuterungen zum Vorentwurf muss die Anhörung **kostenlos** sein. Eine solch strenge Regelung ist in der Konvention 108 nicht vorgesehen, weil dadurch Missbrauch Tür und Tor geöffnet würde. In Missbrauchsfällen sollte damit zumindest eine Kostenpflichtigkeit der Anhörung eingeführt werden.
CRIF AG	VE DSG	15	2		Eine betroffene Person hat bereits im Rahmen von VE DSG Art. 4 Abs. 5 die Möglichkeit, sich zu den über sie bearbeiteten Daten zu äussern. VE DSG Art. 15 Abs. 2 kann deshalb **als redundant gestrichen werden**. Auch die DSGVO sieht in Art. 22 ein Recht zur Äusserung zu den bearbeiteten Daten für automatisierte Einzelentscheide nicht vor.
CRIF AG	VE DSG	16	1		Die Hürde für eine Datenschutz-Folgeabschätzung ist zu tief angesetzt. Die Durchführung einer Datenschutz-Folgenabschätzung muss gemäss VE DSG 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. 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. Sodann wird gemäss Erläuterndem Bericht zum Vorentwurf (Seite 61) bereits ein Profiling als Indiz für ein erhöhtes Risiko bezeichnet. Dies ist nicht sachgerecht. Der Aufwand wäre enorm, ohne dass für den Datenschutz wirklich etwas gewonnen wäre. Um Rechtsunsicherheiten zu vermeiden, müssen die **Voraussetzungen, bei deren Vorliegen eine Datenschutz-Folgenabschätzung durchgeführt werden muss**, genauer und einschränkender 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 sollte aus der Bestimmung gestrichen werden.
CRIF AG	VE DSG	16	3		Die in VE DSG Art. 16 Abs. 3 vorgesehene **Meldepflicht** sollte 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 (entsprechend Art. 36 Abs. 1 DSGVO). Die im VE DSG vorgesehene Regelung würde zu massenhaften Meldungen an den Beauftragten führen, die er allein mangels Ressourcen nicht in der Lage wäre 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. Dafür muss ein angemessener Schutz vorgesehen werden.
CRIF AG	VE DSG	16	4		Die **Frist** von drei Monaten, die dem Beauftragten für die Prüfung der Massnahmen zur Verfügung stehen, ist in der Praxis vollkommen untauglich und führt dazu, dass wichtige Projekte ungebührlich lang verzögert

					bzw. erhebliche Kosten verschlingen werden. Diese Bestimmung sollte gestrichen bzw. durch eine angemessene kürzere Frist ersetzt werden. Zudem sollten Unternehmen, die einen betrieblichen Datenschutzbeauftragten bezeichnet haben, von der Meldepflicht generell ausgenommen sein.
CRIF AG	VE DSG	19		b	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, da 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 im VE DSG 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.
CRIF AG	VE DSG	20	1		Es sind **Ausnahmen von der Kostenlosigkeit** für Auskunftsersuchen vorzusehen. Auch gemäss geltendem Recht, sind Auskünfte unter Umständen kostenpflichtig (z.B. in Missbrauchsfällen, siehe VDSG Art. 2 Abs. 1). Gemäss DSGVO (Art. 12 Abs. 5 Bst. a) müssen Auskunftsersuchen ebenfalls nicht zwingend kostenlos sein. Durch die Einführung des Begriffs „kostenlos“ in VE DSG Art. 20 Abs. 1 wird eine Änderung gegenüber der heutigen Praxis statuiert, welche nicht sachgerecht ist. Das Wort „kostenlos“ ist deshalb zu

					streichen. Sodann sind auf dem Verordnungswege Ausnahmen von der Kostenlosigkeit des Auskunftsrechtes zu statuieren. 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 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) Zwecke 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. Mindestens sollten Auskunftsersuchen aber auf jene Fälle beschränkt werden, in denen nachgewiesen werden kann, dass ein Auskunftsersuchen primär aus Datenschutzgründen erfolgt, und nicht zu anderen Zwecken.
CRIF AG	VE DSG	20	2		Das Auskunftsrecht nach Art. 8 DSG galt bisher nur für **Daten in Datensammlungen**. Neu soll es - jedenfalls nach dem Wortlaut der revidierten Bestimmung - für alle Daten gelten, die ein Verantwortlicher bearbeitet. Wird diese Auskunftspflicht absolut verstanden, müssten jedes Schreiben, jede E-Mail und sogar interne Notizen beauskunftet werden, auch wenn diese Informationen nicht in die Datensammlung selbst aufgenommen worden sind. Für eine Kreditauskunftei wie die CRIF AG bedeutet dies, dass alle Daten aus dem eigentlichen Geschäftsbetrieb offengelegt werden müssen, obwohl diese Daten Dritten niemals zur Verfügung gestellt werden. Das geht zu weit! Das Auskunftsrecht ist deshalb wieder ausdrücklich auf Daten in Datensammlungen zu beschränken. Die Wiedereinführung des gestrichenen Begriffes der „Datensammlung“ (bisheriger Art. 3 Bst. g DSG) könnte darüber hinaus dafür verwendet werden, weitere Pflichten unter dem neuen DSG (z.B. Informationspflichten) einer sinnvollen Beschränkung zu unterziehen (siehe dazu auch die Bemerkungen zu VE DSG Art. 3 vorstehend).
CRIF AG	VE DSG	20	2	f	Gemäss Lehre und Rechtsprechung zum geltenden DSG müssen nur die Angaben über die Herkunft der Daten mitgeteilt werden, soweit dies für den Antragsteller **nötig ist, um seine Rechte gegenüber diesen Quellen geltend zu machen**. Diese Einschränkung ist in den VE DSG zu übernehmen.

CRIF AG	VE DSG	20	2	g	Es ist im Zusammenhang mit dem Verweis auf VE DSG Art. 13 Abs. 3 klarzustellen, dass nicht die Identität der Datenempfänger, sondern allein **die Kategorien der Empfängerinnen und Empfänger** zu beauskunften sind.
CRIF AG	VE DSG	20	3		Gemäss VE DSG Art. 20 Abs. 3 ist ein Datenbearbeiter verpflichtet, bei jedem Entscheid aufgrund einer Datenbearbeitung (neben den eigentlichen Daten) noch zusätzlich Rechenschaft darüber abzulegen, wie und warum er so entschieden hat und welche Konsequenzen die Entscheidung für die betroffene Person hat. Eine **solch breite Auskunftspflicht** ist überzogen und greift massiv in die Freiheiten der betroffenen Datenbearbeiter ein. Sie gefährdet unter anderem auch das Geschäftsgeheimnis einer Auskunftei, indem diese gemäss dieser Bestimmung gezwungen wäre, die ein Geheimnis bildenden Informationen über die Berechnung der Kreditwürdigkeit zu beauskunften. Eine erweiterte Auskunftspflicht kann sich höchstens für von der betroffenen Person spezifizierte automatisierte Einzelentscheide rechtfertigen, welche erhebliche Auswirkungen zeigen und deshalb Anspruch auf ein „menschliches Gehör“ einräumen. Aber auch in diesen Fällen sind Auskünfte hinsichtlich des Zustandekommens und der Auswirkungen des Entscheides auszunehmen.
CRIF AG	VE DSG	21	1		Mit dem Verweis in VE DSG Art. 21 Abs. 1 auf VE DSG Art. 14 Abs. 4 (Bst. a) wird **das Recht zur Einschränkung des Auskunftsrechtes durch Berufung auf ein überwiegendes privates Interesse** des Datenbearbeiters für den Fall aufgehoben, bei welchem die Personendaten an Dritte bekannt gegeben werden. Das Recht zur Einschränkung des Auskunftsrechtes bei überwiegendem privatem Interesse sollte jedoch auch gewährleistet sein, wenn die Daten Dritten bekannt gegeben werden. Entscheidend sollte allein die Gewichtung der Interessen von Datenbearbeiter und betroffener Person sein. Siehe dazu auch die Ausführungen zu VE DSG Art. 14 Abs. 4 Bst. a. Zur näheren Erläuterung der Einschränkungen des Auskunftsrechtes sollten im Gesetz auch exemplarische Beispiele aufgelistet werden (z.B. Berufs- und Geschäftsgeheimnisse, Sicherheitsvorbehalte, Unterlagen, die der Auskunftssuchende schon hat, etc.).
CRIF AG	VE DSG	23	2	d	Gemäss VE DSG Art. 23 Abs. 2 Bst. d gilt **das Profiling per se als Persönlichkeitsverletzung**, was einen Rechtfertigungsgrund erfordert, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden ist. Diese (Dis-)Qualifikation des Profilings ist zu weitgehend und wird weder vom bestehenden Recht noch von

					der DSGVO noch von der Konvention 108 so vorgenommen. Die betreffende Bestimmung ist deshalb **ersatzlos zu streichen**.
CRIF AG	VE DSG	24	2		VE DSG Art. 24 Abs. 2 sieht neu vor, dass in den darauf folgend aufgeführten Fällen ein überwiegendes Interesse der bearbeitenden Person **nur noch „möglicherweise" gegeben ist**. Gemäss Erläuterungen zum Vorentwurf soll damit das Erfordernis zur Interessenabwägung im Einzelfall stärker betont werden. Die bisher bestehende Regelung hat sich jedoch bestens bewährt; eine Neuformulierung schafft nur Rechtsunsicherheit und ist überflüssig. Das Wort „möglicherweise" ist deshalb ersatzlos zu streichen.
CRIF AG	VE DSG	24	2	c	**Ziffer 1**: Der Rechtfertigungsgrund der Prüfung der Kreditwürdigkeit gilt gemäss VE DSG Art. 24 Abs. 2 Bst. c Ziffer 1 nur dann, wenn nicht besonders schützenswerte Personendaten betroffen sind. **Daten über die Verfolgung von Vermögensdelikten** sind gemäss VE DSG Art. 3 Bst. c Ziffer 5 unter die besonders schützenswerten Personendaten zu subsumieren. Entsprechend kann für diese Daten der Rechtfertigungsgrund der Kreditüberprüfung nicht beansprucht werden, obwohl Daten zu Verurteilungen im Zusammenhang mit Vermögensdelikten von erheblicher Relevanz für die Kreditwürdigkeit einer Person sind. Für die entsprechenden Daten ist deshalb in VE DSG Art. Art. 24 Abs. 2 Bst. c Ziffer 1 eine Ausnahme von der Ausnahme als Rechtfertigungsgrund vorzusehen. Alternativ sind Daten über Verfolgungen im Zusammenhang mit Vermögensdelikten in VE DSG Art. 3 Bst. c Ziffer 5 von den besonders schützenswerten Personendaten auszunehmen. Vgl. dazu auch vorstehend zu VE DSG Art. 3 Bst. c Ziffer 5.
CRIF AG	VE DSG	24	2	c	**Ziffer 3**: Gemäss dieser Bestimmung soll der Rechtfertigungsgrund der Kreditüberprüfung nur noch gelten, wenn die betroffene Person **volljährig** ist. Dies mag zwar auf den ersten Blick zum Schutze von Kindern einleuchten, ist aber bei näherer Betrachtung nicht nur nicht sinnvoll, sondern geradezu kontraproduktiv. Online-Shops, welche auch von nicht volljährigen Kunden genutzt werden, stellen in der Regel auf Kreditüberprüfungen ab, in deren Rahmen sie auch erfahren, ob eine Person volljährig ist oder nicht. Mit der vorgeschlagenen Änderung gemäss VE DSG müsste auf die entsprechenden Daten verzichtet werden, was zur Folge hätte, dass nicht volljährige Personen nicht mehr als solche ausgewiesen werden könnten und ein entsprechender Warnhinweis im Rahmen des Kreditratings unterbleiben müsste. Damit würde dem Online-Handel mit nicht zahlungsfähigen Minderjährigen Vorschub geleistet, was der **Absicht des Kindesschutzes gerade widerspricht**.

					Die Bestimmung von VE DSG Art. 24 Abs. 2 Bst. c Ziffer 3 ist deshalb **ersatzlos zu streichen**.
CRIF AG	VE DSG	50 51			VE DSG Art. 50 und Art. 51 setzen primär auf private, strafrechtliche Sanktionen gegen Organe und Mitarbeiter, die in eine Verletzung des DSG involviert sind. Der Vorentwurf geht damit über die Anforderungen der DSGVO sowie der Konvention 108 hinaus. Der **persönliche, strafrechtliche Charakter der Sanktionen ist unverhältnismässig und nicht zielführend**. Betriebliche Datenschutzverantwortliche, welche eigentlich in ihrer Tätigkeit für den Datenschutz gestärkt und geschützt werden sollten, werden durch die Schaffung eines persönlichen Strafbarkeitsrisikos unnötig unter Druck gesetzt. Dies trifft insbesondere zu für die Strafbarkeit von fahrlässigen Verstössen gegen den VE DSG. Eine Kriminalisierung von einzelnen Mitarbeitern ist stossend, zumal die Delikte in den meisten Fällen „nur“ in der Verletzung flankierender Massnahmen (z.B. unterlassene Datenschutz-Folgeabschätzung oder Dokumentation der Datenbearbeitung) besteht. 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**. Ferner ist bei diversen der Antragsdelikte unklar, wer überhaupt antragsberechtigt ist bzw. von wem der Strafantrag ausgehen sollte (z.B. bei einer unterlassenen Datenschutzfolgeabschätzung). Die Strafsanktionen sind somit durch **Verwaltungssanktionen gegen das betroffene Unternehmen** zu ersetzen, welche u.a. Bussen vorsehen für die Fälle, in welchen die betroffenen Personen tatsächlich in ihrer Persönlichkeit verletzt werden.
CRIF AG	VE DSG	53			Eine Sanktionierung sollte nach Ansicht der CRIF AG **primär das Unternehmen** betreffen. Die Regelung gemäss VE DSG Art. 53 hilft in diesem Zusammenhang nicht weiter, da die Mitarbeiter sich nicht darauf verlassen können, dass die betragsmässige Grenze für die Verfolgung des Geschäftsbetriebes erreicht wird. Ausserdem handelt es sich bei VE DSG Art. 53 nur um eine “Kann-Vorschrift“, von welcher auch abgewichen werden kann.
CRIF AG	VE DSG	54			Die Regelung ist 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. Vielfältige Abgrenzungsfragen und –probleme werden bei dieser

					Regelung unausweichlich sein.
CRIF AG	VE DSG	59			Die Übergangsbestimmungen sind **ungenügend**. Bedarf für solche gibt es auch bei etlichen anderen der geänderten Regelungen. Beispielsweise sollte geklärt werden, ob die Informationspflichten gemäss VE DSG Art. 13 auch für schon vorhandene Daten (Bestandesdaten) einer bestehenden Datensammlung gelten, oder nur für neu beschaffte Daten. Es fehlen auch Übergangsregelungen zu den neuen Auskunftspflichten sowie zu automatisierten Einzelentscheiden. Es ist überdies eine generelle Übergangsfrist von zwei Jahren vorzusehen, analog der Regelung der DSGVO.
CRIF AG	ZPO				Die **Befreiung von Gerichtskosten** für Datenschutzverfahren ist eine unnötige Belastung der Kantone. Sie wird den Datenschutz nicht fördern. Ausserdem ist zu erwarten, dass dadurch die Fallzahlen markant ansteigen und Prozesse auch leichtfertig eingeleitet werden. Gerade Personen mit der Berechtigung zu unentgeltlicher Prozessführung sind nach der Erfahrungen der CRIF AG überdurchschnittlich oft bereit, unnötige Prozesse zu führen. Daran wird auch die Gefahr einer Parteientschädigung im Falle des Unterliegens nichts ändern, falls die Gerichtskosten befreit 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

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

curafutura
Die innovativen Krankenversicherer
Les assureurs-maladie innovants
Gli assicuratori-malattia innovativi

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Simonetta Sommaruga
Bundeshaus West
3003 Bern

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

Bern, 4. April 2017

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

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 21. Dezember 2016 laden Sie uns ein, an der Vernehmlassung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG) und die Änderung weiterer Erlasse zum Datenschutz teilzunehmen, wofür wir uns bedanken.

Gerne nehmen wir zum Vorentwurf über die Totalrevision des DSG und die Änderung weiterer Erlasse zum Datenschutz Stellung. Die beiden Vorlagen *Bundesbeschluss über die Genehmigung des Notenaustausches (...)* und *Entwurf zur Revision des Übereinkommens SEV 108 (...)* werden wir nachfolgend nicht kommentieren. Wir verweisen zudem auf die Stellungnahme des SVV zu diesem Thema.

Position curafutura

curafutura begrüsst grundsätzlich die Revision des Datenschutzgesetzes, da dieses aufgrund der fortschreitenden Digitalisierung und den europäischen Entwicklungen notwendig ist. Die Regulierungen müssen den Kundinnen und Kunden jedoch einen Mehrwert bieten, die den zusätzlichen Verwaltungsaufwand legitimieren.

curafutura spricht sich gegen einen „Swissfinish“ aus. Das Gesetz soll innerhalb des europäischen Rahmens revidiert werden und keine strengeren Regelungen vorsehen.

curafutura lehnt die Sanktionsmassnahmen gegen natürliche Personen ab. Strafbestimmungen sollten sich gegen die juristischen Personen richten, in deren Interesse die Datenbearbeitungen erfolgen.

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 absi-

Gutenbergstrasse 14, CH-3011 Bern, +41 31 310 01 80, info@curafutura.ch, www.curafutura.ch

chern 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.

curafutura erachtet die Bestimmungen zum Profiling, die das Vorhandensein einer Grundlage in einem formellen Gesetz verlangen, als nicht erreichbar, da schon heute die gesetzlichen Grundlagen fehlen. Für curafutura ist es deshalb zentral, dass die vorgenannten Datenbearbeitungen immer dann als zulässig gelten, soweit sie vom Sinn und Zweck des Gesetzes als gedeckt betrachtet werden können.

1. Ausgangslage

Das heutige Datenschutzgesetz stammt aus dem Jahr 1992, ist seit 1. Juli 1993 in Kraft und wurde mit einer Teilrevision im 2006 geändert, die seit 2008 in Kraft ist.

Die Totalrevision des DSG hat zum Ziel, den Schutz von Personendaten zu stärken und den Entwicklungen im Bereich des Datenschutzes in der Europäischen Union und auf Ebene des Europarates Rechnung zu tragen.

2. Wichtigkeit der Vorlage

Der Umgang mit Kundendaten bildet eine unentbehrliche Grundlage des Versicherungsgeschäftes. Krankenversicherer sind auf die Daten ihrer Kundinnen und Kunden angewiesen. Sei es beim Abschluss eines Versicherungsvertrages (Risikoprüfung und Tarifierung) oder im Leistungsfall. Die Datenschutzgesetzrevision ist für die Mitglieder von curafutura deshalb von zentraler Bedeutung.

Die Revisionsbestrebungen sind aufgrund der europäischen Entwicklungen und der Digitalisierung grundsätzlich zu begrüssen. curafutura spricht sich jedoch gegen Regelungen aus, die strenger ausgelegt werden, als in den vergleichbaren europäischen Gesetzen. Alle neuen Regulierungen müssen zwingend einen Mehrnutzen für unsere Kundinnen und Kunden aufweisen, da ansonsten der zusätzliche Verwaltungsaufwand nicht legitimiert ist. Zusätzlich gilt es zu vermeiden, dass das Datenschutzgesetz der Schweiz ein „Swissfinish“ erhält und somit Dinge grundsätzlich anders regelt, als dies in der EU vorgesehen ist.

3. Details zu den wichtigsten Punkten

Statt der Einführung von Verwaltungssanktionen soll die strafrechtliche Verantwortung der mit Datenbearbeitungen befassten natürlichen Personen massiv ausgebaut und verschärft werden (vgl. Art. 50 ff. VE-DSG). Praktisch alle Informations- und Sorgfaltspflichten sind nunmehr strafrechtlich sanktioniert, auch deren fahrlässige Begehung. Ausserdem richten sich die Sanktionen primär an die für die Datenbearbeitung verantwortliche natürliche Person und nicht an das Unternehmen, in dessen Interesse die Datenbearbeitungen erfolgen. Für eine natürliche Person können sich die Bussenbeträge (maximal CHF 500‘000.00 bei Vorsatz und CHF 250‘000.00 bei Fahrlässigkeit) erheblich auswirken. Dies ist abzulehnen. Stattdessen sollten sich die Strafbestimmungen gegen die juristischen Personen richten (selbstverständlich unter Vorbehalt von vorsätzlich kriminellen Machenschaften von Mitarbeitern, wie z.B. Datendiebstahl) und ausschliesslich als Vorsatztatbestände konzipiert sein.

Gutenbergstrasse 14, CH-3011 Bern, +41 31 310 01 80, info@curafutura.ch, www.curafutura.ch

Mit Art. 27 Abs. 2 verlangt der Vorentwurf für das Profiling, welches im Digitalisierungszeitalter meist im Rahmen einer automatisierten Einzelentscheidung erfolgt, je das Vorhandensein einer Grundlage in einem formellen Gesetz. Die Abwicklung des Krankenversicherungs- als Massenversicherungsgeschäft beinhaltet eine Vielzahl solcher Profile und Entscheide. Es muss daher mit Blick auf die noch immer fehlende gesetzliche Grundlage z.B. für Case Management als Illusion betrachtet werden, dass der Gesetzgeber die erforderlichen Grundlagen schafft. Aus diesem Grund ist es für die Krankenversicherer zentral, dass die vorgenannten Datenbearbeitungen immer dann als zulässig gelten, soweit sie vom Sinn und Zweck des Gesetzes als gedeckt betrachtet werden können. So ja auch die derzeitige Lesart des Gesetzes für Case Management in der Praxis.

Die Regelungen betreffend der Einzelfallentscheidungen werden für die Datenbearbeiter ausserdem einschränkende Auswirkungen haben. Diese sind so gering wie möglich zu halten. Generell soll eine Informationspflicht ausreichend sein und keine weitergehenden Rechte der betroffenen Person mit sich bringen.

Mit der Verschärfung der Schweigepflicht wird jede unbefugte Offenlegung von geheimen Personendaten unter Strafe gestellt (vgl. Art. 52 VE-DSG). Diese verschärfte Schweigepflicht führt dazu, dass bei geheimen Personendaten bei der Bekanntgabe an Dritte faktisch immer eine Zustimmung der betroffenen Person, ein überwiegendes Interesse oder eine gesetzliche Offenlegungspflicht gegeben sein muss. Dies führt dazu, dass allenfalls eine Zustimmung notwendig ist, obwohl die Datenbearbeitungsgrundsätze keine solche vorsehen.

Während das geltende DSG die Sorgfaltspflichten in Art. 7 DSG ganz allgemein regelt, enthält der VE-DSG in Art. 16 ff. einen umfangreichen Katalog von Pflichten. Diese umfangreichen neuen Pflichten sind teilweise gar nicht umsetzbar und bringen für die betroffenen Personen keinen Nutzen. Ausserdem tragen sie der künftigen Digitalisierung der Datenbearbeitungen nicht Rechnung. Vielmehr sollte die Tendenz von strengeren Einwilligungsvorschriften hin zu mehr und klareren Informationspflichten des Datenbearbeiters hin erfolgen.

4. Fazit

curafutura unterstützt die Revision des Datenschutzgesetzes unter der Berücksichtigung der oben genannten Punkte. Das revidierte DSG wird nach der Verabschiedung der Botschaft in den zugehörigen bundesrätlichen Verordnungen konkretisiert. Da diese Verordnungen bereits heute von grosser Tragweite sind, begrüsst es curafutura sehr, wenn zu diesen Entwürfen zu gegebener Zeit ebenfalls wieder die Möglichkeit für eine Stellungnahme besteht.

Für die Kenntnisnahme und Berücksichtigung unserer Stellungnahme danken wir Ihnen, sehr geehrte Frau Bundesrätin, bestens.

Freundliche Grüsse

curafutura

Pius Zängerle
Direktor

Luca Petrini
Projektleiter Gesundheitspolitik

Gutenbergstrasse 14, CH-3011 Bern, +41 31 310 01 80, info@curafutura.ch, www.curafutura.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 curafutura

Name / Firma / Organisation : **curafutura**, das sind die folgenden Versicherungen
- Helsana
- CSS
- KPT
- Sanitas

Adresse : Gutenbergstrasse 14, 3011 Bern

Kontaktperson : Luca Petrini

Telefon : 031 310 07 92

E-Mail : luca.petrini@curafutura.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!

ENTWURF

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 2
Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 2
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 Fehler! Textmarke nicht definiert.
Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten Fehler! Textmarke nicht definiert.
Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") Fehler! Textmarke nicht definiert.
Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" Fehler! Textmarke nicht definiert.

Allgemeine Bemerkungen	
Name/Firma	**Bemerkung/Anregung**
curafutura	Wir verweisen auf unser separates Schreiben vom 4. April 2017.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)					
Name/Firma	**Gesetz**	**Art.**	**Abs.**	**Bst.**	**Bemerkung/Anregung**
curafutura	VE-DSG	3		j.	Definition betrieblicher Datenschutzbeauftragter: Antrag: Eine Aufnahme der Definition des betrieblichen Datenschutzbeauftragten bzw. des Datenschutzverantwortlichen sollte ins Gesetz aufgenommen werden. Der betriebliche Datenschutzbeauftragte soll den EDÖB in seinen Aufsichtspflichten entlasten, was der Datenschutz-Governance im Betrieb zu Gute kommt. Im Gegenzug muss dies zu einer Befreiung von gewissen Pflichten führen (niederschwellige interne Datenschutzverletzungen bzw. Datenschutzfolgeabschätzungen mit ebensolchen Risiken müssen einzig an den betrieblichen Datenschutzbeauftragten gemeldet werden).

ENTWURF

					Die Definition hat sich an der heutigen in Art. 12a und 12b VDSG zu orientieren. Definition Profiling: Die Definition von Profiling in Art. 3 lit. f VE-DSG geht deutlich über die EU-Regelung hinaus. Antrag: Die Begriffsdefinition ist enger zu fassen. Sie darf nicht jede Auswertung erfassen und nicht weitergehen als in der EU-DSGVO, wo nur die **automatisierte** personenbezogene Auswertung darunter fällt.
curafutura	VE-DSG	4	6		**Grundsätze** Antrag: «[6] … Für die Bearbeitung von besonders schützenswerten Personendaten ~~und das Profiling~~ muss die Einwilligung zudem ausdrücklich erfolgen.» Begründung: Der Vorschlag ist eindeutig eine klare Verschärfung zum geltenden Recht, da bis anhin bei der Bearbeitung von Persönlichkeitsprofilen nicht in jeder Konstellation eine Einwilligung erforderlich war. Selbst bei der Möglichkeit einer Rechtfertigung ist die Vermutung einer Persönlichkeitsrechtsverletzung im Vergleich zum geltenden Recht ein Nachteil. Eine solche Regelung wäre zudem innovationsfeindlich, behinderte oder verhinderte gar unnötig personalisiertes Marketing, sowie Big Data. Schweizerische Unternehmen könnten durch diese Bestimmung allenfalls einen Wettbewerbsnachteil erleiden.

ENTWURF

curafutura	VE-DSG	5	5		**Bekanntgabe ins Ausland** 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: Diese Frist von sechs Monaten ist für ein 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.
curafutura	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).
curafutura	VE-DSG	6	2		**Bekanntgabe ins Ausland in Ausnahmefällen** Antrag: Streichen von Art. 6 Abs. 2 VE-DSG Begründung:

ENTWURF

					Wir verweisen auf die Überlegungen zu Art. 5 Abs. 6 VE-DSG.
curafutura	VE-DSG	8	1-3		**Empfehlungen der guten Praxis** Antrag: Der Beauftragte gibt selbst keine rechtsverbindlichen Empfehlungen der guten Praxis ab, jedoch können interessierte Kreise ihre eigenen Empfehlungen vom Beauftragten genehmigen lassen. Begründung: Es gibt keine Veranlassung, um von der heutigen bewährten Praxis abzuweichen. Unzulässige und rechtsstaatlich problematische Vermischung der Kompetenzen von Gesetzgeber und Aufsichtsbehörde. Zumal solche Empfehlungen des EDöB gerichtlich gar nicht überprüfbar wären (Fehlen des Verfügungscharakters).
curafutura	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. Es wird vorgeschlagen, die Regelung an anderer Stelle aufzunehmen, insbesondere im Personenrecht (ZGB).

ENTWURF

curafutura	VE-DSG	13	1		**Informationspflicht bei der Beschaffung von Personendaten** Antrag: Streichen bzw. Anpassen von Art. 13 Abs. 1 VE-DSG sowie der mit dieser Bestimmung verbundenen Strafbestimmung Begründung: Eine Vereinheitlichung der Informationspflicht beim Beschaffen von *besonders schützenswerten Personendaten* und *Persönlichkeitsprofilen (neu: Profililing)* ist nicht grundsätzlich abzulehnen. Die Bestimmung von Art. 13 Abs. 1 E-DSG stellt jedoch eine klare Verschärfung gegenüber den heutigen Art. 14 und Art. 18a DSG dar, da sie die Informationspflicht auf alle personenbezogenen Informationen ausdehnt. Die geplante Verschärfung ist daher abzulehnen, insbesondere auch die strafrechtlich massive Sanktionierung, die sogar Fahrlässigkeit umfasst. Eine Informationspflicht bei der Beschaffung von Daten bei Dritten ist nicht praxistauglich. Diese zusätzliche Informationspflicht wäre mit einem unverhältnismässigen administrativen Aufwand mit entsprechenden Kosten verbunden. Wenn beispielsweise ein Versicherungsunternehmen Adressen von natürlichen Personen über einen Adressbroker einkauft, welche noch keine Kunden (Versicherungsnehmer, versicherte Personen) sind, so müsste der Verantwortliche (also das Versicherungsunternehmen) die betroffenen Personen im Zeitpunkt der Speicherung der Daten informieren. Im Bereich der Kollektivversicherungen wäre die Informationspflicht gar nicht umsetzbar.
curafutura	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:

ENTWURF

					Eine Pflicht des Verantwortlichen, die betroffenen Personen über die Identität und Kontaktdaten sämtlicher eingesetzter Auftragsbearbeiter zu informieren, geht viel zu weit. Deren Umsetzung ist nicht praktikabel: Für die Verantwortlichen wäre eine solche Pflicht mit einem enormen Aufwand verbunden, weil die eingesetzten Auftragsbearbeiter oft ändern und gerade grosse Auftragsbearbeiter – wie z.B. Salesforce – eine sehr grosse Anzahl von Subakkordanten einsetzen, die auch von dieser Pflicht erfasst wären. Eine solche Informationspflicht dürfte kaum zum Datenschutz der betroffenen Personen beitragen. Informationspflichten, die über Wesentliches hinausgehen, bewirken kaum Aufklärung oder ein mehr an Datenschutz, sondern eher Verwirrung. Es besteht die Gefahr, dass Wichtiges neben Unwichtigem untergeht. Eine allgemeine Informationspflicht, dass Auftragsbearbeiter eingesetzt werden, ist absolut ausreichend.
curafutura	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 ist per Definition eine Bekanntgabe von Daten an Dritte. Die Einschränkung der Informationspflicht muss gewährleistet sein und darf bspw. durch Weitergabe/Bekanntgabe innerhalb der Konzerngesellschaften (Dritte) nicht vereitelt werden. Die Einschränkung der Informationspflicht muss allein aufgrund überwiegender privater Interessen möglich bleiben.
curafutura	VE-DSG	15	2		**Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung** Antrag:

ENTWURF

					«[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung ~~und zu den bearbeiteten Personendaten~~ zu äussern.» Begründung: Die Anhörungspflicht bezüglich der bearbeiteten Daten geht zu weit und wäre in der Praxis äusserst aufwändig. Zumal der versicherten Person das Auskunftsrecht nach Art. 20 VE-DSG ja jederzeit kumulativ zur Verfügung stehen.
curafutura	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.» Begründung: 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.
curafutura	VE-DSG	16	3		**Datenschutz-Folgenabschätzung** Antrag: Streichen von Art. 16 Abs. 3 VE-DSG sowie der mit dieser Bestimmung verbundenen Strafbestimmungen. Begründung: Eine Benachrichtigung des EDÖB wird durch E-SEV 108 nicht vorgeschrieben (siehe Art. 8bis Abs. 2 E-SEV 108). Sie ist praxisfern und führt zu einer massiven Behinderung bei der Datenbearbeitung und einer massiven Mehrbelastung des EDÖB.

ENTWURF

curafutura	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.
curafutura	VE-DSG	17	1		**Meldung von Verletzungen des Datenschutzes** Antrag: -"unbefugte Datenbearbeitung" ist analog EU-DSGVO durch "Verletzung einer getroffenen Sicherheitsmassnahme, dass zu einem Gewahrsamsbruch/Verlust an den Daten führt" zu ersetzen. -Die Bestimmung ist wie folgt zu ergänzen: "…nicht zu einem hohen Risiko…" führt. -Löschen der Strafbewehrung dieser Bestimmung. -unverzüglich ist zu löschen bzw. allenfalls durch "binnen 72 Stunden" analog EU-DSGVO zu ersetzen. Begründung: Die Umstände der Meldepflicht sollte bereits aus Gründen der Rechtsicherheit analog EU-DSGVO übernommen werden bzw. mindestens auf dieses Niveau gesenkt werden. Die hier vorgeschlagene Regelung würde zu einer unsinnigen Meldeflut an den EDÖB führen und die strafrechtlichen Sanktionen zu einem unverhältnismässigen Druck und zu einer Angstkultur in den Betrieben, was dem Datenschutz keineswegs förderlich wäre.
curufutura	VE-DSG	19		b.	**Weitere Pflichten** Antrag:

ENTWURF

					Streichen von Art. 19 Bst. b VE-DSG sowie der mit dieser Bestimmung verbundenen Strafbestimmungen Begründung: Art. 19 lit. b VE-DSG ist in der Praxis nicht umsetzbar. Denn es ist nicht möglich, jederzeit sämtliche Empfänger/innen über sämtliche in der Bestimmung erwähnten Schritte (Berichtigung, Löschung oder Vernichtung von Daten, etc.) zu informieren. Kein Unternehmen führt akribisch Buch, welche Personendaten wann genau im Einzelfall übermittelt werden. Wenn die Unternehmen neu verpflichtet würden, die Empfänger/innen von Personendaten über die in Art. 19 lit. b VE-DSG aufgeführten Schritte zu informieren, wären sie gezwungen, unzählige umfangreiche Prozesse mit einem völlig unverhältnismässigen und äusserst kostspieligen Aufwand aufzusetzen. Und selbst dann könnte eine fehlerfreie Umsetzung der Bestimmung aufgrund der Komplexität nicht garantiert werden. Zudem ist unklar, welcher Aufwand im Einzelfall noch verhältnismässig wäre, da unbekannt ist, welche Kriterien denn zur Prüfung der Verhältnismässigkeit herangezogen werden müssten. Festgehalten werden kann jedoch, dass bereits der Initialaufwand in den Unternehmen zur Aufsetzung der notwendigen Prozesse als absolut unverhältnismässig bezeichnet werden muss. Eine Informationspflicht, wie in Art. 19 Bst. b VE-DSG vorgesehen, wird notabene durch E-SEV 108 nicht vorgeschrieben (siehe Seite 65 erläuternder Bericht).
curafutura	VE-DSG	20	2	g.	**Auskunftspflicht an Betroffene bei Nutzung von Auftragsbearbeitern** Antrag: «gegebenenfalls die Informationen **nach Artikel 13 Abs. 3.**» Begründung: 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.
curafutura	VE-DSG	20	3		**Auskunftspflicht bei einer Entscheidung aufgrund einer Datenbearbeitung**

ENTWURF

					Antrag: Streichen von Art. 20 Abs. 3 VE-DSG sowie der mit dieser Bestimmung verbundenen Strafbestimmungen Begründung: 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. Beispiel: Bezüglich der Prämien 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).
curafutura	VE-DSG	23	2	d.	**Persönlichkeitsverletzungen**

ENTWURF

					Antrag: «d. durch Profiling ohne ~~ausdrückliche Einwilligung~~ **Information** der betroffenen Person.» Begründung: curafutura anerkennt, dass eine Erhöhung der Transparenz über die Datenbearbeitungen ein Anliegen der Vernehmlassungsvorlage ist. Auch in Bezug auf Profiling sollte eine entsprechende Information genügen. Mit einer Information kann der Konsumentendatenschutz genügend gewährleistet werden. Eine Information steht zudem im Einklang mit dem Gebot zur Wahl der mildesten Massnahme. Die Informationspflicht sollte analog den Erläuterungen zu Art. 13 VE-DSG ohne Formerfordernis erfüllbar sein (siehe Seite 56 Erläuternder Bericht). Eine ausdrückliche Einwilligung ist nicht durchführbar, insbesondere bei Bestandeskunden. Versicherungsverträge sind vielfach lange Zeit in Kraft. Das heisst, gibt ein bestehender Kunde seine Einwilligung nicht oder widerruft er diese, müsste dieser Kunde von jedem weiteren Profiling ausgenommen werden. Dies ist in der Praxis nicht umsetzbar und geht weiter als die europäischen Bestimmungen. Diese Bestimmung schädigt die Geschäftstätigkeit einer Versicherung erheblich.
curafutura	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: Die vorgeschlagene Formulierung ist zu unbestimmt. curafutura 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.

ENTWURF

curafutura	VE-DSG	27			Die Bestimmung fordert im Bereich der obligatorischen Unfall- und Krankenversicherung für das Profiling und die automatisierten Einzelfallentscheidung eine Grundlage in einem Gesetz im formellen Sinn. Art. 27 Abs. 2 VE-DSG erweist sich damit in diesem Bereich als praxisfremd und schiesst über das Ziel hinaus: Antrag: Art. 27 Abs. 2 VE-DSG ist wie folgt anzupassen: "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". Diese Systematik entspricht zudem Ziffer 42 des Anhangs zum VE-DSG, wonach "Profiling" keine Erwähnung findet. Damit verbunden ist der Antrag auf ersatzlose Streichung von Art. 23 Abs. 2 lit. d VE-DSG im Bereich der Zusatzversicherungen nach VVG (ausdrückliche Einwilligung für Profiling). 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 autom. Einzelfallentscheide/Profiling ist im Bereich der Grundversicherung nach KVG 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. Beispiel: Die Identifikation und Bearbeitung von Hoch- und Höchstkostenfällen bedingt, dass der Versicherer seinen Datenbestand unter Anwendung eines einschlägigen Regelwerks bearbeiten darf. Die Zulässigkeit der Durchführung eines Case Managements dürfte ebenso unbestritten sein wie das Faktum,

ENTWURF

					dass Case Management einen wichtigen Beitrag zur Reduktion der Kranken- und Unfallversicherungskosten leistet. Dennoch enthält das KVG bereits heute nicht eine einzige gesetzliche Bestimmung über Case Management. Die effiziente Abwicklung des Krankenversicherungsgeschäfts als Massengeschäft bedingt einen sehr hohen Automatisierungsgrad. Die Leistungsprüfung erfolgt damit zu einem sehr hohen Anteil vollautomatisch anhand vordefinierter Regelwerke. Das KVG enthält jedoch keine entsprechenden Grundlagen.
curafutura	VE-DSG	36			**Register** Antrag: Die bisherige bewährte Praxis für die Bundesorgane (OKP-Versicherer) ist beizubehalten, wonach mit Bestellung eines internen Datenschutzbeauftragten die Pflicht zur Meldung der Datensammlungen gegenüber dem EDöB entfällt. Stattdessen muss es ausreichen, wenn der interne Datenschutzbeauftragte ein solches Register führt.
curafutura	VE-DSG	41			**Untersuchung** Das bisherige System mit Sachverhaltsabklärungen, Empfehlungen und Klagen vor Bundesverwaltungsgericht hat sich in der Praxis bestens bewährt, weshalb es ohne Not nicht geändert werden sollte.
curafutura	VE-DSG	42	3		**Verfahren** Antrag: «[3] Beschwerden gegen vorsorgliche Massnahmen nach Art. 42 kommt ~~keine~~ aufschiebende Wirkung zu.» Begründung:

ENTWURF

					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).
curafutura	VE-DSG	50ff			Die Strafbestimmungen gegen einzelne Personen und Organe sind unverhältnismässig und führen zu einem unnötigen Druck. Stossend ist insbesondere auch die Strafbarkeit von fahrlässigen Verstössen. Die Ausgestaltung der Strafbestimmungen ist generell zu überarbeiten.
curafutura	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 gar nicht nötig, da die Verletzung dieser Pflicht durch die neue Bestimmung von Art. 54 Abs. 1 lit. d KVAG mit Bussen bis CHF 500'000.— heute bereits scharf sanktioniert ist.

ENTWURF

					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.
curafutura	VE-DSG	59			**Übergangsbestimmung** Antrag: Es ist eine **generelle** Übergangsbestimmung für die Umsetzung des revidierten DSG aufzunehmen (keine Beschränkung auf einzelnen Bestimmungen). Es ist eine angemessene Übergangsfrist für die Umsetzung des revidierten DSG von zwei Jahren vorzusehen. Keine Rückwirkung oder beschränkte Rückwirkung ist zu prüfen und auszuformulieren. Begründung: Die Vernehmlassungsvorlage sieht keine umfassenden Übergangsbestimmungen 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.
curafutura	42. KVG				Antrag: Dem Antrag unter Art. 27 VE-DSG folgend, ist auf das Wort "Profiling" zu verzichten. Begründung:

ENTWURF

					Vgl. Art. 27 VE-DSG Beispiel: Grosse Auswirkung in der Praxis: Jeder Krankenversicherer muss in der Lage bleiben, seine Daten z.B. zum Zweck der Identifikation von CM-Potential (Profiling) etc. bearbeiten zu können.
curafutura	VAG	45	1	e.	Antrag: Streichen von Art. 45 Abs. 1 Bst. e VAG Begründung: Das Versicherungsaufsichtsgesetz (VAG) ist nicht Bestandteil der Vernehmlassungsvorlage. curafutura 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.
curafutura	VVG	3	1	g.	Antrag: Streichen von Art. 3 Abs. 1 Bst. g VVG Begründung: Das Versicherungsvertragsgesetz (VVG) ist nicht Bestandteil der Vernehmlassungsvorlage. curafutura 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.

ENTWURF

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zürich, im März 2017

Vernehmlassung zur Totalrevision des Bundesgesetzes über den Datenschutz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Das Datenschutz-Forum Schweiz wurde im September 1999 als Verein mit dem Zweck gegründet, die praktische Umsetzung sowie die Forschung auf dem Gebiet des Datenschutzes und der Datensicherheit zu fördern. Seit nunmehr 18 Jahren geschieht dies insbesondere durch den Informations- und Erfahrungsaustausch unter den am Datenschutz interessierten Personen aus allen Fachrichtungen der Wirtschaft, der öffentlichen Verwaltung und der Wissenschaft.

Das Datenschutz-Forum stellt betroffenen Personen, Datenbearbeitenden, Behörden, Politikern und Medien Informationen sowie Unterlagen für die Meinungsbildung und Entscheidungsfindung in Datenschutz- und Datensicherheitsfragen zur Verfügung. Es fördert die Aus- und Weiterbildung auf diesem Gebiet und pflegt Kontakte zu Organisationen mit gleichen Zielsetzungen.

Vor diesem Hintergrund nehmen wir gerne die Gelegenheit wahr, uns am Vernehmlassungsverfahren zur Totalrevision des Bundesgesetzes über den Datenschutz (DSG) zu beteiligen und dazu aus unserer Sichtweise Stellung zu nehmen. Das Datenschutz-Forum Schweiz hat sich dabei nur auf diejenigen Normen des Vorentwurfs konzentriert, welche stark nachbesserungsfähig sind.

1. Stellungnahme zu einzelnen Normen

Art. 3 Bst. c Ziff. 2 E-DSG (Begriff): Zu den besonders schützenswerte Personendaten wird die Zugehörigkeit zu einer Rasse aufgezählt. Tatsache ist, dass es keine Menschenrassen gibt und dass somit keine Person aufgrund ihrer „Rasse" identifiziert werden kann. Rassismus, um den es entgegen dem Wortlaut geht, stellt im Strafgesetzbuch korrekterweise einen Straftatbestand dar. Mit der Bezeichnung „Zugehörigkeit zu einer Rasse" wird bereits impli-

ziert, dass es Menschenrassen gibt. Deshalb sollte dieser Begriff aus dem Gesetz gestrichen werden. Das Gleiche gilt für die Zugehörigkeit zu einer Ethnie, die in der bunten Schweiz des 21. Jahrhunderts veraltet wirkt. Besonders schützenswert sind dagegen Personendaten, die sich mit der Abstammung (Adoption, leibliche Eltern usw.) gemäss BGE 128 I 63 auseinandersetzen. Diese sollten jedoch aus systematischen Gründen als materielle Datenschutznormen im ZGB geregelt werden, damit sie nicht aus den ursprünglichen Zusammenhang gerissen werden können.

Art. 3...E-DSG (Begriff betriebliche/r Datenschutzbeaufte/r): Das heutige, in der zugehörigen Verordnung geregelte Institut des betrieblichen Datenschutzbeauftragten hat sich in der Praxis sehr bewährt. Wir regen an, dieses auch im revidierten Gesetz aufzunehmen und zu definieren. Weiterhin soll die Einführung eines betrieblichen Datenschutzbeauftragten freiwillig und in der Folge mit gewissen Erleichterungen (interne Meldepflichten, Befreiung von gewissen Pflichten etc.) verbunden sein.

Art. 8 E-DSG (Empfehlung der guten Praxis): Best-Practice-Empfehlungen gehören aus systematischen Gründen nicht auf Gesetzesstufe. In der Regel sind sie für Behörden in Richtlinien, Empfehlungen, Amtspraxis oder Kreisschreiben verankert und können durch Gerichtsinstanzen frei überprüft werden. Auch Private können sie in geeigneter Form im Betrieb verankern. Das soll u.E. so beibehalten werden.

Zudem ist es in der Praxis mit sehr hohem Aufwand verbunden, wenn Verantwortliche ihre Empfehlungen dem EDÖB (Beauftragten) zur Genehmigung vorlegen. Um eine solche Aufgabe korrekt vornehmen zu können, braucht der EDÖB vertieftes Wissen über die Behörden und privaten Unternehmen, über das er in der Regel nicht verfügt. Eine vom EDÖB genehmigte Best-Practice-Empfehlung gibt keine Garantie, wie Datenschutz in der Praxis gelebt wird und kann falsche Signale nach Aussen senden. Private und Behörden können Datenschutzexperten (interne, externe) für solche Aufgaben beauftragen oder sich zertifizieren lassen. Diese Norm ist ersatzlos zu streichen.

Art. 12 E-DSG (Daten einer verstorbenen Person): Mit dieser Norm wird das Amts- und Berufsgeheimnis (v.a. das Arztgeheimnis) in zu hohem Masse unterwandert. Deshalb lehnen wir die Norm in dieser Form ab. Es ist die Revision des Erbrechts abzuwarten und der digitale Tod als materielle Datenschutznorm im ZGB zu regeln.

Art. 15 E-DSG (Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung): Die Informationspflicht begrüssen wir, die Anhörungspflicht ist jedoch pra-

Datenschutz-Forum Schweiz
www.datenschutz-forum.ch
c/o Ursula Uttinger, Hotzestrasse 35, 8006 Zürich
Phone: +41 79 682 35 09

xisfern und führt zu bürokratischem Leerlauf. Die Anhörungspflicht ist deshalb ersatzlos zu streichen.

Art. 17 E-DSG (Meldung von Verletzungen des Datenschutzes): Eine Meldung ist ausschliesslich ratsam angezeigt, wenn ein Verstoss gegen Sicherheitsmassnahmen im Unternehmen vorliegt. Auch die Information der betroffenen Person ist zu begrüssen, wenn dies zum Schutz dieser Person nötig ist. Es ist nicht ersichtlich, was in einem konkreten Fall die zusätzliche Information an den EDÖB bringen soll, auch nicht, weshalb die Meldepflicht weit über diejenige der EU-DSGVO hinausgeht. Die Norm ist praxisfern und bedeutet einen Mehraufwand für die Unternehmen und für den Beauftragten - ohne effektiven Nutzen. Wir empfehlen, alles was über die EU-DSGVO hinausgeht, ist aus Art. 17 E-DSG zu streichen.

Art. 20 E-DSG (Auskunftsrecht): Die Ausdehnung des Geltungsbereichs des Auskunftsrechts auf alle prozessrechtliche Verfahren ist zu streichen. Ansonsten ist zu befürchten, dass die verfahrensrechtliche Akteneinsicht unterlaufen und damit dem Rechtsmissbrauch Vorschub geleistet wird.

Art. 23 Abs. 2 Bst. d E-DSG (Profiling): Beim Profiling ist es nicht möglich, jederzeit eine ausdrückliche Einwilligung einzuholen, deshalb kann in diesen Fällen nicht automatisch von einer Persönlichkeitsverletzung ausgegangen werden. Problematisch ist Profiling bei der automatischen Datenbearbeitung. Im Gegensatz zur EU-DSGVO, welche nur die automatische Datenbearbeitung regelt, umfasst das DSG jede Datenbearbeitung, auch von Hand. Deshalb schiesst die Norm weit über das Ziel hinaus. Art. 23 Abs. 2 Bst. d E-DSG sollte sich auf das Profiling bei der automatischen Datenbearbeitung beschränken und nicht weiter gehen als die EU-DSGVO.

Art. 24 Abs. 2 E-DSG (Rechtfertigungsgründe): Die Formulierung „möglicherweise" ist äusserst schwammig formuliert, wie wäre es mit „der bearbeitenden Person ...fällt insbesondere in Betracht..., wenn"

Art. 40 Abs. 2 E-DSG (Aufsicht): Diese Norm unterstellt anderen Bundesbehörden mangelnde Datenschutzkompetenz. Dabei stützen diese Behörden ihre Verfügungen regelmässig auf materielle Datenschutznormen ab, wo sie über das entsprechende Fachwissen ver-

fügen. Der entsprechende Absatz ist ersatzlos zu streichen, da er unnötig das Verfahren verlängert.

Artikel 50 – 55 E-DSG (Absatz: Strafbestimmungen):
Die vorgesehenen Strafbestimmungen dienen nicht dem primären Schutz der Persönlichkeit der betroffenen Personen. Vielmehr soll im DSG die vorsätzlich zweckwidrige und/oder unverhältnismässige Datenbearbeitung sanktioniert werden. Eine persönliche Strafbarkeit der Mitarbeitenden entspricht auch nicht der Regelungen in anderen Gesetzen (vgl. KG, UWG, FMG, BEHG), bei welchen der Fokus klar auf der Bestrafung der Unternehmen liegt. Wir schlagen daher Folgendes vor:

- Statt Strafverfahren sind Verwaltungssanktionen das geeignete Mittel.
- Die fahrlässige Begehung eines Tatbestandes soll nicht strafbar sein.
- Sanktioniert werden sollen die „Verantwortlichen" und nicht die einzelnen Mitarbeitenden eines Unternehmens. Das DSG soll bei Verstössen gegen die Datenschutzbestimmungen eine Sanktionierung der Unternehmen vorsehen.

ZGB Beweislastumkehr: Die Beweislastumkehr ist ein äusserst wichtiges Betroffenenrecht, um Schadensersatz (materieller und immaterieller) aufgrund einer rechtswidrigen Personendatenbearbeitung geltend zu machen. Dieses Betroffenenrecht fehlt bei den vorgesehen Änderungen des ZGB. Ein Betroffener kann schwer beweisen, dass Profiling rechtswidrig durchgeführt wurde und insbesondere besonders schützenswerte Daten, beispielsweise über die Gesundheit, rechtswidrig verarbeitet wurden. Wir schlagen vor, dass die Beweislastumkehr in das ZGB aufgenommen wird, denn bekanntermassen ist heute das Prozessrisiko so gross, dass die Betroffenen sich scheuen, dieses einzugehen. Zudem sind die Betroffenenrechte in der EU-DSGVO damit immer noch wesentlich stärker ausgebaut als in der Schweiz.

2. Fazit

Es ist unbestritten, dass das Bundesgesetz über den Datenschutz eine Totalrevision benötigt. Die Bevölkerung soll darauf vertrauen dürfen, dass sie im zunehmend global ausgerichteten digitalen Markt nicht komplett von Unternehmen erfasst wird und ihre persönlichen Daten von diesen nicht zweckentfremdet werden.

Datenschutz-Forum Schweiz
www.datenschutz-forum.ch
c/o Ursula Uttinger, Hotzestrasse 35, 8006 Zürich
Phone: +41 79 682 35 09

Der Vorentwurf vom 21. Dezember 2016 zum DSG und die Änderung weiterer Erlasse bieten nach unserer Auffassung *keine Lösungen an für die Herausforderungen, die sich durch den technischen Fortschritt, die dadurch gestiegene Komplexität und den globalisierten Informationsaustausch ergeben.* Die technischen Innovationen des letzten Jahrzehnts wie Internet der Dinge, Suchtechnologien und Analyseauswertungen wie Big Data sind bei einer zeitgemässen und zukunftsorientierten Gesetzgebung zu berücksichtigen. Für die mit Personendaten handelnden globalen Unternehmen braucht es auch in der Schweiz durchsetzbare Datenschutz- und Datensicherheitsregeln. Der Staat hat griffigere Normen zu entwickeln, damit die Betroffenen ihre Rechte effektiv wahrnehmen können; und er hat den Unternehmen gleichzeitig Rechtsicherheit zu bieten ohne ausufernde Bürokratie. Die Europäische Union hat dagegen mit ihrer Datenschutz-Grundverordnung (DSGVO) zumindest teilweise Regelungen für den digitalen Markt gefunden.

Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte erhält durch den Vorentwurf mehr Kompetenzen und vor allem einen stark erweiterten Aufgabenkatalog. Wir befürchten, dass ihm damit keine Zeit mehr verbleibt, seine Kerntätigkeiten wahrzunehmen.

Freundliche Grüsse

Ursula Uttinger, Präsidentin

DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Bundesamt für Justiz
z. H. Jonas Amstutz
Bundesrain 20

3003 Bern

30. März 2017

Vernehmlassungsantwort: Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse zum Datenschutz (SR 235.1)

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Am 21. Dezember 2016 haben Sie das Vernehmlassungsverfahren über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz eröffnet.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur sowie weitreichende Transparenz und Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft auf dem Hintergrund der Persönlichkeits- und Menschenrechte. Gerne nehmen wir zum Vorentwurf wie folgt Stellung.

Die Digitale Gesellschaft begrüsst die Vorlage ausdrücklich und ist mit der Stossrichtung, die der Bundesrat eingeschlagen hat, einverstanden.

Zusätzlich zu den geplanten Strafbestimmungen (oder als Ersatz) sind jedoch sinnvollere und griffige **Verwaltungssanktionen** sowie ein **Verbandsbeschwerderecht** zur Stärkung der Rechte der betroffenen Personen und zur Entlastung des Beauftragten vorzusehen. In Gerichtsverfahren zu schwerwiegenden Fällen sind die Verantwortlichen zudem zu einer angemessenen und beschleunigenden Mithilfe durch eine **Beweislastumkehr** zu verpflichten.

Nicht nur private Verantwortliche oder Bundesorgane sollen zu Datenschutz-Folgeabschätzungen verpflichtet werden. Auch beim Erlass neuer Gesetze muss dem Datenschutz und dem Schutz der Persönlichkeitsrechte mehr Beachtung geschenkt werden. Entsprechend sind auch **Datenschutz-Folgeabschätzungen im**

Gesetzgebungsprozess vorzusehen. Gesetze, welche eine Überwachung von Personen beinhalten, müssen zudem nach den ersten fünf Jahren seit Inkrafttreten zwingend einer **Evaluation, welche die Wirksamkeit und Verhältnismässigkeit prüft**, unterzogen werden.

Diese und weitere Änderungsvorschläge finden Sie in der ausführlichen Vernehmlassungsantwort zu den einzelnen Gesetzesartikeln.

Wir bedanken uns für die Berücksichtigung unserer Anmerkungen und Vorschläge.

Mit freundlichen Grüssen

Erik Schönenberger

Vernehmlassungsantwort der Digitalen Gesellschaft:
Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse zum Datenschutz (SR 235.1)

Art. 2 – Räumlicher Geltungsbereich

Im Gegensatz zur neuen Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) enthält der vorliegende Entwurf zum revidierten Datenschutzgesetz (DSG) keine besondere Bestimmung zum räumlichen Geltungsbereich. 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 Inhaber von Datensammlungen – nach heutiger Terminologie – vergleichbar, die komplett aus dem Ausland operieren, sich aber an Personen in der Schweiz richten. Zu erwähnen sind etwa Amazon (unter anderen mit Amazon Web Services), Facebook (auch mit Instagram und WhatsApp), Google (unter anderem mit Gmail, Google Analytics und YouTube), LinkedIn, Microsoft (unter anderem mit Office 365), Twitter, Salesforce und XING.

In all diesen Fällen kann – im Unterschied zur neuen EU-DSGVO – 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 der neuen EU-DSGVO entsprechendes *Marktortprinzip* muss daher vorgesehen werden. Damit würde dann auch ein in der Schweiz nötiges, vergleichbares Datenschutzrecht gelten.

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.

Art. 3 lit. a – Personendaten

Der erläuternde Bericht hält in der Definition zum Begriff «bestimmbare Person» folgendes fest:

«Wie auch nach dem aktuellen Recht reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei bestimmbar. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Die zur Verfügung stehenden technischen Möglichkeiten werden in Bezug darauf geprüft, wie hoch der zeitliche und finanzielle Aufwand für ihre Anwendung ist. Mit Blick auf die immer gezielteren Technologien zur Datenauswertung und deren konstante Weiterentwicklung verschwimmt die Grenze zwischen Personendaten und anderen Daten indes zusehends. Daten, bei denen heute noch eine rein theoretische Möglichkeit der Identifizierung anzunehmen ist, können morgen vielleicht bereits einer bestimmbaren Person zugeordnet werden.»

Es genügt nicht, wenn besonders schützenswerte Personendaten bearbeitet, Dritten bekannt gegeben und veröffentlicht werden dürfen, sofern die Möglichkeit besteht, dass sich diese Personendaten allenfalls zukünftig deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann.

Insbesondere in der Forschung, Planung und Statistik sind Konzepte, wie Differential Privacy seit langem bekannt. Mithilfe von Noise Injection lassen sich beispielsweise Daten so verfremden, dass sie zwar statistisch weiterhin auswertbar sind, sie aber keine verlässlichen Rückschlüsse auf Personen mehr zulassen.

Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten.

Art. 3 lit. c Ziff. 4 – Biometrische Daten

Biometrische Merkmale lassen 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. Wenn

folglich biometrische Merkmale zur Identifizierung geeignet sind oder zur Identifikation 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). Der Absatz ist zu ergänzen mit:

«Die Bearbeitung personenbezogener Daten sowie die Auswahl und Gestaltung der Datenbearbeitungssysteme sind dahin gehend 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.

Übermittelt die betroffene Person (wie beispielhaft im erläuternden Bericht festgehalten) ihre Adresse im Hinblick auf den Erhalt einer Kundenkarte, so mag die Weiterbenutzung dieser Adresse durch das betreffende Unternehmen zu Werbezwecken im Rahmen einer anfänglich erkennbaren Zweckbestimmung liegen. Findet die Übermittlung im Rahmen einer Bestellung (online oder nicht) statt, sollte jedoch nicht davon ausgegangen werden können.

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», der nicht abgelehnt werden kann, ist für die betroffene Person wenig hilfreich. Es muss auch jederzeit die Möglichkeit des Widerrufs einer Einwilligung gegeben sein. Zudem müssen Personen in einem Abhängigkeitsverhältnis

vor unwillentlich abgegebenen und unverhältnismässigen Zustimmungen geschützt werden (zum Beispiel Arbeitnehmer vor Pauschalvollmachten 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 ein entsprechendes 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. Wir erwarten vom Bundesrat, dass die erwähnten technischen und organisatorischen Schutzmassnahmen mindestens auf Verordnungsstufe konkretisiert werden.

Art. 12 – Daten einer verstorbenen Person

Die neue Bestimmung über «Daten einer verstorbenen Person» wird begrüsst.

Art. 13 Abs. 3 und 4 – Informationspflicht bei der Beschaffung von Personendaten

Die Bestimmungen gilt auch für die Auskunftspflicht nach Art. 20 Abs. 2 lit. g. Zur Erfüllung der *Informationspflicht* ist die Bekanntgabe der Kategorien der bearbeiteten Daten, der Kategorien der zur Auftragsbearbeitung übergebenen Daten und der Kategorien der Datenempfänger ausreichend. Die *Auskunftspflicht* hingegen muss aber neben den Daten auch die Empfänger der Daten – und nicht nur deren Kategorien umfassen. Eine Unterscheidung der Auskunftspflicht und der Informationspflicht ist

daher (in Art. 20) sinnvoll.

Art. 14 Abs. 3 und 4 – Ausnahmen von der Informationspflicht und Einschränkungen

Die Einschränkungen und Bestimmungen gelten speziell für die Auskunftspflicht nach Art. 21. Sind von der *Auskunftspflicht* jedoch «überwiegende Interessen Dritter» betroffen, sollten diese Angaben geschwärzt werden, damit keine Rückschlüsse auf die betroffenen Personen gemacht werden können. Um beispielsweise in Telekommunikationsmetadaten die Rechte der anderen an der Kommunikation beteiligten Personen zu schützen, sind diese zu anonymisieren. Die Auskunftspflicht ist dadurch aber nicht weiter einzuschränken (oder aufzuschieben oder darauf zu verzichten). Daher ist Abs. 3 wie folgt abzuändern:

Abs. 3: *«Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn ein Gesetz im formellen Sinn dies vorsieht. Er anonymisiert die Auskunft in Teilen, falls dies aufgrund überwiegender Interessen Dritter erforderlich ist.»*

Weitere Ausnahmen vom Auskunftsrecht für Bundesorgane sind formell in den betreffenden Gesetzen, wie beispielsweise dem Nachrichtendienstgesetz, zu regeln.

Abs. 4 lit. b: *«[…] wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls die Übermittlung der Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage stellt.»*

Die Abs. 3 und 4 wären unseres Erachtens in Art. 21 besser aufgehoben.

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

Es 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.

Alternativen: Es könnte auch der Beauftragte zur Prüfung herangezogen werden, ob es sich beim angewandten Entscheidungsprozess um eine automatisierte Einzelentscheidung im Sinne von Art. 15 handelt. Und/oder das angewandte Verfahren müsste im Rahmen einer Datenschutz-Folgenabschätzung nach Art. 16 regelmässig auf seine Wirksamkeit geprüft werden.

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.

Zudem müssen Datenschutz-Folgenabschätzungen auch rückwirkend, wie in Art. 59 lit. a vorgesehen, für bereits bestehende Datenbearbeitungen durchgeführt werden.

«Die Datenschutz-Folgeabschätzung muss vom Verantwortlichen oder vom Auftragsbearbeiter bei einer Änderung des Risikos oder spätestens alle fünf Jahre wiederholt werden. Eine Benachrichtigung des Beauftragten durch den Verantwortlichen und eine Beurteilung durch den Beauftragten erfolgt bei einem abweichenden Ergebnis der Datenschutz-Folgenabschätzung oder einer Anpassung der Massnahmen.»

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

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».*

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.

«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. 17 Abs. 4 – Meldung von Verletzungen des Datenschutzes

Der Auftragsbearbeiter muss den Verantwortlichen nicht nur über eine unbefugte Datenbearbeitung, sondern auch – wie in Abs. 1 für den Verantwortlichen festgehalten – über einen Verlust von Daten informieren. Der Absatz muss daher lauten:

«Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung oder den Verlust von Daten.»

Art. 17 Abs. 5 (neu) – Meldung von Verletzungen des Datenschutzes durch Internetkriminalität

Beim Verlust von Daten durch Internetkriminalität sollte neben dem Beauftragten und den betroffenen Personen auch die Melde- und Analysestelle Informationssicherung MELANI informiert werden. Durch das Wissen aus konkreten Fällen ist es ihr möglich, Gefahren für Schweizer Unternehmen zu erkennen, ein Gefahrenbild zu erstellen und Massnahmen zu empfehlen. Entsprechend ist der Beauftragte zu ermächtigen, MELANI zu informieren.

«Bei Verlust von Daten informiert der Beauftragte die für die Sicherheit von Computersystemen und des Internets zuständige Melde- und Analysestelle Informationssicherung MELANI.»

Art. 18 – Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sind wichtige Prinzipien und sorgen erst dafür, dass die Einwilligung der betroffenen Person nach Art. 4 Abs. 6 auch tatsächlich eingeholt wird. Ein Verstoss muss sanktioniert sein/bleiben.

Zudem müssen Massnahmen für Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen auch rückwirkend, wie in Art. 59 lit. b vorgesehen, für bereits bestehende Datenbearbeitungen umgesetzt 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 entspricht nicht den Anforderungen aus dem Übereinkommen SEV 108 und der EU-DSGVO. Vielmehr muss auch nachgewiesen werden können, dass die Datenschutzbestimmungen eingehalten werden. Dies geht über ein Register der Datenbearbeitungen hinaus.

Dies ist zu verdeutlichen.

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

Die Auskunft ist - wie im Vorentwurf vorgesehen - kostenlos vom Verantwortlichen zu leisten.

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

Gegenüber der Bestimmung im geltenden DSG wurde hinsichtlich dem Auskunftsrecht 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.

lit. c.: «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 aber 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 statt. Beispiele sind Social Media-Plattformen, personalisierte Werbung und Beeinflussung durch Microtargeting.

In Zukunft werde noch viel mehr persönliche Daten aus dem «Internet of Things», vom Strom-Smart-Meter über Mobilitäts- und Gesundheitsdaten bis zu Sensordaten aus «intelligenten» Fernsehern 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 automatisierte Einzelentscheidung zusätzlich die Auswirkungen der Entscheidung, mitgeteilt.»

Neue Formulierung für Art. 20 Abs. 2 lit. e:

«[…] das Vorliegen einer automatisierten Bearbeitung;»

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

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, da Schweizer Firmen, falls sie sich an Personen in der EU richten, dies nach EU-Recht einführen müssen. Ein Verzicht nützt den Unternehmen nichts, schwächt aber die Konsumentenrechte in der Schweiz.

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. 21 – Einschränkung des Auskunftsrechts

Die Ausnahmen zur *Informationspflicht* und Einschränkungen aus Art. 14 sollten von der Auskunftspflicht getrennt werden. Sind von der *Auskunftspflicht* «überwiegende Interessen Dritter» betroffen (bei denen die betroffene Person durch die Information über die Datenbearbeitung auch Informationen über Drittpersonen erhält und dadurch die Interessen dieser Drittpersonen beeinträchtigt werden können), müssen diese Angaben so «geschwärzt» werden, dass keine Rückschlüsse auf die betroffenen Personen gemacht werden können. Um beispielsweise in Telekommunikationsmetadaten die Rechte der anderen an der Kommunikation beteiligten Personen zu schützen, sind diese zu anonymisieren. Die Auskunftspflicht ist dadurch aber nicht weiter einzuschränken (oder aufzuschieben oder darauf zu verzichten).

Übernahme von Art. 14 Abs. 3:

Abs. 1: *«Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn ein Gesetz im formellen Sinn dies vorsieht. Er anonymisieren die Auskunft in Teilen, falls dies aufgrund überwiegender Interessen Dritter erforderlich ist.»*

Weitere Ausnahmen vom Auskunftsrecht für Bundesorgane sind formell in den betreffenden Gesetzen, wie zum Beispiel dem Nachrichtendienstgesetz, zu regeln.

Übernahme von Art. 14 Abs. 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 die Übermittlung der Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage stellt.»

Der zweite Satz in Art. 21 Abs. 2 ist damit überflüssig. Der Absatz lautet neu verkürzt:

«Der Verantwortliche muss begründen, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt.»

Art. 22 und Art. 24 Abs. 2 lit. d – Medien

Die Medienlandschaft hat sich in den letzten Jahren dramatisch gewandelt. Traditionelle Zeitungen verschwinden, Online-Angebote nehmen deren Platz ein und Betreiber von Blogs tragen immer mehr zur journalistischen Arbeit bei. Die Einschränkung des Auskunftsrechts für Medienschaffende sollte sich daher stärker am Zweck der Datenbearbeitung als an einem «periodischen Medium» oder dem Beruf des «Medienschaffenden» orientieren.

Auf die Anforderungen bezüglich «beruflich» und «periodisch» ist deshalb zu verzichten.

Art. 24 Abs. 2 lit. e – Anonymisierung usw.

Gemäss den Erläuterungen zum Vorentwurf, wie auch nach dem aktuellen Recht, reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei *bestimmbar*. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren.

Der Begriff wird hiermit zu eng gefasst, da unnötig in Kauf genommen wird, dass besonders schützenswerte Personendaten sich (zukünftig) deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann.

Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten (siehe Art. 3 lit. a).

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 ist weniger relevant. Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen (s.a. Ausführungen zu Art. 50 ff.).

Art. 25 Abs. 1 lit. c – Recht auf Vergessenwerden

Im Entscheid zum «Recht auf Vergessenwerden», wie ihn der Europäische Gerichtshof gegenüber Google gefällt hat, geht es nicht primär um das Löschen oder Vernichten von Daten. Vielmehr musste der Suchalgorithmus von Google dahingehend angepasst werden, dass Suchergebnisse zu einem bestimmten Ereignis bei der Suche nach einer Person nicht mehr angezeigt werden. Der Begriff des «Löschens» sollte entsprechend mit diesem Bezug erläutert werden.

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 einzelner Kunde oder 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).

Gemäss dem erläuternden Bericht sollen die Instrumente der kollektiven Rechtsdurchsetzung im Rahmen der Umsetzung der Motion 13.3931 Birrer-Heimo in einem grösseren, möglichst sektorübergreifenden Kontext geprüft werden. In der Stellungnahme des Bundesrates zur Motion ist zu entnehmen:

«Neben der Verbesserung im Rahmen der bereits bestehenden Instrumente erachtete er dabei die Einführung neuer, eigenständiger Instrumente der kollektiven Rechtsdurchsetzung für denkbar, namentlich die Schaffung eines Muster- oder Testverfahrens sowie eines Gruppenklage- oder Gruppenvergleichsverfahrens. Vor diesem Hintergrund ist der Bundesrat bereit, entsprechende punktuelle Gesetzesänderungen vorzuschlagen oder im Rahmen laufender Gesetzgebungsarbeiten zu berücksichtigen. In diesem Zusammenhang sei beispielsweise auf die laufende Aktienrechtsrevision sowie die Arbeiten an einem Finanzdienstleistungsgesetz (Fidleg) hingewiesen. Dagegen erachtet es der Bundesrat nicht als opportun, einen eigenständigen Erlass zum kollektiven Rechtsschutz (‹Sammelklagengesetz›) zu erarbeiten.»

Folgerichtig muss im neuen DSG eine Regelung zur kollektiven Rechtsdurchsetzung (Verbandsklagerecht und Sammelklage), analog beispielsweise zum UWG, vorgesehen sein.

Art. 25 Abs. 4 (neu): *«Klageberechtigt sind auch Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die sich statutengemäss unter anderem dem Datenschutz widmen.»*

Art. 25 Abs. 5 (neu) – Beweislastumkehr

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

Beispiel: Ein Online-Dienstleister bearbeitet Daten «im Auftrag» der Personen, die den Dienst nutzen. Dies können zum Beispiel deren Fotos, das Adressbuch und die Kontakte innerhalb der Plattform sein. Als Dienstanbieter verwendet er diese Daten aber ebenfalls für sich selbst oder für Dritte, zum Beispiel für Werbung. Und wiederum verwendet er diese Daten «im Auftrag» für andere Personen, die den Dienst nutzen, um Kontakte zu verknüpfen oder Personen in deren Fotos zu erkennen. Betroffen von dieser vielfältigen Datenbearbeitung sind aber nicht nur die beauftragenden Personen, sondern auch unbeteiligte Dritte, zum Beispiel auf den Fotos oder in den Adressbüchern.

Der Anbieter ist zu einer angemessenen Mithilfe zu verpflichten. Den Beweis einer rechtmässige 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.

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

Art. 27 Art. 2 – Rechtsgrundlagen

Das Profiling birgt immer besondere Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen. Daher muss für ein Profiling immer eine Grundlage in einem formellen Gesetz gegeben sein; eine Regelung in einem Gesetz im materiellen Sinn ist nicht ausreichend.

Art. 29 Abs. 4 – Bekanntgabe von Personendaten

Wir lehnen die Ausnahme gemäss Art. 29 Abs. 4 ab. Die Annahme, solche Grundangaben zur Identifizierung einer Person könnten ohnehin auf einfachem Weg in Erfahrung gebracht werden, ist nicht zulässig. Gerade in einem digitalen Kontext stellt beispielsweise das Geburtsdatum ein wichtiges Identitäts- und Sicherheitsmerkmal dar.

Art. 29 Abs. 5 – Bekanntgabe von Personendaten

Die Adressangaben beispielsweise aus der Switch-WHOIS-Datenbank werden regelmässig automatisiert ausgelesen und unrechtmässig weiterbearbeitet. Bei der Zugänglichmachung von Personendaten mittels automatisierter Informations- und Kommunikationsdienste muss entsprechender Missbrauch wirkungsvoll verhindert werden.

Anhängen an Abs. 5: *«Ein missbräuchliches, insbesondere automatisiertes Beschaffen der Daten durch Dritte ist wirkungsvoll zu verhindern.»*

Art. 30 Abs. 2 – Widerspruch gegen die Bekanntgabe von Personendaten

Die historische Rechtsabwägung nach lit. b ist nicht mehr nötig und zu streichen.

Abs. 2: *«Das Bundesorgan weist das Begehren ab, wenn eine Rechtspflicht zur Bekanntgabe besteht.»*

Art. 32 Abs. 1 – Datenbearbeitung für Forschung, Planung und Statistik

Gemäss den Erläuterungen zum Vorentwurf, wie auch nach dem aktuellen Recht, reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei *bestimmbar*. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren.

Der Begriff wird hiermit zu eng gefasst, da unnötig in Kauf genommen wird, dass besonders schützenswerte Personendaten sich (zukünftig) deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann.

Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten (siehe Art. 3 lit. a).

Art. 34 Abs. 3bis (neu) – Verbands- und Sammelverfahren

Analog zu Art. 25 Abs. 4 (neu) sind auch die Voraussetzungen für Verbands- und Sammelverfahren zu schaffen.

«Ansprüche und Verfahren stehen ebenso Organisationen von gesamtschweizerischer oder regionaler Bedeutung zu, die sich statutengemäss unter anderem dem Datenschutz widmen.»

Art. 37 Abs. 1 – Ernennung und Stellung

Der Beauftragte kontrolliert unter anderem auch die Verwaltung. Er sollte daher unabhängig vom Bundesrat und der übrigen Exekutive beziehungsweise Verwaltung gewählt werden.

«Die oder der Beauftragte wird von der Bundesversammlung für eine Amtsdauer von vier Jahren gewählt.»

Art. 41 – Untersuchung

Die erweiterten Untersuchungsbefugnisse werden begrüsst. Diese entsprechen auch den Vorgaben von Europarat und EU. Allerdings geben diese eine Behandlungspflicht

(und nicht nur eine Möglichkeit) durch den Beauftragten vor. 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 eröffnen, 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 in der Regel ein Organisationsverschulden anzunehmen. Die Feststellung des schuldhaften Verhaltens einzelner Personen ist weniger relevant. Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen (s.a. Ausführungen zu Art. 50 ff.).

Art. 50 und 51 – Verwaltungssanktionen

Die aktuell bereits bestehenden Strafbestimmungen im DSG haben sich nicht bewährt: Entsprechende Urteile sind fast gänzlich unbekannt.

Der Entwurf sieht vor, auf die in der EU-DSGVO verankerten Verwaltungssanktionen zu verzichten. Stattdessen sollen die Strafbarkeitsbestimmungen ausgebaut und insbesondere der Strafrahmen stark ausgedehnt werden. Die Wirksamkeit strafrechtlicher Sanktionen vermag jedoch offenkundig nicht an jene von Verwaltungssanktionen heranzureichen.

Strafrechtliche Sanktionen können nur greifen, soweit der Rechtsverstoss einer Person individuell zugeordnet werden kann. Die Höhe der Busse orientiert sich wesentlich am individuellen Verschulden dieser Person und ist auch durch ihre persönlichen finanziellen Verhältnisse limitiert.

Im Rahmen von Verwaltungssanktionen kann ein Verstoss viel umfassender gewürdigt und sanktioniert werden. Anders als bei einer strafrechtlichen Verfolgung fällt dabei jede in einer Organisation feststellbare Pflichtverletzung ins Gewicht. Ihre Auswirkungen können umfassend berücksichtigt werden, ebenso die wirtschaftliche Potenz der betroffenen Organisation und die von ihr - allenfalls unter Inkaufnahme von datenschutzrechtlichen Pflichten - erzielten Gewinne.

Nach Art. 30 Abs. 1 StGB kann auch nur die Person, die durch eine Tat verletzt worden ist, die Bestrafung des Täters beantragen. Bei der Pflicht zur Dokumentation von Datenbearbeitungen oder der Durchführung einer Datenschutz-Folgenabschätzung dürfte jedoch oft unklar sein, wer durch eine Unterlassung konkret betroffen ist.

Insbesondere bei gravierenden Verstössen gegen das Datenschutzrecht ist zudem in der Regel von einem Organisationsverschulden auszugehen, bei dem unterschiedliche Akteure in vielfältigen Funktionen und verteilt über verschiedene Gremien und Hierarchien beteiligt sind. Untersuchungen, die darauf ausgerichtet sind, den Grad des schuldhaften Verhaltens von einzelnen Akteuren festzustellen, scheinen wenig sinnvoll. Dabei droht die Sicht auf das Ganze verloren zu gehen.

Insbesondere bei Verstössen von grosser Tragweite wird der Beauftrage mit grosser Wahrscheinlichkeit zugezogen. Das Argument des Bundesrats ist daher falsch, dass die Organisation des Beauftragten verändert werden müsste, um Verwaltungssanktionen durch den Beauftragten aussprechen zu können, worauf insbesondere mit Blick auf die Kosten verzichtet wurde. Es ist auch ökonomisch sinnvoll, die Kompetenz für solche komplexen Untersuchungen zentral zu halten. Im Strafrecht droht zudem die Gefahr von Bauernopfern.

Die EU sowie der Europarat verlangen ausdrücklich auch Verwaltungssanktionen, die der Beauftragte verhängen kann. Die Sanktionen müssen wirksam, verhältnismässig und abschreckend sein. Strafrechtliche Massnahmen vermögen a priori nicht die Wirksamkeit und Abschreckung zu gewährleisten, welche denjenigen von Verwaltungsmassnahmen entsprechen.

Um nicht zuletzt die Angemessenheit hinsichtlich der EU-DSGVO zu gewährleisten, erscheint es daher (allenfalls zusätzlich zu den vorgeschlagenen Strafbestimmungen) als erforderlich, Verwaltungssanktionen durch den Beauftragten vorzusehen. Die Konzepte sind nicht neu. Die Schweiz kennt sie zum Beispiel aus der Wettbewerbskommission und der ComCom.

Art. 50 und 51 – Strafmass

Auch gegenüber grossen Unternehmen, die unter Umständen mehrere Milliarden Dollar Gewinn pro Quartal erzielen, müssen Sanktionen genügend abschreckend sein. Die in der EU drohenden Strafen von 20 Mio. Euro oder 4 % des Umsatzes (was entsprechend höher ist) scheinen angemessen. Mit den im Entwurf vorgesehenen Bussen ist eine vergleichbare Wirksamkeit und Abschreckung gegenüber grossen Unternehmen nicht zu erzielen.

Art. 52 – Verletzung der beruflichen Schweigepflicht

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

Art. 57 Abs. 1 – Vollzug durch die Kantone

Die Unterstellung der Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unter das Bundesgesetz über den Datenschutz wird begrüsst.

Zivilprozessordnung (ZPO)

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

Ermächtigungen zur Datenbearbeitung in anderen Gesetzen

Das totalrevidierte Datenschutzgesetz beruht über weite Strecken auf denselben Grundprinzipien wie das bisherige Recht. Die Tragweite neu geschaffener Vorschriften ist grösstenteils aus sich selbst genügend klar. Unmittelbarer Änderungsbedarf in Einzelgesetzen besteht somit nur beschränkt. Jedenfalls ist die Totalrevision des Datenschutzgesetzes nicht der richtige Ort, um spezifische Bestimmungen zur Bearbeitung von Personendaten in einzelnen Bundesgesetzen zu schaffen oder abzuändern. Sofern der Bundesrat hier Änderungen anstrebt, sind diese im Rahmen einer Revision des jeweiligen Bundesgesetzes zu diskutieren und allenfalls zu

beschliessen. Nur so erscheint als gewährleistet, dass die im Rahmen der konkreten Materie vorzunehmenden Abwägungen im Gesetzgebungsprozess mit der erforderlichen Sorgfalt getroffen werden.

Abgesehen von redaktionellen Änderungen, welche sich aus der neuen Terminologie ergeben, ist daher im Rahmen dieser Revision von der Änderung spezifischer datenschutzrechtlicher Bestimmungen in Einzelgesetzen abzusehen. Namentlich sind sämtliche Bestimmungen, mit denen Ermächtigungen zur Datenbearbeitung in anderen Gesetzen geschaffen oder ausgedehnt werden, zu streichen. Dies betrifft insbesondere die Ermächtigungen zum Profiling. In den Bundesgesetzen müssen individuelle, klare und strenge Rahmenbedingungen für das Profiling vorgesehen 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

Stellungnahme von

Name / Firma / Organisation : Digitale Gesellschaft

Abkürzung der Firma / Organisation : DigiGes

Adresse : 4000 Basel

Kontaktperson : Erik Schönenberger

Telefon : 061 551 03 45

E-Mail : kire@digitale-gesellschaft.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

Allgemeine Bemerkungen ____ 4

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ 6

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 ____ 14

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ____ 16

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") ____ 18

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" ____ 21

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.	
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	2			**Räumlicher Geltungsbereich** Im Gegensatz zur neuen Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) enthält der vorliegende Entwurf zum revidierten Datenschutzgesetz (DSG) keine besondere Bestimmung zum räumlichen Geltungsbereich. 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 Inhaber von Datensammlungen – nach heutiger Terminologie – vergleichbar, die komplett aus dem Ausland operieren, sich aber an Personen in der Schweiz richten. Zu erwähnen sind etwa Amazon (unter anderen mit Amazon Web Services), Facebook (auch mit Instagram und WhatsApp), Google (unter anderem mit Gmail, Google Analytics und YouTube), LinkedIn, Microsoft (unter anderem mit Office 365), Twitter, Salesforce und XING. In all diesen Fällen kann – im Unterschied zur neuen EU-DSGVO – 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 der neuen EU-DSGVO entsprechendes *Marktortprinzip* muss daher vorgesehen werden. Damit würde dann auch ein in der Schweiz nötiges, vergleichbares Datenschutzrecht gelten.
Fehler! Verweisquel					

le konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	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.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	3		a	**Personendaten** Der erläuternde Bericht hält in der Definition zum Begriff «bestimmbare Person» folgendes fest: *«Wie auch nach dem aktuellen Recht reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei bestimmbar. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Die zur Verfügung stehenden technischen Möglichkeiten werden in Bezug darauf geprüft, wie hoch der zeitliche und finanzielle Aufwand für ihre Anwendung ist. Mit Blick auf die immer gezielteren Technologien zur Datenauswertung und deren konstante Weiterentwicklung verschwimmt die Grenze zwischen Personendaten und anderen Daten indes zusehends. Daten, bei denen heute noch eine rein theoretische Möglichkeit der Identifizierung anzunehmen ist, können morgen vielleicht bereits einer bestimmbaren Person zugeordnet werden.»*

					Es genügt nicht, wenn besonders schützenswerte Personendaten bearbeitet, Dritten bekannt gegeben und veröffentlicht werden dürfen, sofern die Möglichkeit besteht, dass sich diese Personendaten allenfalls zukünftig deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann. Insbesondere in der Forschung, Planung und Statistik sind Konzepte, wie Differential Privacy seit langem bekannt. Mithilfe von Noise Injection lassen sich beispielsweise Daten so verfremden, dass sie zwar statistisch weiterhin auswertbar sind, sie aber keine verlässlichen Rückschlüsse auf Personen mehr zulassen. Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	3		c	**Ziff. 4 – Biometrische Daten** Biometrische Merkmale lassen 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. Wenn folglich biometrische Merkmale zur Identifizierung geeignet sind oder zur Identifikation bearbeitet werden, müssen sie als besonders schützenswerte Personendaten gelten. Das Wort «eindeutig» ist daher zu streichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	4	2		**Verhältnismässigkeit** «Datenvermeidung» und «Datensparsamkeit» fehlen als explizite Grundkonzepte und als Teil der notwendigen Verhältnismässigkeit (s. Art. 4 Abs. 6). Der Absatz ist zu ergänzen mit: *«Die Bearbeitung personenbezogener Daten sowie die Auswahl und Gestaltung der Datenbearbeitungssysteme sind dahin gehend auszurichten, dass so wenig personenbezogene Daten wie möglich von der Bearbeitung betroffen sind.»*

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	4	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. Übermittelt die betroffene Person (wie beispielhaft im erläuternden Bericht festgehalten) ihre Adresse im Hinblick auf den Erhalt einer Kundenkarte, so mag die Weiterbenutzung dieser Adresse durch das betreffende Unternehmen zu Werbezwecken im Rahmen einer anfänglich erkennbaren Zweckbestimmung liegen. Findet die Übermittlung im Rahmen einer Bestellung (online oder nicht) statt, sollte jedoch nicht davon ausgegangen werden können. An der Bestimmung soll – wie im Vorentwurf vorgesehen – festgehalten werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	4	6		**Einwilligung** Die Bestimmung ist nur zusammen mit den Grundsätzen der Datenvermeidung und der Datensparsamkeit wirksam. Dies zeigen aktuelle Beispiele: Ein «Cookies-Balken», der nicht abgelehnt werden kann, ist für die betroffene Person wenig hilfreich. Es muss auch jederzeit die Möglichkeit des Widerrufs einer Einwilligung gegeben sein. Zudem müssen Personen in einem Abhängigkeitsverhältnis vor unwillentlich abgegebenen und unverhältnismässigen Zustimmungen geschützt werden (zum Beispiel Arbeitnehmer vor Pauschalvollmachten 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 ein entsprechendes 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.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	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.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	11			**Sicherheit von Personendaten** Der Artikel im Vorentwurf ist wie der bestehende Art. 7 DSG vage. Er hält insbesondere keine Schutzziele fest. Wir erwarten vom Bundesrat, dass die erwähnten technischen und organisatorischen Schutzmassnahmen mindestens auf Verordnungsstufe konkretisiert werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	12			**Daten einer verstorbenen Person** Die neue Bestimmung über «Daten einer verstorbenen Person» wird begrüsst.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	14	3 und 4		**Ausnahmen von der Informationspflicht und Einschränkungen** Die Einschränkungen und Bestimmungen gelten speziell für die Auskunftspflicht nach Art. 21. Sind von der *Auskunftspflich*t jedoch «überwiegende Interessen Dritter» betroffen, sollten diese Angaben geschwärzt werden, damit keine Rückschlüsse auf die betroffenen Personen gemacht werden können. Um beispielsweise in Telekommunikationsmetadaten die Rechte der anderen an der Kommunikation beteiligten Personen zu schützen, sind diese zu anonymisieren. Die Auskunftspflicht ist dadurch aber nicht weiter einzuschränken (oder aufzuschieben oder darauf zu verzichten). Daher ist Abs. 3 wie folgt abzuändern: Abs. 3: «*Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn ein Gesetz im formellen Sinn dies vorsieht. Er anonymisiert die*

					Auskunft in Teilen, falls dies aufgrund überwiegender Interessen Dritter erforderlich ist.» Weitere Ausnahmen vom Auskunftsrecht für Bundesorgane sind formell in den betreffenden Gesetzen, wie beispielsweise dem Nachrichtendienstgesetz, zu regeln. Abs. 4 lit. b: *«[…] wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls die Übermittlung der Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage stellt.*» Die Abs. 3 und 4 wären unseres Erachtens in Art. 21 besser aufgehoben.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	15	1		**Informationspflicht bei einer automatisierten Einzelentscheidung** Es 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. **Alternativen**: Es könnte auch der Beauftragte zur Prüfung herangezogen werden, ob es sich beim angewandten Entscheidungsprozess um eine automatisierte Einzelentscheidung im Sinne von Art. 15 handelt. Und/oder das angewandte Verfahren müsste im Rahmen einer Datenschutz-Folgenabschätzung nach Art. 16 regelmässig auf seine Wirksamkeit geprüft werden.
Fehler! Verweisquelle konnte	DSG	15	2		**Anhörungspflicht bei einer automatisierten Einzelentscheidung** Die betroffene Person muss sich nicht nur zur automatisierten Einzelentscheidung und den bearbeiteten

nicht gefunden werden.					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.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	16			**Datenschutz-Folgenabschätzun**g Die Regelung der Datenschutz-Folgeabschätzung wird begrüsst. Dies entspricht dem gewählten, ausdrücklich risikobasierten Ansatz im revidierten DSG.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	16	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. Zudem müssen Datenschutz-Folgenabschätzungen auch rückwirkend, wie in Art. 59 lit. a vorgesehen, für bereits bestehende Datenbearbeitungen durchgeführt werden. *«Die Datenschutz-Folgeabschätzung muss vom Verantwortlichen oder vom Auftragsbearbeiter bei einer Änderung des Risikos oder spätestens alle fünf Jahre wiederholt werden. Eine Benachrichtigung des Beauftragten durch den Verantwortlichen und eine Beurteilung durch den Beauftragten erfolgt bei einem abweichenden Ergebnis der Datenschutz-Folgenabschätzung oder einer Anpassung der Massnahmen.»*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	16	1, 3, 4, sowie 5 (neu)		**Datenschutz-Folgeabschätzung für Gesetzeserlasse** 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»*.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	59		a	**Übergangsbestimmung** 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».*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	16	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. *«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.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	17	4		**Meldung von Verletzungen des Datenschutzes** Der Auftragsbearbeiter muss den Verantwortlichen nicht nur über eine unbefugte Datenbearbeitung, sondern auch – wie in Abs. 1 für den Verantwortlichen festgehalten – über einen Verlust von Daten informieren. Der Absatz muss daher lauten: *«Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung oder den Verlust von Daten.»*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	17	5 (neu)		**Meldung von Verletzungen des Datenschutzes durch Internetkriminalität** Beim Verlust von Daten durch Internetkriminalität sollte neben dem Beauftragten und den betroffenen Personen auch die Melde- und Analysestelle Informationssicherung MELANI informiert werden. Durch das Wissen aus konkreten Fällen ist es ihr möglich, Gefahren für Schweizer Unternehmen zu erkennen, ein Gefahrenbild zu erstellen und Massnahmen zu empfehlen. Entsprechend ist der Beauftragte zu ermächtigen, MELANI zu informieren. *«Bei Verlust von Daten informiert der Beauftragte die für die Sicherheit von Computersystemen und des Internets zuständige Melde- und Analysestelle Informationssicherung MELANI.»*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	18			**Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen** Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sind wichtige Prinzipien und sorgen erst dafür, dass die Einwilligung der betroffenen Person nach Art. 4 Abs. 6 auch tatsächlich eingeholt wird. Ein Verstoss muss sanktioniert sein/bleiben. Zudem müssen Massnahmen für Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen auch rückwirkend, wie in Art. 59 lit. b vorgesehen, für bereits bestehende Datenbearbeitungen umgesetzt werden.

Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	19		a	**Weitere Pflichten** Gemäss dem erläuternden Bericht wird dadurch für Private die bisherige Verpflichtung ersetzt, Datensammlungen beim Beauftragten zu registrieren. Dies entspricht nicht den Anforderungen aus dem Übereinkommen SEV 108 und der EU-DSGVO. Vielmehr muss auch nachgewiesen werden können, dass die Datenschutzbestimmungen eingehalten werden. Dies geht über ein Register der Datenbearbeitungen hinaus. Dies ist zu verdeutlichen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	20			**Auskunftsrecht** Das Auskunftsrecht ist ein zentrales Element des Datenschutzes und schafft die Grundlage für die Durchsetzung weiterer Rechtsansprüche der betroffenen Personen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	20	1	c	**Auskunftsrecht zur Rechtsgrundlage** Gegenüber der Bestimmung im geltenden DSG wurde hinsichtlich dem Auskunftsrecht 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. lit. c.: «der Zweck der Bearbeitung und die Rechtsgrundlage;»
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	20	2	g	**Auskunftsrecht und Informationspflicht** Zur Erfüllung der *Informationspflich*t 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 *Auskunftspflich*t hingegen muss aber 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.»*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	20	3		**Auskunftsrecht und Entscheidunge**n Bereits heute finden massenhaft automatisierte Einzelentscheidungen – die ausschliesslich auf Algorithmen beruhen und ohne menschliches Eingreifen getroffen werden – auf Grund von Personendaten statt. Beispiele sind Social Media-Plattformen, personalisierte Werbung und Beeinflussung durch Microtargeting. In Zukunft werde noch viel mehr persönliche Daten aus dem «Internet of Things», vom Strom-Smart-Meter über Mobilitäts- und Gesundheitsdaten bis zu Sensordaten aus «intelligenten» Fernsehern 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 automatisierte Einzelentscheidung zusätzlich die Auswirkungen der Entscheidung, mitgeteilt.*» Neue Formulierung für Art. 20 Abs. 2 lit. e: *«[…] das Vorliegen einer automatisierten Bearbeitung;»*
Fehler!	DSG	20	7, 8, 9		**Datenauskunft und Datenportabilität**

Verweisquelle konnte nicht gefunden werden.			und 10 (neu)		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, da Schweizer Firmen, falls sie sich an Personen in der EU richten, dies nach EU-Recht einführen müssen. Ein Verzicht nützt den Unternehmen nichts, schwächt aber die Konsumentenrechte in der Schweiz. 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.*»
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	21			**Einschränkung des Auskunftsrechts** Die Ausnahmen zur *Informationspflich*t und Einschränkungen aus Art. 14 sollten von der Auskunftspflicht getrennt werden. Sind von der *Auskunftspflich*t «überwiegende Interessen Dritter» betroffen (bei denen die betroffene Person durch die Information über die Datenbearbeitung auch Informationen über Drittpersonen erhält und dadurch die Interessen dieser Drittpersonen beeinträchtigt werden können), müssen diese Angaben so «geschwärzt» werden, dass keine Rückschlüsse auf die betroffenen Personen gemacht werden

					können. Um beispielsweise in Telekommunikationsmetadaten die Rechte der anderen an der Kommunikation beteiligten Personen zu schützen, sind diese zu anonymisieren. Die Auskunftspflicht ist dadurch aber nicht weiter einzuschränken (oder aufzuschieben oder darauf zu verzichten). Übernahme von Art. 14 Abs. 3: Abs. 1: «*Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn ein Gesetz im formellen Sinn dies vorsieht. Er anonymisieren die Auskunft in Teilen, falls dies aufgrund überwiegender Interessen Dritter erforderlich ist.*» Weitere Ausnahmen vom Auskunftsrecht für Bundesorgane sind formell in den betreffenden Gesetzen, wie zum Beispiel dem Nachrichtendienstgesetz, zu regeln. Übernahme von Art. 14 Abs. 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 die Übermittlung der Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage stellt.*» Der zweite Satz in Art. 21 Abs. 2 ist damit überflüssig. Der Absatz lautet neu verkürzt: *«Der Verantwortliche muss begründen, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt.»*
Fehler! Verweisquelle konnte nicht	DSG	22			**Medien** Die Medienlandschaft hat sich in den letzten Jahren dramatisch gewandelt. Traditionelle Zeitungen verschwinden, Online-Angebote nehmen deren Platz ein und Betreiber von Blogs tragen immer mehr zur

gefunden werden.					journalistischen Arbeit bei. Die Einschränkung des Auskunftsrechts für Medienschaffende sollte sich daher stärker am Zweck der Datenbearbeitung als an einem «periodischen Medium» oder dem Beruf des «Medienschaffenden» orientieren. Auf die Anforderungen bezüglich «beruflich» und «periodisch» ist deshalb zu verzichten.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	24	2	d	**Medien** Die Medienlandschaft hat sich in den letzten Jahren dramatisch gewandelt. Traditionelle Zeitungen verschwinden, Online-Angebote nehmen deren Platz ein und Betreiber von Blogs tragen immer mehr zur journalistischen Arbeit bei. Die Einschränkung des Auskunftsrechts für Medienschaffende sollte sich daher stärker am Zweck der Datenbearbeitung als an einem «periodischen Medium» oder dem Beruf des «Medienschaffenden» orientieren. Auf die Anforderungen bezüglich «beruflich» und «periodisch» ist deshalb zu verzichten.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	24	2	e	**Anonymisierung usw.** Gemäss den Erläuterungen zum Vorentwurf, wie auch nach dem aktuellen Recht, reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei *bestimmba*r. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Der Begriff wird hiermit zu eng gefasst, da unnötig in Kauf genommen wird, dass besonders schützenswerte Personendaten sich (zukünftig) deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann. Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten (siehe Art. 3 lit. a).
Fehler! Verweisquel	DSG	25			**Rechtsansprüche**

le konnte nicht gefunden werden.					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 ist weniger relevant. Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen (s.a. Ausführungen zu Art. 50 ff.).
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	25	1	c	**Recht auf Vergessenwerde**n Im Entscheid zum «Recht auf Vergessenwerden», wie ihn der Europäische Gerichtshof gegenüber Google gefällt hat, geht es nicht primär um das Löschen oder Vernichten von Daten. Vielmehr musste der Suchalgorithmus von Google dahingehend angepasst werden, dass Suchergebnisse zu einem bestimmten Ereignis bei der Suche nach einer Person nicht mehr angezeigt werden. Der Begriff des «Löschens» sollte entsprechend mit diesem Bezug erläutert werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	25	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 einzelner Kunde oder 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). Gemäss dem erläuternden Bericht sollen die Instrumente der kollektiven Rechtsdurchsetzung im Rahmen der Umsetzung der Motion 13.3931 Birrer-Heimo in einem grösseren, möglichst sektorübergreifenden Kontext geprüft werden. In der Stellungnahme des Bundesrates zur Motion ist zu entnehmen: *«Neben der Verbesserung im Rahmen der bereits bestehenden Instrumente erachtete er dabei die Einführung neuer, eigenständiger Instrumente der kollektiven Rechtsdurchsetzung für denkbar, namentlich die Schaffung eines Muster- oder Testverfahrens sowie eines Gruppenklage- oder Gruppenvergleichsverfahrens. Vor diesem Hintergrund ist der Bundesrat bereit, entsprechende punktuelle Gesetzesänderungen vorzuschlagen oder im Rahmen laufender Gesetzgebungsarbeiten zu berücksichtigen. In diesem Zusammenhang sei beispielsweise auf die laufende Aktienrechtsrevision sowie die Arbeiten an einem Finanzdienstleistungsgesetz (Fidleg) hingewiesen. Dagegen erachtet es der Bundesrat nicht als opportun, einen eigenständigen Erlass zum kollektiven Rechtsschutz (‹Sammelklagengesetz›) zu erarbeiten.»* Folgerichtig muss im neuen DSG eine Regelung zur kollektiven Rechtsdurchsetzung (Verbandsklagerecht und Sammelklage), analog beispielsweise zum UWG, vorgesehen sein. Art. 25 Abs. 4 (neu): *«Klageberechtigt sind auch Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die sich statutengemäss unter anderem dem Datenschutz widmen.»*
Fehler! Verweisquelle konnte nicht gefunden	DSG	25	5 (neu)		**Beweislastumkehr** Eine unrechtmässige Bearbeitung von Daten ist nur schwierig und/oder in einem langwierigen Verfahren nachzuweisen, wenn die Klärung des Sachverhalts auf die Mitarbeit und Informationen der beschuldigten Partei angewiesen ist. In schwerwiegenden Fällen muss die Beweislast daher umgedreht werden.

werden.					Beispiel: Ein Online-Dienstleister bearbeitet Daten «im Auftrag» der Personen, die den Dienst nutzen. Dies können zum Beispiel deren Fotos, das Adressbuch und die Kontakte innerhalb der Plattform sein. Als Dienstanbieter verwendet er diese Daten aber ebenfalls für sich selbst oder für Dritte, zum Beispiel für Werbung. Und wiederum verwendet er diese Daten «im Auftrag» für andere Personen, die den Dienst nutzen, um Kontakte zu verknüpfen oder Personen in deren Fotos zu erkennen. Betroffen von dieser vielfältigen Datenbearbeitung sind aber nicht nur die beauftragenden Personen, sondern auch unbeteiligte Dritte, zum Beispiel auf den Fotos oder in den Adressbüchern. Der Anbieter ist zu einer angemessenen Mithilfe zu verpflichten. Den Beweis einer rechtmässige 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. *«Besteht der Verdacht auf eine schwerwiegende und systematische Verletzung der Persönlichkeit, ist der Verantwortliche verpflichtet, die rechtmässige Bearbeitung der Daten nachzuweisen.»*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	27	2		**Rechtsgrundlagen** Das Profiling birgt immer besondere Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen. Daher muss für ein Profiling immer eine Grundlage in einem formellen Gesetz gegeben sein; eine Regelung in einem Gesetz im materiellen Sinn ist nicht ausreichend.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	29	4		**Bekanntgabe von Personendaten** Wir lehnen die Ausnahme gemäss Art. 29 Abs. 4 ab. Die Annahme, solche Grundangaben zur Identifizierung einer Person könnten ohnehin auf einfachem Weg in Erfahrung gebracht werden, ist nicht zulässig. Gerade in einem digitalen Kontext stellt beispielsweise das Geburtsdatum ein wichtiges Identitäts- und Sicherheitsmerkmal dar.
Fehler!	DSG	29	5		**Bekanntgabe von Personendaten**

Verweisquelle konnte nicht gefunden werden.					Die Adressangaben beispielsweise aus der Switch-WHOIS-Datenbank werden regelmässig automatisiert ausgelesen und unrechtmässig weiterbearbeitet. Bei der Zugänglichmachung von Personendaten mittels automatisierter Informations- und Kommunikationsdienste muss entsprechender Missbrauch wirkungsvoll verhindert werden. Anhängen an Abs. 5: *«Ein missbräuchliches, insbesondere automatisiertes Beschaffen der Daten durch Dritte ist wirkungsvoll zu verhindern.»*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	30	2		**Widerspruch gegen die Bekanntgabe von Personendaten** Die historische Rechtsabwägung nach lit. b ist nicht mehr nötig und zu streichen. Abs. 2: *«Das Bundesorgan weist das Begehren ab, wenn eine Rechtspflicht zur Bekanntgabe besteht.»*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	32	1		**Datenbearbeitung für Forschung, Planung und Statistik** Gemäss den Erläuterungen zum Vorentwurf, wie auch nach dem aktuellen Recht, reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei *bestimmba*r. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Der Begriff wird hiermit zu eng gefasst, da unnötig in Kauf genommen wird, dass besonders schützenswerte Personendaten sich (zukünftig) deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann. Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten (siehe Art. 3 lit. a).
Fehler! Verweisquel	DSG	34	3bis (neu)		**Verbands- und Sammelverfahren**

le konnte nicht gefunden werden.					Analog zu Art. 25 Abs. 4 (neu) sind auch die Voraussetzungen für Verbands- und Sammelverfahren zu schaffen. *«Ansprüche und Verfahren stehen ebenso Organisationen von gesamtschweizerischer oder regionaler Bedeutung zu, die sich statutengemäss unter anderem dem Datenschutz widmen.»*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	37	1		**Ernennung und Stellung** Der Beauftragte kontrolliert unter anderem auch die Verwaltung. Er sollte daher unabhängig vom Bundesrat und der übrigen Exekutive beziehungsweise Verwaltung gewählt werden. *«Die oder der Beauftragte wird von der Bundesversammlung für eine Amtsdauer von vier Jahren gewählt.»*
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	41			**Untersuchung** Die erweiterten Untersuchungsbefugnisse werden begrüsst. Diese entsprechen auch den Vorgaben von Europarat und EU. Allerdings geben diese eine Behandlungspflicht (und nicht nur eine Möglichkeit) durch den Beauftragten vor. 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 eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.*» Abs. 5: Ist verbindlicher zu formulieren und eine Behandlungsfrist festzuhalten.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	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 in der Regel ein Organisationsverschulden anzunehmen. Die Feststellung des schuldhaften Verhaltens einzelner Personen ist weniger relevant. Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen (s.a. Ausführungen zu Art. 50 ff.).
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	50 und 51			**Verwaltungssanktionen** Die aktuell bereits bestehenden Strafbestimmungen im DSG haben sich nicht bewährt: Entsprechende Urteile sind fast gänzlich unbekannt. Der Entwurf sieht vor, auf die in der EU-DSGVO verankerten Verwaltungssanktionen zu verzichten. Stattdessen sollen die Strafbarkeitsbestimmungen ausgebaut und insbesondere der Strafrahmen stark ausgedehnt werden. Die Wirksamkeit strafrechtlicher Sanktionen vermag jedoch offenkundig nicht an jene von Verwaltungssanktionen heranzureichen. Strafrechtliche Sanktionen können nur greifen, soweit der Rechtsverstoss einer Person individuell zugeordnet werden kann. Die Höhe der Busse orientiert sich wesentlich am individuellen Verschulden dieser Person und ist auch durch ihre persönlichen finanziellen Verhältnisse limitiert. Im Rahmen von Verwaltungssanktionen kann ein Verstoss viel umfassender gewürdigt und sanktioniert werden. Anders als bei einer strafrechtlichen Verfolgung fällt dabei jede in einer Organisation feststellbare Pflichtverletzung ins Gewicht. Ihre Auswirkungen können umfassend berücksichtigt werden, ebenso die wirtschaftliche Potenz der betroffenen Organisation und die von ihr - allenfalls unter Inkaufnahme von datenschutzrechtlichen Pflichten - erzielten Gewinne. Nach Art. 30 Abs. 1 StGB kann auch nur die Person, die durch eine Tat verletzt worden ist, die Bestrafung des Täters beantragen. Bei der Pflicht zur Dokumentation von Datenbearbeitungen oder der Durchführung

					einer Datenschutz-Folgenabschätzung dürfte jedoch oft unklar sein, wer durch eine Unterlassung konkret betroffen ist. Insbesondere bei gravierenden Verstössen gegen das Datenschutzrecht ist zudem in der Regel von einem Organisationsverschulden auszugehen, bei dem unterschiedliche Akteure in vielfältigen Funktionen und verteilt über verschiedene Gremien und Hierarchien beteiligt sind. Untersuchungen, die darauf ausgerichtet sind, den Grad des schuldhaften Verhaltens von einzelnen Akteuren festzustellen, scheinen wenig sinnvoll. Dabei droht die Sicht auf das Ganze verloren zu gehen. Insbesondere bei Verstössen von grosser Tragweite wird der Beauftrage mit grosser Wahrscheinlichkeit zugezogen. Das Argument des Bundesrats ist daher falsch, dass die Organisation des Beauftragten verändert werden müsste, um Verwaltungssanktionen durch den Beauftragten aussprechen zu können, worauf insbesondere mit Blick auf die Kosten verzichtet wurde. Es ist auch ökonomisch sinnvoll, die Kompetenz für solche komplexen Untersuchungen zentral zu halten. Im Strafrecht droht zudem die Gefahr von Bauernopfern. Die EU sowie der Europarat verlangen ausdrücklich auch Verwaltungssanktionen, die der Beauftragte verhängen kann. Die Sanktionen müssen wirksam, verhältnismässig und abschreckend sein. Strafrechtliche Massnahmen vermögen a priori nicht die Wirksamkeit und Abschreckung zu gewährleisten, welche denjenigen von Verwaltungsmassnahmen entsprechen. Um nicht zuletzt die Angemessenheit hinsichtlich der EU-DSGVO zu gewährleisten, erscheint es daher (allenfalls zusätzlich zu den vorgeschlagenen Strafbestimmungen) als erforderlich, Verwaltungssanktionen durch den Beauftragten vorzusehen. Die Konzepte sind nicht neu. Die Schweiz kennt sie zum Beispiel aus der Wettbewerbskommission und der ComCom.
Fehler! Verweisquelle konnte nicht gefunden	DSG	50 und 51			**Strafmass** Auch gegenüber grossen Unternehmen, die unter Umständen mehrere Milliarden Dollar Gewinn pro Quartal erzielen, müssen Sanktionen genügend abschreckend sein. Die in der EU drohenden Strafen von 20 Mio. Euro oder 4 % des Umsatzes (was entsprechend höher ist) scheinen angemessen. Mit den im Entwurf

werden.					vorgesehenen Bussen ist eine vergleichbare Wirksamkeit und Abschreckung gegenüber grossen Unternehmen nicht zu erzielen.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	52			**Verletzung der beruflichen Schweigepflicht** Mit der Bestimmung würde (im Bereich der Personendaten) ein Tatbestand für Mitarbeiter von Privatfirmen geschaffen, welcher der Amtsgeheimnisverletzung bei staatlichen Angestellten entspricht. Dies könnte negative Auswirkungen für Informanten (Whistleblower) haben, welche berechtigterweise auf Missstände in ihren Unternehmen aufmerksam machen wollen. Wir lehnen die neue Bestimmung deshalb ab.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	57	1		**Vollzug durch die Kanton**e Die Unterstellung der Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unter das Bundesgesetz über den Datenschutz wird begrüsst.
Fehler! Verweisquelle konnte nicht gefunden werden.	ZPO				**Zivilprozessordnung (ZPO**) Die Erleichterungen für die private Rechtsdurchsetzung durch den Verzicht auf Gerichtskosten und Leistung einer Sicherheit werden begrüsst.
Fehler! Verweisquelle konnte nicht gefunden werden.					**Ermächtigungen zur Datenbearbeitung in anderen Gesetze**n Das totalrevidierte Datenschutzgesetz beruht über weite Strecken auf denselben Grundprinzipien wie das bisherige Recht. Die Tragweite neu geschaffener Vorschriften ist grösstenteils aus sich selbst genügend klar. Unmittelbarer Änderungsbedarf in Einzelgesetzen besteht somit nur beschränkt. Jedenfalls ist die Totalrevision des Datenschutzgesetzes nicht der richtige Ort, um spezifische Bestimmungen zur Bearbeitung von Personendaten in einzelnen Bundesgesetzen zu schaffen oder abzuändern. Sofern der Bundesrat hier Änderungen anstrebt, sind diese im Rahmen einer Revision des jeweiligen Bundesgesetzes zu diskutieren und allenfalls zu beschliessen. Nur so erscheint als gewährleistet, dass die im Rahmen der konkreten

					Materie vorzunehmenden Abwägungen im Gesetzgebungsprozess mit der erforderlichen Sorgfalt getroffen werden. Abgesehen von redaktionellen Änderungen, welche sich aus der neuen Terminologie ergeben, ist daher im Rahmen dieser Revision von der Änderung spezifischer datenschutzrechtlicher Bestimmungen in Einzelgesetzen abzusehen. Namentlich sind sämtliche Bestimmungen, mit denen Ermächtigungen zur Datenbearbeitung in anderen Gesetzen geschaffen oder ausgedehnt werden, zu streichen. Dies betrifft insbesondere die Ermächtigungen zum Profiling. In den Bundesgesetzen müssen individuelle, klare und strenge Rahmenbedingungen für das Profiling vorgesehen werden.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	13	3 und 4		**Informationspflicht bei der Beschaffung von Personendaten** Die Bestimmungen gilt auch für die Auskunftspflicht nach Art. 20 Abs. 2 lit. g. Zur Erfüllung der *Informationspflicht* ist die Bekanntgabe der Kategorien der bearbeiteten Daten, der Kategorien der zur Auftragsbearbeitung übergebenen Daten und der Kategorien der Datenempfänger ausreichend. Die *Auskunftspflicht* hingegen muss aber neben den Daten auch die Empfänger der Daten – und nicht nur deren Kategorien umfassen. Eine Unterscheidung der Auskunftspflicht und der Informationspflicht ist daher (in Art. 20) sinnvoll.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	20	1		**Auskunftsrecht und Kosten** Die Auskunft ist - wie im Vorentwurf vorgesehen - kostenlos vom Verantwortlichen zu leisten.
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.		

digitalswitzerland

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

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

4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Frau Bundesrätin

Hiermit nehmen wir Stellung zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes. Dürfen wir Sie bitten, digitalswitzerland für zukünftige Einladungen zu Vernehmlassungsantworten auf die Adressliste zu setzen.

digitalswitzerland schliesst sich der Stellungnahme des Dachverbands der Schweizer Wirtschaft economiesuisse an und möchte nachfolgend auf die wesentlichsten Punkte kurz eingehen.

Unsere Kernanliegen kurz notiert

Profiling
Die im jetzigen Entwurf vorgesehene Verschärfung, die sogar über europäische Reformbestrebungen ausgeht, gilt es zu aufzuheben. Auch wir plädieren für mehr Information statt Einwilligung. Im digitalen Zeitalter nimmt das personalisierte Marketing und dadurch massgeschneiderte und zielgruppengerechte Werbung zu. Neue und bestehende Firmen sind heutzutage auf solche Kanäle angewiesen, um für ihre Produkte und Dienstleistungen zu werben. Im Vergleich zum Ausland könnte uns dadurch ein erheblicher Wettbewerbsnachteil entstehen.

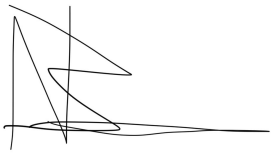
Selbstregulierung
Wir unterstützen die Richtung der Selbstregulierung. Wir lehnen aber die Genehmigung dieser Empfehlungen der guten Praxis seitens EDÖB klar ab. Empfehlungen funktionieren nur, wenn diese von “Innen”, also Verbänden, kommen. Die jetzige Regelung, dass das EDÖB die Empfehlungen genehmigen muss, lässt kaum Freiraum und macht die Empfehlungen faktisch zum Gesetz. Dadurch können die unterschiedlichen Bedürfnisse der betreffenden Branchen kaum einzeln geprüft werden.

Informationspflichten und Sanktionssystem

Die definierten Informations- und Meldepflichten greifen zu weit und sind massiv zu reduzieren. Auch die private, strafrechtliche Sanktionierung ist unverhältnismässig. Die erste der sieben Leitlinien für die Revision des Datenschutzrechts ist die “Einführung und Orientierung am risikobasierten Ansatz”. Der eigentlich zu erwartende Umsetzungsspielraum, der durch den Wegfall von detaillierten Regelungen entsteht, wird aufgehoben durch den starken Ausbau strafrechtlicher Sanktionierung bei zahlreichen Pflichtverletzungen. Auch die weitreichenden Informations-und Meldepflichten generieren bei den Unternehmen massiven Mehraufwand.

Wir bedanken uns für die Berücksichtigung unserer Eingabe und stehen für Fragen jederzeit gerne zur Verfügung.

Freundliche Grüsse
digitalswitzerland



Nicolas Bürer
Geschäftsführer

Daniel Scherrer
Leiter Kommunikation

Amstutz Jonas BJ

Von: _BAG-Direktionsgeschäfte
Gesendet: Dienstag, 4. April 2017 07:54
An: Amstutz Jonas BJ
Betreff: WG: Totalrevision DSG//Vernehmlassung Vorentwurf
Anlagen: Totalrevision_DSG_Stellungnahme_Daten_und_Gesundheit.doc

Guten Morgen Herr Amstutz

Wir haben eine weitere Stellungnahme erhalten, die fälschlicherweise an unsere Adresse weitergeleitet wurde. Ich sende sie Ihnen in der Beilage.

Mit freundlichen Grüssen
Patrick Allemann

Von: Saxer Markus BAG **Im Auftrag von** _BAG-DM
Gesendet: Dienstag, 4. April 2017 06:52
An: _BAG-Direktionsgeschäfte <direktionsgeschaefte@bag.admin.ch>
Betreff: WG: Totalrevision DSG//Vernehmlassung Vorentwurf

Von: Mathis Brauchbar [mailto:mathis@brauchbar.com]
Gesendet: Montag, 3. April 2017 20:30
An: _BAG-DM <DM@bag.admin.ch>
Cc: Verein Daten und Gesundheit <contact@datenundgesundheit.ch>
Betreff: Totalrevision DSG//Vernehmlassung Vorentwurf

Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Für die Möglichkeit, uns an der Vernehmlassung zum Vorentwurf einer Totalrevision des Datenschutzgesetzes zu beteiligen, möchten wir uns bedanken.

Der Verein Daten und Gesundheit ist einer Totalrevision gegenüber grundsätzlich positiv eingestellt. Als national tätiger Verein, der die bürgerzentrierte Nutzung von Gesundheitsdaten fördert, ist der Verein stark an der Datenschutzgesetzgebung und der Datenpolitik in der Schweiz interessiert.

Unsere Kommentare zum aktuellen Vorentwurf finden Sie in der beiliegenden Stellungnahme.

Für die weiteren Arbeiten an der Datenschutzgesetzgebung sowie an den weiteren Erlassen wünschen wir Ihnen viel Erfolg.

Mit freundlichen Grüssen

Mathis Brauchbar, Aktuar

Verein «Daten und Gesundheit»
c/o Mathis Brauchbar
Hambergersteig 17
CH-8008 Zürich
www.datenundgesundheit.ch
contact@datenundgesundheit.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 : Verein Daten & Gesundheit

Abkürzung der Firma / Organisation : DuG

Adresse : c/o M. Brauchbar, Hambergersteig 17, 8008 Zürich

Kontaktperson : M. Brauchbar

Telefon : 0794079362

E-Mail : contact@datenundgesundheit.ch

Datum : 3.4.2017

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!

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 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 8

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 8

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten 9

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") 9

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" 10

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. DuG	**Totalrevision**: Der Verein Daten und Gesundheit ist grundsätzlich einer Totalrevision gegenüber positiv eingestellt. Als national tätiger Verein, der die bürgerzentrierte Nutzung von Gesundheitsdaten fördert, ist der Verein stark an der Datenschutzgesetzgebung und der Datenpolitik in der Schweiz interessiert. Zu diesem Zweck engagiert sich Daten und Gesundheit auch in der neu gegründeten Swiss Data Alliance. Daten und Gesundheit stellt im Zusammenhang mit der Totalrevision DSG fest, dass die zentralen Fragen, die für die Datenwirtschaft und –gesellschaft in der Schweiz gelöst werden müssen, nicht adressiert sind. **Daten und Gesundheit empfiehlt, die Chance einer Totalrevision dazu zu nutzen, nicht nur die Datenschutz-, sondern ergänzend auch die Datennutzungsgesetzgebung voranzubringen. Ob dies im Datenschutzgesetz stehen muss, ist letztlich eine formale Frage. Aber es bietet sich jetzt die Chance, den Datenschutz richtig zu verorten, und gleichzeitig Nebenaspekte, die nicht weggedacht werden können, zu adressieren. Dies betrifft insbesondere das Recht auf Kopie und die Datenportabilität (siehe weiter unten).** **Der Vorentwurf löst die sich stellenden Probleme nicht, verursacht umgekehrt aber hohe Kosten.** 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. Daten und Gesundheit ist diesbezüglich sehr besorgt.
DuG	**Insgesamt kommt Daten und Gesundheit zur folgenden Empfehlung**: **Der Vorentwurf muss zurückgezogen und fundamental überarbeitet werden.**
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**Daten und Gesundheit fordert, dass mit der laufenden Gesetzgebung auch ein Recht auf Kopie in die Schweizerische Gesetzgebung eingeführt wird.** Ob das Recht auf Kopie formal im Datenschutzgesetz zu regeln ist oder in einer Nebengesetzgebung, ist ohne Bedeutung. In den nachfolgenden Abschnitten führt Date und Gesundheit Ergänzendes bzw. Erläuterndes zur Begründung an.

Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**Begriffliches zum Recht auf Kopie bzw. Recht auf Datenportabilität:** 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 verbieten; 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).
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**Daten und Gesundheit fordert, die Diskussion zum Recht auf Kopie mit verbesserten Detailkenntnissen zu führen.**
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**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 Da-ten 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-Daten-schutzgrundverordnung im Rahmen dieser Geschäftsbeziehungen zu gewährleisten.
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**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.
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**Daten und Gesundheit fordert, den Nutzen von Datenportabilität bzw. vom Recht auf Kopie zur Kenntnis zu nehmen und diesbezüglich gesetzgeberisch tätig zu werden.**
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**Kommentar zum Vorgehen** (Abschreibung des Postulats Derder) **(15.4045)**: 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). – Daten und Gesundheit ist 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.

	Daten und Gesundheit 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.
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**Ergänzende Informationen technischer und organisatorischer Art und Umsetzungshinweise:** ● Daten und Gesundheit 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 Datenportabilität bedarf 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.
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**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 ohnehin 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.
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**Daten und Gesundheit spricht sich für eine aktive Vorwärtsstrategie zum Recht auf Kopie und ggf. zum Recht auf Datenportabilität aus**.
Fehler! Verweisquelle konnte nicht gefunden werden. DuG	**Daten und Gesundheit schlägt vor, den folgenden Artikel in das Datenschutzgesetz oder ein Nebengesetz aufzunehmen**: *(1) Jede Person hat das Recht, Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, sofern das Bearbeiten mithilfe automatisierter Verfahren erfolgt. (Recht auf Kopie)* *(2) Jede betroffene Person hat darüber hinaus das Recht, sie betreffende Profilings, zu den Bedingungen und im Format nach Absatz 1 zu erhalten. (verlängertes Recht auf Kopie)* *(3) Der Bundesrat regelt Einzelheiten. Er kann namentlich das Recht auf Kopie gemäss Absatz 1 generell einschränken oder für bestimmte Fallkonstellationen auch aufheben.* *(4) Der Bundesrat kann einen Anspruch auf Datenportabilität begründen. Er regelt diesfalls Aspekte der massgeblichen Ausgangs- und Eingangsformate. Der Anspruch auf Datenportabilität ist in jedem Fall zwingend (d.h. ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden) und diskriminierungsfrei auszugestalten.* Daten und Gesundheit schlägt vor, den folgenden Artikel auf Verordnungsstufe aufzunehmen: *(1) Das Recht auf Kopie gemäss Art. .. Abs. 1 des Gesetzes gilt nicht in den folgenden Fällen: ..., ..., ...* *(2) Das Recht auf Kopie gilt mit den folgenden Einschränkungen oder nur unter ergänzenden Voraussetzungen für die Branchen, A, B, C: ...* *(3) Die betroffene Person hat das Recht, für die Art. .. Abs. 1 des Gesetzes unterstehenden Daten neben der Herausgabe (mit oder ohne Löschung beim Anspruchsgegner) auch die Portierung auf einen Dritten zu verlangen.*
Fehler! Verweisquelle konnte nicht	

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

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

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

31. März 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Frau Bundesrätin

Im Dezember 2016 haben Sie uns eingeladen, zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. economiesuisse nimmt gestützt auf den Input der betroffenen Mitglieder aus einer übergeordneten, gesamtwirtschaftlichen Sicht wie folgt Stellung:

Kernanliegen der Wirtschaft

Der Umgang mit Daten ist für die Digitale Wirtschaft zentral. «Entfaltungsmöglichkeit der Unternehmen» und «Vertrauen der Nutzer» beschreiben die Leitlinien einer optimalen Datenpolitik. In diesem Sinne gilt es, die übergeordneten Ziele der Strategie «Digitale Schweiz» des Bundesrates im Fokus zu behalten: Zu berücksichtigen ist dabei insbesondere auch der Nutzen der Daten für den digitalen Fortschritt und für die Ausschöpfung des wirtschaftlichen Potentials im Interesse der Konsumenten und Unternehmen. Eine einseitige Orientierung lediglich an potentiellen Risiken ist verfehlt. Zentral ist deshalb: Innovation und Entwicklung dürfen durch den Datenschutz nicht behindert werden.

Die Regulierung hat sich am Verhältnismässigkeitsprinzip zu orientieren und alle Eingriffe sind auf das Minimum zu beschränken. Entsprechend ist im Datenschutzgesetz für die Unternehmen ein Maximum an Flexibilität 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 insbesondere

economiesuisse
Hegibachstrasse 47
Postfach CH-8032 Zürich
Telefon +41 44 421 35 35
Telefax +41 44 421 34 34

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

auch genutzt werden, um bestehende Bestimmungen im Hinblick auf ihre Praxistauglichkeit zu hinterfragen und an die technologische Entwicklung anzupassen.

Die Kernanliegen der Wirtschaft 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);

— 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 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. Die Wirtschaft skizziert ein eigenes Sanktionsmodell als Grundlage für die Entwicklung eines alternativen Lösungsansatzes.

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 Bürgerinnen und 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 Austausch international und insbesondere mit dem EU-Raum nicht unnötig einschränkt. Damit die Schweizer Regulierung aus Sicht der EU ein «angemessenes Schutzniveau» i.S.v. Art. 45 DSGVO gewährleistet, reicht es jedoch, wenn sie die grundlegenden Garantien einhält (vgl. Erw. 104 DSGVO / US-EU Privacy Shields). Die entsprechenden Kriterien sind in der EU-Verordnung abschliessend aufgezählt. 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 sichern; die Wirtschaft darf nicht durch übertriebene Bestimmungen («Swiss Finish») mit unnötigem administrativen und finanziellen Aufwand belastet werden. Dieser wäre gerade 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. Nur die Verwendung von Begriffen, welche mit den internationalen Texten übereinstimmen, erleichtert den internationalen Verkehr.

Auf Basis des Vorentwurfes unter Berücksichtigung der Rückmeldungen der Mitglieder und der Arbeiten in der Arbeitsgruppe Datenschutz sowie in der Rechtkommission wurde der Anpassungsbedarf aus einer gesamtwirtschaftlichen Sicht erarbeitet. Im Folgenden wird aufgezeigt, wie die Regelungen bzw. deren Reichweite mit Sicht auf ihre Praxistauglichkeit abgestimmt werden müssen und wo 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 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, auf freiwilliger Basis eine Regelung zur Bezeichnung eines betrieblichen Datenschutzbeauftragten 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 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. 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.

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

[1] Vgl. dazu EuGH-Entscheid Schrems und Entscheid der EU-Kommission vom 16.12.2016 (keine erneute Einwilligung im Einzelfall).

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 weiterhin 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.

[2] Vgl. mehr dazu unter „Aufsicht und Sanktionen“.

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, sofern sie in Bezug auf den Datenschutz keine risikoreiche Tätigkeit ausüben. Aus systematischen Gründen sollte auch diese Bestimmung in Art. 11 VE-DSG integriert werden.

Fokus auf Praxistauglichkeit bei 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).

Verhinderung einer möglichen Informationsflut 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 strafrechtliche 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

Aufgrund der vorangehenden Überlegungen haben wir eine Grobskizze für ein alternatives Sanktionsmodell ausgearbeitet. 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.

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).

Grundsatz: verwaltungsrechtliche Sanktionen gegen Unternehmen

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.

Eine Sanktionierung der Mitarbeitenden soll 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).

Angepasste Rolle des EDÖB und verbesserte Gewaltentrennung durch eine neu zu bildende Spruchbehörde

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 zu viele Aufgaben bei EDÖB zusammenfliessen. 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).

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 etwa:

- 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.

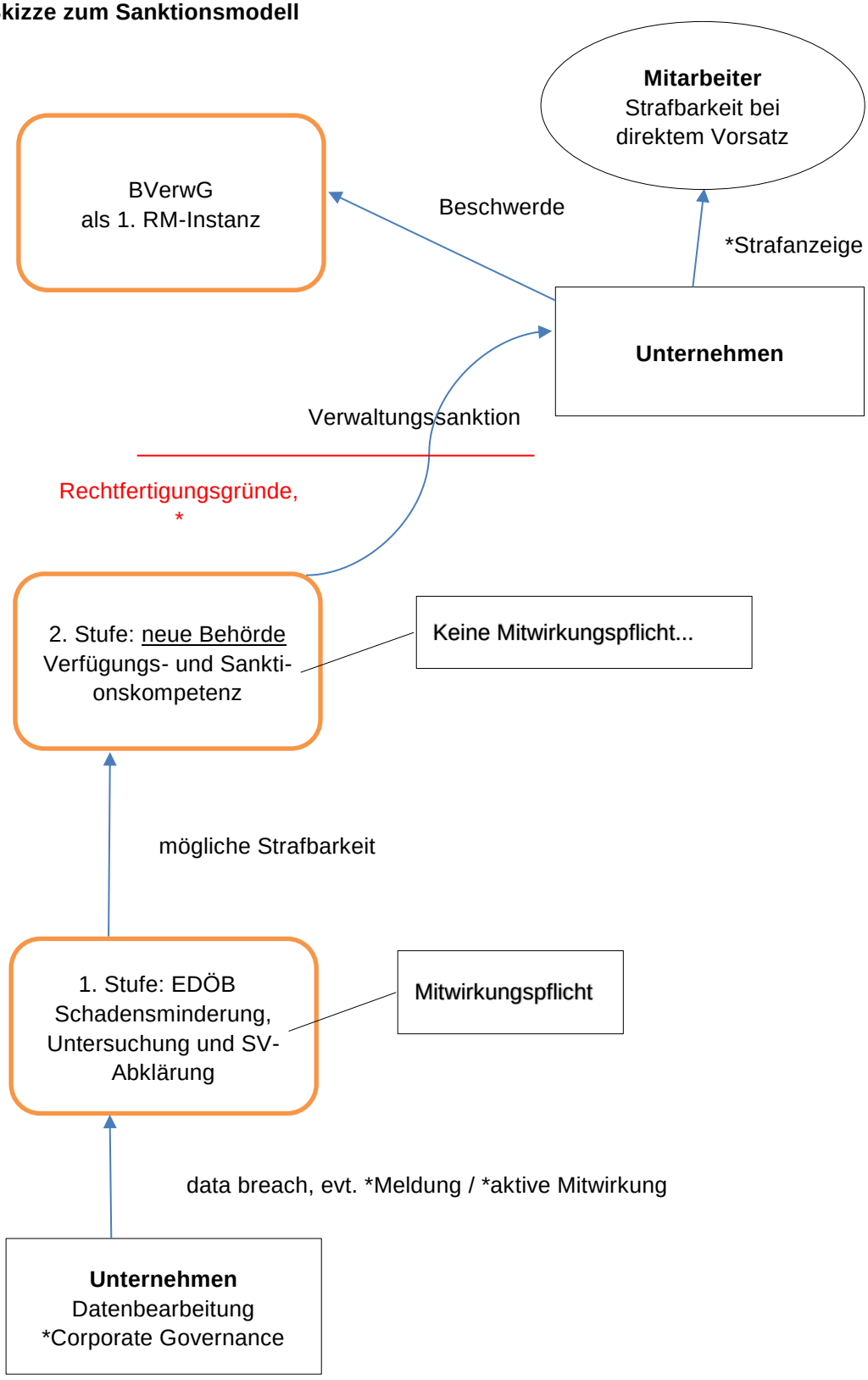
Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
economiesuisse

Thomas Pletscher
Mitglied der Geschäftsleitung

Erich Herzog
Stv. Leiter Wettbewerb & Regulatorisches

Anhang: Skizze zum Sanktionsmodell



ENERCOM
EnerCom Kirchberg AG

Eidg. Justiz- und
Polizeidepartement
- 4. April 2017

BA Justiz
E - 5. April 2017
Act

Eidgenössisches Justiz-
und Polizeidepartement EJPD
Bundesrätin Frau Sommaruga
Bundesrain 20
3003 Bern

Kirchberg, 03.04.2017

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 EnerCom Kirchberg AG gerne wahr.

Die EnerCom Kirchberg 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 an-

---

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.

wesenden 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 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
	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.	**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
	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.
[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.	**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:	**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 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:	

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;	**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.
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);	

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

Alfred Bütikofer
VR-Präsident

Beat Wyss
Leiter Betriebe

Amstutz Jonas BJ

Von: Imsand Cheseaux Barbara <Barbara.Imsand@chuv.ch>
Gesendet: Dienstag, 4. April 2017 17:12
An: Amstutz Jonas BJ
Betreff: LPD prise de position ERSP
Anlagen: ERSP_Révision LPD_prise de position_04032017.docx

Cher Monsieur Amstutz,

Voici la prise de position de l'ERSP concernant le projet de LPD.

Merci et meilleures salutations

CHUV
centre hospitalier universitaire vaudois

Barbara Imsand PharmDipl, MAS
Cheffe d'unité uFSP et Coordinatrice ERSP

Unité des formations en santé publique (uFSP)
IUMSP - Institut universitaire de médecine sociale et préventive
Biopôle 2, Etage 2, Bureau 143
Route de la Corniche 10, CH - 1010 Lausanne

+ 41 (0)21 314 3357 TEL
barbara.imsand@chuv.ch
http://www.iumsp.ch/fr

ersp école romande de santé publique

Pôle romand de la swiss school of public health +

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 : Ecole Romande de Santé Publique

Abréviation de la société / de l'organisation : ERSP

Adresse : Biopole 2, Route de la Corniche 10, CH-1010 Lausanne

Personne de référence : Barbara Imsand

Téléphone : +41 21 314 3357

Courriel : barbara.imsand@chuv.ch

Date : 04.04.2017

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

Remarques générales 3

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 7

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 10

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel 10

Rapport explicatif : chap. 8 « Commentaire des dispositions » 10

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 :
ERSP	L'ERSP 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.
ERSP	De manière générale, l'avant-projet de révision de la LPD a été judicieusement conçu. L'ERSP 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.
ERSP	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.
ERSP	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).
ERSP	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.
ERSP	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.
ERSP	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

ERSP	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).
ERSP	Dans le cadre de la présente prise de position, l'absence de remarque sur une disposition ne vaut pas approbation de la part de l'ERSP.

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 :
ERSP	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.* »

ERSP	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.
ERSP	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			**L'ERSP salue l'introduction d'un devoir de protection des données dès la conception et par défaut. Cette disposition doit absolument être maintenue.**

ERSP	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.
ERSP	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:* - *…* - *…* -

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 :
ERSP	

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 :
ERSP	

Rapport explicatif : chap. 8 « Commentaire des dispositions »

nom/société	art.	remarque / suggestion :
ERSP		

Rat der Eidgenössischen Technischen Hochschulen ETH-Rat
Präsident

Conseil des écoles polytechniques fédérales CEPF
Président

Consiglio dei politecnici federali CPF
Presidente

Cussegl da las scolas politecnicas federalas CSPF
President

Board of the Swiss Federal Institutes of Technology ETH Board
President

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz
3003 Bern

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

Zürich, 14. März 2017/MW

Vernehmlassung zur Totalrevision des Datenschutzgesetzes

Sehr geehrte Damen und Herren

Für die Gelegenheit, im Rahmen der Vernehmlassung zur Totalrevision des Datenschutzgesetzes Stellung zu nehmen, bedanken wir uns. Wir haben die Institutionen des ETH-Bereichs gebeten, die Vorlage zu prüfen und geben die eingegangenen Rückmeldungen mit dem beiliegenden Formular wieder. Dabei ordnen wir die einzelnen Bemerkungen der Institution zu, die sie jeweils eingebracht hat, da die Institutionen des ETH-Bereichs beim vorliegenden Geschäft nicht in jedem Fall alle Positionen teilen.

Der vorliegende Entwurf für eine Totalrevision des Datenschutzgesetzes wird von den Institutionen des ETH-Bereichs grundsätzlich begrüsst. Er ist klar in der Struktur und Nomenklatur. So ist die Nennung von Personendaten und Bundesorganen nachvollziehbar und einheitlich. Ebenso erweist sich der Katalog der besonders schützenswerten Personendaten im vorliegenden Entwurf als verständlich.

Besonders begrüssenswert ist aus Sicht des ETH-Bereichs Art. 8 Abs. 2 bezüglich der Empfehlungen der guten Praxis. Wir unterstützen ausdrücklich die Regelung, wonach der Beauftragte (EDÖB) bei der Erarbeitung dieser Empfehlungen die interessierten Kreise beizieht. Ebenso begrüssen wir, dass die interessierten Kreise die Empfehlungen des Beauftragten ergänzen können oder eigene Empfehlungen erarbeiten könnten, die sie vom Beauftragten genehmigen lassen können.

Hingegen bedauern wir, dass gemäss Art. 36 die verantwortlichen Bundesorgane dem Beauftragten ihre Datenbearbeitungstätigkeiten ausnahmslos zu melden haben und damit offenbar die Möglichkeit fallen gelassen werden soll, dem Beauftragten einen eigenen betrieblichen Datenschutzverantwortlichen zu melden. Dies stellte bisher eine wesentliche Vereinfachung dar, auf die nun ersatzlos verzichtet werden soll.

Ferner möchten wir den aus unserer Sicht wichtigen Hinweis der EPFL in Bezug auf das Amtsgeheimnis hervorheben: aufgrund des tiefgreifenden Wandels im IT-Bereich, insb. beim *Outsourcing* und den *Cloud services*, stellt sich die Frage, wie das Amtsgeheimnis, das vor mehreren Jahrzehnten geschaffen wurde, heute vor dem Hintergrund des Transparenzprinzips (Öffentlichkeitsprinzip) genau auszulegen bzw. neu zu definieren ist (vgl. dazu die Ausführungen der EPFL zu Art. 43 Abs. 2 in der Beilage).

Dr. iur. Fritz Schiesser | Häldeliweg 15, CH-8092 Zürich | Telefon: +41 44 632 20 01 | Fax: +41 44 632 14 10 | E-Mail: schiesser@ethrat.ch

Alle weiteren Anregungen und Anliegen, die von den Institutionen des ETH-Bereichs eingebracht wurden, entnehmen Sie bitte der Zusammenstellung der Rückmeldungen in der Beilage. Wir bedanken uns für die Kenntnisnahme dieser Stellungnahme und die Berücksichtigung der vorgebrachten Anmerkungen. Für weitergehende Auskünfte stehen wir gerne zur Verfügung.

Mit freundlichen Grüssen

Fritz Schiesser

Beilage: Zusammenstellung der Rückmeldungen der Institutionen des ETH-Bereichs

Kopien: Frau Verena Weber, GS WBF
Herrn Maurizio Toneatto, SBFI
Institutionen des ETH-Bereichs

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	: Rat der Eidgenössischen Technischen Hochschulen
Abkürzung der Firma / Organisation	: ETH-Rat
Adresse	: Häldeliweg 15, 8092 Zürich
Kontaktperson	: Dr. iur. Fritz Schiesser, Präsident ETH-Rat / Dr. iur. Monique Weber-Mandrin, Leiterin Stabsbereich Recht ETH-Rat
Telefon	: 044 632 53 77
E-Mail	: fritz.schiesser@ethrat.ch / monique.weber@ethrat.ch
Datum	: 14. 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

Allgemeine Bemerkungen ____ **3**

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ **4**

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 ____ **11**

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ____ **11**

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") ____ **12**

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" ____ **12**

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
ETH-Rat	Generell wird der überarbeitete Entwurf zum DSG begrüsst: - Er ist klar in der Struktur und Nomenklatur. - Es wird konsequent von Personendaten und Bundesorganen gesprochen. - Der Katalog zu den besonders schützenswerten Personendaten ist gut verständlich.

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
PSI	DSG	5/6	-	-	Im Fall des PSI werden Patientendaten und damit besonders schützenswerte Daten regelmässig an medizinische Einrichtungen ins Ausland bekannt gegeben. Gemäss Art. 5 ist hierfür ein Entscheid des Bundesrates erforderlich. Gemäss Art. 6 Abs. 1 Bst. a dürfen in Abweichung von Artikel 5 Absätze 1 bis 3 ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn unter anderem die betroffene Person im Einzelfall eingewilligt hat. Für das PSI, das immer wieder Tumorpatienten aus dem Ausland behandelt, ist es wichtig, dass an die Form dieser Einwilligung keine speziellen Anforderungen gestellt werden. Es versteht sich von selbst, dass die Ergebnisse der Behandlung zwingend ins Ausland bekannt gegeben werden müssen, wo diese Patienten ihren Wohnsitz haben. Wichtig ist, dass von einer stillschweigenden Einwilligung ausgegangen werden darf, wenn ein Patient eigens für die Tumorbehandlung in die Schweiz einreist.
ETH-Rat	DSG	5	5	-	Es ist uns bewusst, dass der Beauftragte für die Genehmigung genügend Zeit braucht. Trotzdem stellt sich die Frage, ob 4 oder 5 Monate auch reichen würden, denn 6 Monate sind eine relativ lange Zeit und könnten in der Praxis zu Schwierigkeiten führen.
ETH-Rat	DSG	8	2	-	Begrüssenswert ist, dass der Beauftragte bei der Erarbeitung der Empfehlungen der guten Praxis die interessierten Kreise beizieht und die Besonderheiten des jeweiligen Anwendungsbereichs (insb. Bildungsbereich) sowie den Schutz von besonders schutzbedürftigen Personen berücksichtigt. Ebenfalls begrüsst wird, dass der Verantwortliche sowie interessierte Kreise die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten können, die dem Beauftragten zur Genehmigung vorlegt werden. Somit kann der ETH-Bereich, falls er dies wünscht, spezifisch auf die besonderen Bedürfnisse des Hochschulwesens und der Forschung hinweisen und mitwirken.
ETH-Rat	DSG	12	3	-	Dies ist eine begrüssenswerte Abgrenzung zum Amts- oder Berufsgeheimnis.

ETH Zürich	DSG	12	4	-	Mindestens in der Botschaft sollte festgehalten sein, dass Art. 34 Abs. 4 lex specialis zu Art. 12 Abs. 4 ist. Somit sollen Erben generell nicht die Daten verstorbener Personen aus den Studierenden- oder Personaldossiers der ETH löschen können.
Empa	DSG	12	5	-	Der Vorbehalt von Abs. 5 sollte sich auf spezielle Bestimmungen des DSG selber beziehen.
EPFL	DSG	13	-	-	L'information systématique de la personne concernée sera extrêmement difficile à mettre en pratique, y compris la mention de la base juridique du traitement (art.13). Le traitement des données étant déjà limité par la loi, cette information n'est pas nécessaire et causera une charge de travail importante. Les personnes concernées seront de plus noyées sous un lot de notices et n'en prendront plus connaissance. L'Union européenne est d'ailleurs déjà en train de faire machine arrière en matière de cookies. D'autre part, les organes fédéraux ne pouvant que traiter des données si la loi le prévoit, l'exception de l'art. 14 al. 2 lit 2 s'appliquerait toujours, mais serait limitée aux données qui ne sont pas collectées auprès de la personne concernée. Cette exception devrait au contraire s'appliquer de manière systématique, indépendamment de savoir où les données sont collectées.
PSI	DSG	13	1	-	Ergänzte Formulierung: „Der Verantwortliche informiert die betroffene Person über die Beschaffung von *nicht bereits öffentlich zugänglichen* Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden." Begründung: Art. 13 Abs. 1 ist zu präzisieren, damit nicht durch Bagatellvorgänge (z.B. durch den Blick ins Telefonbuch) eine umfangreiche Informationspflicht ausgelöst wird.
ETH Zürich	DSG	16	-	-	Der EDÖB sollte Dokumentvorlagen für die Datenschutz-Folgenabschätzung zum Download anbieten. Begründung: Für die Forschenden der ETH Zürich gehören die Datenschutzanalyse und privacy by design schon heute zum Standard. Die ETH Zürich würde es aber begrüssen, wenn der EDÖB zur Datenschutz-Folgenabschätzung gemäss Art. 8 Vorentwurf einheitliche, unkomplizierte Vorlagen online zur Verfügung stellen würde. Diese könnten – im Umfang aber reduziert und vereinfacht – auf den Dokumentvorlagen „Schutzbedarfsanalyse" und „ISDS" gemäss HERMES 5 basieren (www.hermes.admin.ch; Anwenden).

ETH Zürich	DSG	16	4	-	Neue Formulierung: „Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von einem Monat nach Erhalt aller erforderlichen Informationen mit.“ Begründung: Die lange Frist von 3 Monaten für die Rückmeldung des EDÖB, ob er Einwände gegen vom Datenbearbeiter vorgesehene Schutzmassnahmen hat, ist unbefriedigend und mit der Praxis (Forscheralltag) schwer zu vereinbaren, da (Forschungs-)Projekte so lange in einem Schwebezustand sind. Eine Verkürzung dieser Frist auf 1 Monat oder mindestens die pragmatische zeitnahe Handhabung dieser Maximalfrist wäre begrüssenswert.
EPFL	DSG	27	2	-	Les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale, qui doit être formelle s'il s'agit du traitement de données sensibles, de profilage ou de la prise d'une décision individuelle automatisée au sens de l'art. 15 al. 1. L'art. 27 al. 2 doit préciser que même s'agissant du traitement de données sensibles, de profilage ou de la prise d'une décision individuelle automatisée au sens de l'art. 15 al. 1, une loi au sens matériel peut suffire dans certains cas. Pour toutes les autres données, une base légale matérielle est toujours suffisante. Avec la formulation proposée, on pourrait penser que dans certains cas une base légale formelle est aussi nécessaire pour les données qui ne sont pas sensibles. Les EPF sont des institutions décentralisées et il est donc plus difficile d'obtenir une base légale formelle. Les exceptions de l'art. 27 al. 2 doivent être alternatives et non cumulatives. Une base légale matérielle doit suffire au traitement de données sensibles, de profilage ou de la prise d'une décision individuelle automatisée au sens de l'art. 15 al. 1 soit si le traitement est indispensable à l'accomplissement d'une tâche clairement définie dans une loi au sens formel (a), soit si le traitement n'est pas susceptible d'entraîner des risques particuliers pour la personnalité et les droits fondamentaux de la personne concernée (b).
ETH-Rat	DSG	28	-	-	Dieser Artikel ist begrüssenswert, denn er führt zu mehr Flexibilität bei Pilotprojekten.
EPFL	DSG	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 comme l'EPFL conformément à l'art. 4 al. 3 LAr et l'annexe 2 OLAr.

					L'archivage des données est une activité complexe pour les EPF. La révision de la LPD serait l'occasion de confier cette tâche aux Archives fédérales. D'après l'EPFL et dans le sens de l'art. 31 de l'avant-projet de LPD, l'annexe 2 OLAr doit être modifiée. Pour l'EPFL, une gestion des archives des EPF assumée par les Archives fédérales paraît souhaitable.
ETH Zürich	DSG	32	2	-	Begrüssenswert wäre, wenn der Katalog in 32 Abs. 2 noch um die Informations- und Meldepflichten erweitert würde.
ETH-Rat	DSG	32	-	-	Dies ist ein für den ETH-Bereich zentraler Artikel, es wird begrüsst, dass er übernommen wurde.
Empa	DSG	34	2	-	Es ist zu befürchten, dass der Aufwand für das Anbringen des verlangten Bestreitungsvermerks gross ist und auch die Einschränkung der Bearbeitung mit viel Aufwand verbunden sein wird. Die Empa schlägt vor, dass zumindest in der Verordnung zum DSG klare Ausführungen zu besagtem Bestreitungsvermerk erfolgen, welche einerseits den Aufwand für die Bundesorgane klein halten und andererseits der betroffenen Person keine Rechte eingeräumt werden, um über die Einschränkung der Bearbeitung mitzubestimmen.
ETH-Rat und Empa	DSG	34	4	-	Dieser Absatz ist begrüssenswert, aber es erscheint unklar, ob die Forschungsanstalten des ETH-Bereichs (PSI, WSL, Empa, Eawag) auch zu den „Bildungseinrichtungen" gehören. U.E. sollten sie dazugehören, was in den Erläuterungen zu präzisieren ist.
EPFL	DSG	34	4	-	L'art. 34 al. 4 prévoit que la rectification, l'effacement ou la destruction de données personnelles ne peut être exigée des bibliothèques, des établissements d'enseignement, des musées, des archives accessibles au public et des autres institutions patrimoniales publiques pour les fonds qu'elles gèrent. Pour éviter tout doute sur la portée de la notion d'établissement d'enseignement, l'art. 34 al. 4 devrait inclure les établissements de recherche.
ETH-Rat	DSG	36	-	-	Der Verzicht auf die Möglichkeit, dem Datenschutzbeauftragten einen eigenen betrieblichen Datenschutz-verantwortlichen melden zu können (Art. 11a Abs. 5 Bst. 5 i.V.m. Art. 12a Verordnung DSG), wird bedauert. Wichtig ist zu wissen, wie die Verordnung zum DSG das Meldeverfahren der Datenbearbeitungs-tätigkeiten der Bundesorgane genau regeln wird.

EPFL	DSG	36	-	-	L'art. 36 prévoit que les traitements (au lieu des fichiers) doivent être déclarés. La notion de traitement, comme le prévoit la définition de l'art. 3 est extrêmement large. Les EPF devront donc faire face à des centaines de déclarations, d'autant qu'aucune limite n'est prévue. L'enregistrement des données les plus insignifiantes, comme l'enregistrement du nom de la personne à qui un casier est prêté quelques heures pour déposer ses affaires dans une bibliothèque devrait être déclaré, de même que l'effacement de ce nom lorsque la clé est restituée! Comme c'est le cas aujourd'hui pour les personnes privées, la déclaration est une charge de travail importante qui n'améliore pas la protection des données et qui n'est que rarement effectuée correctement. Il convient d'y renoncer également pour les organes fédéraux. Au surplus, seuls les traitements prévus par la loi sont admissibles. Il est donc déjà possible de savoir quels traitements sont effectués. La déclaration revient donc à faire double emploi.
EPFL	DSG	43	-	-	Le PFPDT pourra ordonner la suspension, la modification ou la cessation de tout ou partie du traitement ainsi que la destruction de tout ou partie des données en cas de violation des dispositions de protection des données, ainsi que suspendre ou interdire la communication de données personnelles à l'étranger si elle est contraire aux conditions des art. 5 ou 6 ou à des dispositions spéciales d'autres lois fédérales en matière de communications de données personnelles à l'étranger (art. 43). Au vu des incertitudes sur la portée du secret de fonction et la légalité de l'outsourcing (y compris lorsqu'il est nécessaire et donc justifié par le *Sozialadäquanz),* on ne peut pas exclure que le PFPDT voie dans le recours à un fournisseur informatique étranger pour traiter des données potentiellement couvertes par le secret de fonction une violation d'une disposition spéciale d'une autre loi fédérale, y compris le code pénal. 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. Du point de vue de l'EPFL, bien que l'OAIF ne soit pas applicable directement au domaine des EPF, son art. 26 qui prévoit l'outsourcing (a priori en Suisse seulement) devrait être coordonné avec la LPD (qui renvoie aux obligations d'autres lois) et la notion de secret de fonction au sens de l'art. 320 CP (qui selon les interprétations interdit tout outsourcing ou l'outsourcing hors de Suisse). Il y a apparemment des incohérences et il est nécessaire de traiter ce sujet. 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. Au surplus, l'art. 51 al. 1 prévoit une amende jusqu'à 500'000 francs pour les personnes privées qui intentionnellement, violent certains devoirs. La let. b punit le fait de confier le traitement de données à un sous-traitant en violation de l'art.7 al. 1 et 2. Il y a un risque de double sanction pénale de la violation d'un secret, à la fois sous l'angle de la disposition de l'art. 320 CP et ensuite sous l'angle de l'art. 51!
ETH Zürich	DSG	50-53	-	-	Die Botschaft äussert sich zur Abgrenzung der Strafbarkeit zwischen privaten Personen und Geschäftsbetrieben (Unternehmen). Zur Abgrenzung der Strafbarkeit zwischen Bundesorganen und ihren Angestellten äussert sie sich jedoch kaum bzw. unklar. Wann ist von Letzteren wer strafbar? Klare Ausführungen dazu wären wünschenswert.
EPFL	DSG	50-53	-	-	Les art. 50 et 51 prévoient des sanctions pénales sous la forme d'amende jusqu'à 500'000 francs pour les personnes privées qui intentionnellement, violent certains devoirs. Le commentaire de l'art. 51 indique que cette disposition ne s'applique pas aux organes fédéraux, ce qui est à saluer, mais il faudrait en revanche le préciser dans le texte de la loi. Il y a en effet un petit risque que la notion de personne privée puisse être interprétée comme étant le fonctionnaire lui-même. Il faudrait aussi préciser que cela s'applique aussi bien pour l'art. 50 car la terminologie est la même pour les art. 50 et 51.
EPFL	DSG	52	-	-	La révélation intentionnelle de données personnelles secrètes serait un délit pénal. L'art. 52 restreint ainsi fortement la communication de données qui ne sont pas soumises au secret de fonction mais qui devraient être gardées secrètes. Même si de tels cas semblent plutôt rares pour les EPF, il est toutefois fondamental de préciser que cet article ne concerne pas la révélation à un sous-traitant, une telle révélation ne devant pas être un délit pénal au risque d'empêcher tout fonctionnement des EPF.
PSI	DSG	52	-	-	Der Begriff der „geheimen Personendaten“ ist nicht definiert und u.E. unklar.

EPFL	ETH-Gesetz vom 4. Oktober 1991	36	-	-	Les art. 36a ss LEPF prévoient que les données pouvant être traitées, soit des données concernant le personnel (36a) et les études (36b). La révision de la LEPF va ajouter un art. 36c permettant de traiter les données de recherches. Ces catégories sont bien trop limitées et doivent être étendues pour tenir compte des besoins réels des EPF. La LEPF doit être complétée pour que les EPF et les établissements de recherche puissent traiter des données personnelles, y compris des données sensibles, dans le cadre de la recherche de fonds, la promotion de l'institution, les relations avec les tiers, la gestion du campus, l'administration des sites web, etc. Une délégation de compétence à la Direction de l'EPFL et l'ETZH doit aussi être ajoutée pour adopter une base légale permettant le traitement d'autres données.
ETH Zürich und ETH-Rat	ETH-Gesetz vom 4. Oktober 1991	36	c	1	Änderung der Formulierung: „Die ETH und die Forschungsanstalten können im Rahmen von Forschungsprojekten Personendaten, einschliesslich besonders schützenswerter Personendaten ~~*sowie Persönlichkeitsprofile*~~, bearbeiten, soweit dies für das entsprechende Forschungsprojekt erforderlich ist. 2 Sie stellen sicher, dass dabei die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz eingehalten werden.“ Begründung: Per 30. September 2016 wurde das ETH-Gesetz geändert. Dabei wurde das Kapitel 6a: Datenbearbeitung eingefügt. Das revidierte Gesetz tritt per 1. Mai 2017 in Kraft. Lediglich der guten Ordnung halber sei nochmals erwähnt, dass im neu einfügten Art. 36c Abs. 1 noch die Terminologie „Persönlichkeitsprofil“ verwendet wird. Der VE-DSG verzichtet darauf.
PSI	Kernenergie-gesetz vom 21. März 2003	24	2		Korrigierte Formulierung: „Im Rahmen dieser Prüfung können Daten über die Gesundheit und psychische Eignung sowie sicherheitsrelevante Daten über die Lebensführung der betroffenen Person bearbeitet werden; *der Bewilligungsinhaber* kann darüber eine Datenbank oder Akten führen.“ Begründung: Die Änderung enthält einen sprachlichen Fehler, es fehlt die Angabe desjenigen, der die Datenbank oder Akten führt.

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

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**

BA Justiz
E - 7. April 2017
Act

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Buchs SG, 3. 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 das Elektrizitäts- und Wasserwerk der Stadt Buchs SG gerne wahr.

Das Elektrizitäts- und Wasserwerk der Stadt Buchs SG 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 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]

---

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 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]

---

[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 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

[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. **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
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 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 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,

VE-DSG	Anträge und Bemerkungen
	die Bearbeitung 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; i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.	**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").

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. [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 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" Datenbear-

VE-DSG	Anträge und Bemerkungen
	beitern 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), 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.	**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	**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"

VE-DSG	Anträge und Bemerkungen
Auswirkungen auf die betroffene Person hat.	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 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 Persönlich-	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschät-

VE-DSG	Anträge und Bemerkungen
keit 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. [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.	zungen 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, 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

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.	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. **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,

VE-DSG	Anträge und Bemerkungen
	diese in ihren Persönlichkeiten schützen.
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 Begrün-

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.	dungspflicht 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 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 be-	

VE-DSG	Anträge und Bemerkungen
arbeitet werden; 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: 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;	**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.

VE-DSG	Anträge und Bemerkungen
f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das 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:	**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
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; 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	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem 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 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 For-	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
schung, Planung und Statistik bearbeiten, wenn: 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	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [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.	

VE-DSG	Anträge und Bemerkungen
[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 [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	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Par-

VE-DSG	Anträge und Bemerkungen
Vorgehen und das Ergebnis einer allfälligen Untersuchung.	teistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte 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.	**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
[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; 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

VE-DSG	Anträge und Bemerkungen
	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.
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 unter-	**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
nehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c 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;	**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.

VE-DSG	Anträge und Bemerkungen
f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert. [2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**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. **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.

VE-DSG	Anträge und Bemerkungen
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone [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.	Keine Bemerkungen
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….	**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
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 ...	

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

Elektrizitäts- und Wasserwerk
der Stadt Buchs

Markus Schommer
Direktor

Matthias Lehmann
Leiter Kommunikation

EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Bundesamt für Justiz
Direktionsbereich öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik
Bundesrain 20
3003 Bern

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

Zürich, 3. April 2017

Stellungnahme zur Vernehmlassung zum Entwurf des Bundesgesetzes über den Datenschutz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Der Bundesrat hat das Eidg. Justiz- und Polizeidepartement (EJPD) am 21. Dezember 2016 beauftragt, bei den interessierten Kreisen zum Entwurf des Bundesgesetzes über den Datenschutz ein Vernehmlassungsverfahren durchzuführen.

Gemäss der Medienmitteilung vom 21. Dezember 2016 will der Bundesrat primär die jüngsten Entwicklungen im Bereich des Datenschutzes in der EU und beim Europarat berücksichtigen sowie mit der Revision die Grundlage dafür schaffen, dass die Schweiz die Datenschutzkonvention des Europarates ratifizieren und die EU-Richtlinie über den Datenschutz im Bereich der Strafverfolgung übernehmen kann. Damit soll sichergestellt sein, dass die grenzüberschreitende Datenübermittlung weiterhin möglich bleibt. Zudem soll die Transparenz bei der Datenbearbeitung erhöht werden, Informationspflichten der Datenbearbeiter ausgeweitet, das Auskunftsrecht der betroffenen Personen präzisiert und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) mehr Kompetenzen verliehen werden. Überdies sollen die Strafbestimmungen verschärft werden.

Gerne nehmen wir zum Vorentwurf Datenschutzgesetz (VE-DSG) wie folgt Stellung:

Auch wir sind der Ansicht, dass das neue Datenschutzrecht der Schweiz den Vorgaben auf EU- und Europarats-Ebene möglichst entsprechen muss. In der VE-DSG sind nun aber verschiedene Regelungen enthalten, die über das Ziel hinausschiessen sowie für die in der Schweiz tätigen Unternehmen zu einem unnötigen administrativen und finanziellen Aufwand und – insbesondere für die international tätigen Unternehmen – zu einem Standortnachteil führen würden.

EXPERTsuisse – Schweizer Expertenverband für Wirtschaftsprüfung, Steuern und Treuhand
Limmatquai 120, Postfach, CH-8021 Zürich, Tel. +41 58 206 05 05, Fax +41 58 206 05 09
info@expertsuisse.ch, www.expertsuisse.ch

Die Totalrevision des Datenschutzgesetzes in der Schweiz darf keinesfalls zur Folge haben, dass der Datentransfer bei grenzüberschreitenden Tätigkeiten der international tätigen Unternehmen erschwert wird. Für die in der Schweiz ansässigen Revisionsgesellschaften, die für einen international tätigen Konzern eine Konzernprüfung durchführen, muss die Zulieferung von Datenmaterial zwischen der Muttergesellschaft und einer Tochtergesellschaft ohne grosse Einschränkung und Aufwand möglich sein.

Der Prüfer, der eine Teileinheit überprüft, ist auf diesen Datentransfer zwingend angewiesen. Es ist somit von grosser Wichtigkeit, dass die Möglichkeit, grenzüberschreitende Daten über verschiedene Kanäle auszutauschen, sichergestellt ist. Ferner ist zu erwarten, dass in ein paar Jahren ein massgebender Teil der Software in einer Cloud abgelegt sein wird. Der entsprechende Server würde dann in der Schweiz oder in der EU bzw. möglicherweise sogar einem Staat ausserhalb der EU liegen. Konzerne, die grenzüberschreitend tätig sind, würden ihre Daten in einer solchen Cloud ablegen.
In der EU-Datenschutz-Grundverordnung (EU-DSGVO) findet sich der Begriff *„Unternehmensgruppe“* (=herrschende(s) Unternehmen und von diesem abhängige Unternehmen). Art. 47 der DSGVO enthält eine Art **Konzernprivileg,** wonach gruppeninterne Datenweitergaben zwischen verbundenen Unternehmen unter erleichterten Voraussetzungen erfolgen. Mittels gruppeninternen vertraglichen Regelungen kann der Mindestinhalt des angemessenen Datenschutzniveaus festgesetzt werden. Es ist im Interesse des Wirtschaftsstandortes Schweiz, sicherzustellen, dass die Äquivalenz zur EU-Regelung gegeben und der grenzüberschreitende Datentransfer mit dem VE-DSG gewährleistet ist.

Mit Art. 52 VE-DSG soll der in Art. 321 StGB vorgesehene Schutz der beruflichen Schweigepflicht ausgebaut werden, da dieser durch die zunehmende Spezialisierung und die neuen Informationsbearbeitungsmethoden lückenhaft geworden sei (siehe Erläuternder Bericht). Gemäss Abs. 1 dieser Bestimmung wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (auf Antrag) bestraft, wer vorsätzlich geheime Daten bekannt gibt. Diese Bestimmung ist von überschiessender Tragweite. Es ist auch nicht wirklich eine Begründung für deren Notwendigkeit ersichtlich. Wohl ist klar, dass die erfolgreiche Ausübung der Berufe gemäss Art. 321 StGB ein besonderes Vertrauensverhältnis zum Klienten voraussetzt. Dementsprechend sind Verletzungen von Geheimhaltungspflichten zu sanktionieren. Alle anderen Berufe, bei welchen durchaus ein Geheimhaltungsbedürfnis besteht, sind aber nicht ohne weiteres gleichzusetzen mit den in Art. 321 StGB genannten. Datenschutzrechtlich ist insbesondere das Verhältnis zu Outsourcing-Konstellationen nicht genügend geklärt (gesetzliche und vertragliche Geheimhaltungspflichten verbieten ja ein Outsourcing ohne Einwilligung).

Für unsere Mitglieder bzw. die gesamte Branche ist das Revisionsgeheimnis eine der wichtigsten Pflichten, die es strikte einzuhalten gilt. Gemäss Art. 730b Abs. 2 OR muss die Revisionsstelle sowohl das Geheimnis über ihre Feststellungen wahren, soweit sie nicht von Gesetzes wegen zur Bekanntgabe verpflichtet ist. Sie wahrt auch die Geschäftsgeheimnisse der Gesellschaft bei der Berichterstattung, der Erstattung von Anzeigen und bei der Auskunftserteilung an die Generalversammlung. Die spezialgesetzlichen Prüfgesellschaften haben noch andere Gesetzesnormen (z.B. Art. 129 Abs. 1 KAG: Prüfgeheimnis) zu beachten. Ferner sei auf das verbandsrechtliche Berufsgeheimnis hingewiesen (vgl. Standes- und Berufsregeln von EXPERTsuisse). Die Pflicht zur *„unverzüglichen“* Meldung an den EDÖB (Art. 17 VE-DSG) birgt das Risiko, dass aus Angst vor der strengen Strafandrohung in Art. 50 Abs. 2 Bst. d VE-DSG vorschnell Informationen an den EDÖB weitergeleitet werden und dabei

(fahrlässig) ein Geschäftsgeheimnis/Berufsgeheimnis verletzt wird. Damit müssen die Unternehmen ihre Prozesse und Systeme deutlich ausbauen, was insbesondere für KMU einen unverhältnismässigen (finanziellen und organisatorischen) Aufwand zur Folge hätte.

Im Übrigen gibt es verschiedene Umsetzungsprobleme der geplanten Regelungen in der Praxis. Zu erwähnen ist beispielsweise das Recht der Betroffenen auf Löschung ihrer Daten. Daten können nur in *„live"*-Systemen gelöscht werden. Daten in einem Backup sind allerdings nicht mit einem vernünftigen Aufwand löschbar.

Wichtig ist auch, dass Innovationen und Entwicklungen in der digitalen Welt nicht durch das Datenschutzgesetz blockiert oder eingeschränkt werden sowie die Strategie des Bundesrates „Digitale Schweiz" im Fokus behalten wird.

Wir beantragen, dass diese Aspekte, insbesondere das Verhältnis zwischen Meldepflicht und Berufsgeheimnis nochmals einer genaueren Betrachtung zu unterziehen sind und bei der Totalrevision des DSG berücksichtigt werden.

Zum Entwurf des Datenschutzgesetzes stellen wir im Einzelnen folgende Hauptanträge:

1. Geltungsbereich

Gemäss dem VE-DSG soll das Datenschutzgesetz auch auf bereits rechtshängige Zivilprozesse und laufende Strafverfahren Anwendung finden, was bei den Auskunftsrechten zu Missbräuchen führen kann. Damit wird die Beweisbeschaffung über die zivilprozessualen Editionsrechte ausgehebelt. Der Geltungsbereich darf in dieser Hinsicht keinesfalls erweitert werden.

Wir beantragen, dass der Geltungsbereich des VE-DSG nicht auf rechtshängige Zivilprozesse und laufende Strafverfahren erweitert wird.

2. Wiederaufnahme Institut des internen Datenschutzbeauftragten

Wie erwartet, orientiert sich der VE-DSG sehr an der EU-DSGVO und es wurden zahlreiche Bestimmungen auf sehr ähnliche Weise übernommen. Es erstaunt daher umso mehr, dass ein wichtiges Element der EU-DSGVO nicht übernommen wurde, nämlich das Institut des betriebsinternen Datenschutzbeauftragten (vgl. Art. 11a Abs. 5 lit. 3 geltendes DSG). Dieser ist im VE-DSG nicht mehr vorgesehen. Weder der, ebenfalls am 21. Dezember 2016 veröffentlichte Erläuternde Bericht, noch eine Stellungnahme des Eidgenössischen Datenschutzbeauftragten erklärt die Löschung des entsprechenden Artikels. Die ersatzlose Streichung ist umso erstaunlicher, weil es sich beim internen Datenschutzbeauftragten um ein Kernelement der EU-DSGVO handelt. Die Streichung führt zu Unsicherheiten und kann u.E. auch zu Problemen im Hinblick auf die Diskussion der Gleichwertigkeit des Schweizerischen Datenschutzes mit demjenigen der EU führen.

Gerade im Hinblick darauf, dass eine grenzüberschreitende Datenübermittlung nach wie vor möglich ist, sollte diese Gleichwertigkeit mit dem aktuellen Vorentwurf angestrebt werden. Zumindest auf

freiwilliger Basis sollten die Unternehmen einen internen Datenschutzbeauftragten einführen können und damit von der Meldepflicht im Sinne von Art. 17 VE-DSG an den EDÖB entbunden sein, was insbesondere für grosse Unternehmen, die aufgrund ihres Gesellschaftszweckes viele Daten bearbeiten müssen, eine grosse Erleichterung wäre.

Wir beantragen die Beibehaltung des betriebsinternen Datenschutzbeauftragten, zumindest auf freiwilliger Basis, und unter gleichzeitiger Entbindung von der Mitteilungspflicht im Sinne von Art. 17 VE-DSG.

3. Begriffe (Art. 3 VE-DSG)

3.1. Bearbeiten

Die Begriffe *"Speichern"* und *"Löschen"* sind unnötig und daher zu löschen.

Wir beantragen die Streichung der Begriffe *„Speichern“* und *„Löschen“.*

3.2. Biometrische Daten (Art. 3 Bst. c Ziff. 3 und 4 VE-DSG)

Die Ausweitung des Begriffs *«besonders schützenswerte 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 des Übereinkommens zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (E-SEV 108). Nach der im VE-DSG vorgeschlagenen Definition wäre beispielsweise künftig jedes Gesichtsfoto als biometrisches Datum erfasst. Die Definition ist entsprechend einzuschränken.

Wir beantragen, die Definition von Art. 3 Bst. c Ziff. 3 und 4 VE-DSG einzuschränken.

3.3. Profiling (Art. 3 Bst. f VE-DSG)

Der Verzicht auf den Begriff *„Persönlichkeitsprofile“* im VE-DSG ist sehr sinnvoll, da dieser immer zu grossen Unsicherheiten geführt hat und er überdies auch im ausländischen Recht kein bekannter Begriff ist. Neu soll *„Profiling“* verwendet werden. Profiling ist *„jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität“.* Ein Profiling ist nur mit der ausdrücklichen Einwilligung der betroffenen Person zulässig. Wer diese Einwilligung nicht einholt, begeht eine widerrechtliche Persönlichkeitsverletzung (vgl. Art. 23 Abs. 2 Bst. d VE-DSG). Gemäss dem Erläuternden Bericht ist massgebend, dass Daten im Hinblick auf die Untersuchung zentraler Persönlichkeitsmerkmale ausgewertet werden. Die Auswertung der Daten kann automatisiert oder nicht-automatisiert erfolgen.

Die Definition des Begriffs *„Profiling“* geht zu weit und auch weiter als die EU-DSGVO. Zukünftig wird beispielsweise jede schriftliche Qualifikation eines Mitarbeiters – ohne explizite Einwilligung des Betroffenen – als Persönlichkeitsverletzung betrachtet. Diese neue Bestimmung ist sehr heikel und nach unserem Dafürhalten ein unnötiges *„Swiss Finish“.* Profiling ist auf die automatisierte Bewertung von Personendaten zu beschränken. Ausserdem sind die Bedingungen zu reduzieren und anstatt einer Einwilligung lediglich eine Informationspflicht festzulegen.

Wir beantragen die Einschränkung des Profiling auf *„besonders schützenswerte Personendaten“* und auf die automatisierte Datenauswertung.

3.4. Auftragsbearbeiter (Art. 3 Bst. i VE-DSG)

Die Bestimmung von Art. 3 Bst. i VE-DSG ist zu ungenau und kann zu Missverständnissen führen.

Wir beantragen daher folgende Präzisierung des Wortlautes: *"… im Rahmen eines Rechtsgeschäfts mit dem Verantwortlichen Personendaten bearbeitet, wobei das Vorliegen eines Arbeitsverhältnisses nicht als Rechtsgeschäft im Sinne dieser Regelung gilt".*

4. Auftragsdatenbearbeitung (Art. 7 VE-DSG)

Die Zustimmungspflicht im (neuen) Art. 7 Abs. 3 VE-DSG zum Sub-Outsourcing ist fragwürdig. Interessanterweise muss in der Systematik der *„Verantwortliche“* die betroffene Person in der Regel nicht um Zustimmung bitten, wenn er ihre Daten outsourct. Der Outsourcer muss dann aber den Verantwortlichen um Zustimmung bitten, wenn er sub-outsourct.

5. Empfehlungen und Einhaltung der guten Praxis (Art. 8 und 9 VE-DSG)

Die Grundidee ist gut, es besteht allerdings das Risiko, dass sie in der Ausführung zu einer Verschärfung des DSG selbst führt. Es fehlen Kontrollmöglichkeiten und Rechtsschutzmechanismen. Auch aus Gründen der Gewaltentrennung sollte die Erstellung der Empfehlungen nicht durch den EDÖB selbst, sondern zwingend durch ein Fachgremium erfolgen. Nur durch den entsprechenden Praxisbezug können sachgerechte Lösungen erarbeitet werden. In der DSGVO wird die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen.

Wir beantragen somit, dass die Empfehlungen der guten Praxis durch ein breit abgestütztes Fachgremium, in welchem neben anderen auch die Wirtschaft vertreten wird, erlassen werden, wobei der EDÖB über eine beratende Stimme verfügt.

6. Daten einer verstorbenen Person (Art. 12 VE-DSG)

Im geltenden DSG ist Art. 12 VE-DSG ein Teilanspruch des Auskunftsrechts. Positiv zu vermerken ist, dass der VE-DSG eine Vorreiterrolle beim *„Persönlichkeitsschutz“* von verstorbenen Personen einnimmt. Art.12 VE-DSG regelt die datenschutzrechtlichen Gegebenheiten nach dem Tod einer Person. Interessanterweise berücksichtigt dies jedoch die EU-DSGVO nicht, obwohl es hierzu seit Jahren

strittige Fälle gibt, z.B. die datenschutzrechtlichen Einstellungen von Facebook, wenn es um die Rechte der Angehörigen nach dem Tode eines Facebook Users geht. Gemäss dieser Regelung sind nebst den (gesetzlichen und eingesetzten) Erben weitere Personen auskunftsberechtigt.

Das Auskunftsrecht geht über den Auskunftsanspruch der Erben hinaus, was unseres Erachtens zu weit geht.

Wir beantragen somit, dass das Auskunftsrecht entsprechend der erbrechtlichen Regelungen auf Erben beschränkt wird.

7. Informationspflicht bei der Beschaffung von Personendaten (Art. 13 VE-DSG)

Nach Art. 13 Abs. 1 VE-DSG muss der Verantwortliche die betroffene Person über die Beschaffung von Personendaten informieren. Diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. Diese Bestimmung soll gemäss dem Erläuternden Bericht vom 21. Dezember 2016 die Transparenz bei der Datenbearbeitung verbessern, was eines der zentralen Ziele der Revision ist.

Der Wortlaut der Bestimmung ist zu unklar und der Begriff *„Beschaffen"* wird nicht definiert, auch nicht in Art. 3 VE-DSG. Im Übrigen geht diese Bestimmung über die EU-DSGVO hinaus. Uns stellt sich insbesondere die Frage, ob ein Internet Research und die Verwertung der darin gefundenen Information zu einer Person bereits unter diese Bestimmung fällt und diese Person informiert werden müsste, was natürlich viel zu weit gehen würde. Die Bestimmung führt zu einer grossen Unsicherheit bei den Unternehmen, auch deshalb weil ein Verstoss sanktioniert wird (vgl. Art. 50 Abs. 1, Bst. a und b, Ziff. 1 und 2 VE-DSG).

Im geltenden DSG besteht die Informationspflicht nur bei der Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen. Als wesentliche Änderung im VE-DSG soll diese Pflicht nun bei allen Daten gelten. Durch eine solche umfassende Informationspflicht würde nicht mehr Transparenz geschaffen, sondern es würde einfach zu einem Mehr an Information kommen, was letztlich der Transparenz zuwiderlaufen würde (kontraproduktive Informationsüberflutung). Eine standardisierte Information in Form von AGB oder in einer generellen Datenschutzerklärung muss genügen. Alles andere ginge viel zu weit.

Wir beantragen daher, dass der Wortlaut nochmals einer kritischen Betrachtung zu unterziehen sei und die Informationspflicht beschränkt wird auf „besonders schützenswerte Personendaten und Persönlichkeitsprofile".

8. Informations- und Anhörungspflichten bei einer automatisierten Einzelentscheidung (Art. 15 VE-DSG)

Der Bundesrat erachtet die Einführung des neuen Begriffs *„automatisierte Einzelentscheidung"* für notwendig, weil diese Entscheidungen in allen Wirtschaftsbereichen immer häufiger und teilweise auf der Grundlage falscher Daten getroffen werden. Eine automatisierte Einzelentscheidung besteht, wenn ohne menschliches Dazutun eine Auswertung von Daten erfolgt, die zu einer konkreten Entscheidung gegenüber der betroffenen Person führt (siehe Erläuternder Bericht zum Vorentwurf).

Dieses Thema ist eine Blackbox, da der Umfang der Informationspflicht unklar ist. Die Übernahme ist aufgrund des E-SEV 108 erforderlich, es wäre allerdings empfehlenswert, den Begriff der *"automatisierten Einzelentscheidung"* in Artikel 3 zu erläutern/definieren. Der völlig uneingeschränkte Äusserungsanspruch geht zudem sehr weit und kann insbesondere auch in kleinen und bescheidenen Verhältnissen zu einem unverhältnismässig und sachlich nicht gerechtfertigten hohen administrativen Aufwand führen. Die Informations- resp. Anhörungspflicht ist eine Einmischung in den zivilrechtlichen Willensbildungsvorgang einer Person bzw. eines Unternehmens. Ein Richtigkeitsgebot würde auch genügen. Auch mit einer allgemeinen Information könnte hier die notwendige Transparenz betreffend die automatisierte Einzelentscheidung erreicht werden, um das effektiv bestehende Bedürfnis nach dem Schutz gegen negative Entscheidfindung mittels falscher Daten zu befriedigen, ohne jedoch die Entwicklung der digitalen Wirtschaft und Gesellschaft übermässig zu behindern.

Wir beantragen, dass der Begriff *„automatisierte Einzelentscheidung“* in Art. 3 VE-DSG zu erläutern ist.

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

Die Datenschutz-Folgenabschätzung ist eine neue Pflicht im VE-DSG, womit die Anforderungen von Art. 8^{bis} Abs. 2 E-SEV 108 sowie die Artikel 27f. der Richtlinie (EU) 2016/680 verwirklicht werden sollen. In der Verordnung (EU) 2016/679 ist eine ähnliche Vorschrift enthalten. Die Datenschutz-Folgenabschätzung soll ein Instrument sein zur Erkennung und Bewertung von Risiken, die den betroffenen Personen durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Ein Verstoss gegen diese Norm wird sanktioniert (vgl. Art. 50 Abs. 1 Bst. c und Art. 51 Abs. 1 Bst. d VE-DSG).

Die gesetzliche Umschreibung ist ausserordentlich vage *("voraussichtlich", "erhöht", "Risiko"*) und kann infolgedessen angesichts der aus einer Missachtung dieser Regelung resultierenden Folgen seitens der Daten verarbeitenden Person zu erheblichen Unsicherheiten führen. Auch der Erläuternde Bericht vom 21. Dezember 2016 legt sich nicht fest, was das *„erhöhte Risiko“* ist. In Verbindung mit der Regelung in Artikel 17 VE-DSG (Meldung von Verletzungen des Datenschutzes) führt diese Bestimmung zu einer drastischen Verschiebung der Schwelle zu einem inkriminierten Verhalten insbesondere auch zu Ungunsten kleinerer und mittlerer Betriebe bzw. bei einfachen Verhältnissen, wo wohl oft auch *"unbewusste"* Datenverarbeitungen in Unkenntnis der gesetzlichen Regelungen erfolgen (z.B. Onlineshop für Bastelartikel mit ausschliesslich Schweizer Kundschaft). Hier wird sehr oft ein die Strafbarkeit rechtfertigendes Unrechtsbewusstsein fehlen.

Die Regelung in Art. 16 Abs. 3 VE-DSG (Benachrichtigung des EDÖB über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen) geht zu weit. Es würde eine Konsultation bei erheblichen Restrisiken genügen. Die geplante Strafbarkeit für private Personen (Busse bis CHF 500‘000.-), wenn die Meldung unterlassen wird, ist nicht angemessen (vgl. Art. 51 Abs. 1 Bst. d VE-DSG).

Die Dreimonatsfrist für Einwände in Art. 16 Abs. 4 VE-DSG ist viel zu lang.

Wir beantragen, dass der Wortlaut von Art. 16 VE-DSG präzisiert und die unbestimmten Begriffe definiert werden sollen sowie die Reduktion der Frist für Einwände auf ein angemessenes Mass zu reduzieren ist.

10. Meldung von Verletzungen des Datenschutzes (Art. 17 VE-DSG)

Art. 17 VE-DSG ist eine neue Bestimmung. Sie verwirklicht (siehe Erläuternder Bericht zum Vorentwurf) die Anforderungen von Art. 7 Abs. 2 E-SEV 108 sowie von Artikel 30 der Richtlinien (EU) 2016/680. In Artikel 33 der Verordnung (EU) 2016/679 ist eine ähnliche Regelung enthalten. Jede Art der unbefugten Bearbeitung, auch die unbefugte Löschung, gilt als Verletzung des Datenschutzes. Die Meldung hat ab Kenntnisnahme unverzüglich zu erfolgen. Ein Verstoss gegen diese Meldepflicht wird sanktioniert (vgl. Art. 50 Abs. 2 Bst. d VE-DSG).

Die Übernahme einer solchen Bestimmung ist aufgrund von übergeordnetem Recht (E-SEV 108) erforderlich. Unternehmen werden somit entsprechende Verfahren schaffen müssen. Hier besteht aber der Fehlgedanke, dass der Datenschutz massgeblich verbessert wird, wenn die Unternehmen bei festgestellter Datenschutzverletzung eine staatliche Institution informieren müssen. Wichtig ist, dass man die Ausnahmebestimmung weit auslegt, also rasch annehmen darf, dass kein *„Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person“* besteht.

Gemäss dem Wortlaut von Art. 17 Abs. 1 VE-DSG hat der Verantwortliche die Meldung *„unverzüglich“* zu machen. Damit enthält die Bestimmung einen unbestimmten Begriff, der zu Verunsicherung führt. Damit besteht auch die Gefahr eines vorschnellen Handelns durch den Verantwortlichen. Nach Abs. 2 von Art. 17 muss der Verantwortliche die betroffene Person informieren, wenn es deren Schutz erfordert oder der EDÖB dies verlangt. Aufgrund der Systematik und dem Wortlaut muss damit zuerst die Meldung an den EDÖB gemacht und erst anschliessend der Betroffene informiert werden. Für die Unternehmen hat diese Meldepflicht einen sehr hohen administrativen und finanziellen Aufwand zur Folge. Für den Verantwortlichen, der diese Meldung machen muss, kommt diese einer zwingenden Selbstanzeige gleich. Unter Umständen muss er sich damit selbst belasten, was nicht angehen kann.

Wir beantragen die Herstellung der Äquivalenz zum EU-Recht. Konkret soll die Meldepflicht auf die Verletzung des Schutzes personenbezogener Daten eingegrenzt werden.

11. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 18 VE-DSG)

Diese neue Regelung soll die Anforderungen von Artikel 8 Ziff. 3 E-SEV 108 sowie von Artikel 20 Abs. 1 der Richtlinie (EU) 2016/680 verwirklichen. Auch in Artikel 25 der Verordnung (EU) 2016/679 ist eine ähnliche Bestimmung enthalten. In Abs. 1 geht es primär darum, Systeme zur Datenbearbeitung technisch und organisatorisch so auszugestalten, dass sie insbesondere den Grundsätzen nach Artikel 4 VE-DSG entsprechen. So kann beispielsweise dafür gesorgt werden, dass Daten in regelmässigen Abständen gelöscht oder standardmässig anonymisiert werden (siehe Erläuternder Bericht zum Vorentwurf). Abs. 2 führt neu die Pflicht zur Verwendung datenschutzfreundlicher Voreinstellungen (*Privacy by Default*) ein.

Zwar sind *Privacy by Default* und *Privacy by Design* stets gehörte Begriffe. Aber auch hier sind wir der Auffassung, dass diese für das CH-Recht nicht wirklich eine Neuerung bedeuten. Die geltenden Bearbeitungsgrundsätze sehen bereits entsprechende Pflichten vor. Hier haben wir nun aber eine Normierung, was den Fokus auf die Einhaltung erhöhen, weiteren Aufwand generieren und damit im Ergebnis zu einer massiv geringeren Datenverfügbarkeit führen wird. Dadurch würden die wirtschaftlichen Nutzungsmöglichkeiten stark eingeschränkt.

12. Weitere Pflichten (Art. 19 VE-DSG)

Wir regen an, zu Art. 19 Bst. b VE-DSG an geeigneter Stelle festzuhalten, dass an den Nachweis zum *„unverhältnismässigen Aufwand"* keine hohen Anforderungen gestellt werden.

13. Auskunftsrecht (Art. 20 VE-DSG)

Das Auskunftsrecht ergänzt die Informationspflicht des Verantwortlichen und bildet die zentrale Grundlage dafür, dass die betroffene Person ihre Rechte nach diesem Gesetz überhaupt wahrnehmen kann. Das Auskunftsrecht ist ein subjektives höchstpersönliches Recht. Ein Verstoss gegen diese Pflicht wird sanktioniert (vgl. Art. 50 Abs. 1 Bst. a VE-DSG).

Das alte Auskunftsrecht war bereits umfassend genug.

Falls doch an einer Änderung festgehalten werden soll, sollten diese Informationen nur auf Antrag der betroffenen Person mitgeteilt werden müssen. Zudem sollte in Absatz 3 das Wort *„Zustandekommen"* gestrichen werden, da dieser Vorgang in der Regel ein schützenswertes Geschäftsgeheimnis darstellt und für den Empfänger auch nicht sehr aufschlussreich sein dürfte.

Wir beantragen, den Umfang des geltenden Auskunftsrechts auch im VE-DSG beizubehalten.

14. Wegfall von Artikel 28 DSG (Beratung Privater) wäre ein Verlust

Falls diese Bestimmung vollständig wegfällt, ist es ein Verlust. Es bestand die Möglichkeit, informelle und pragmatische Auskünfte zu erhalten. Die im Erläuternden Bericht zum Vorentwurf zu Art. 43 Abs. 1 VE-DSG erwähnte Beratungsmöglichkeit muss daher unbedingt aufrechterhalten werden.

Es sei daher Art. 28 DSG auch im VE-DSG beizubehalten.

15. Sanktionen bei Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten (Art. 50 VE-DSG)

Bei den in Art. 50 ff. VE-DSG vorgesehenen Sanktionen handelt es sich um strafrechtliche Sanktionen, die sich direkt gegen die verantwortlichen natürlichen Personen richten. Der maximale Betrag der Busse, der heute gemäss Artikel 106 Abs. 1 StGB bei 10 000 Franken liegt, soll auf 500 000 Franken erhöht werden. Dies ist eine deutliche Verschärfung gegenüber der geltenden Regelung.

Gemäss unserer Beurteilung sanktioniert diese vorgeschlagene neue Regelung teilweise reine *"Ordnungsvorschriften"* mit teilweise völlig unverhältnismässig hohen Bussen, welche in keiner Relation zum möglichen Unrechtsgehalt der Daten verarbeitenden Person stehen.

Dem EDÖB soll keine Kompetenz eingeräumt werden, Verwaltungssanktionen zu sprechen. Um die Rechtmässigkeit und die Akzeptanz solcher Verfügungen sowie die Wahrung der Verfahrensrechte sicherzustellen, hätte die Organisation des EDÖB verändert werden müssen, beispielsweise analog zur Schweizerischen Wettbewerbskommission. Darauf wurde insbesondere mit Blick auf die Kosten verzichtet. Der Bundesrat erachtet es als vorteilhafter, Zuwiderhandlungen im Rahmen eines Strafverfahrens zu ahnden, welches die Garantien des Strafprozessrechts bietet (siehe Erläuternder Bericht vom 21. Dezember 2016). Auch die Empfehlungen EDÖB sollen (nach wie vor) keinen bindenden Charakter haben. Im Vergleich zum europäischen Ausland sind die Befugnisse des EDÖB somit nach wie vor sehr eingeschränkt, was dem Ansinnen, seine Funktion im Zuge der Revision des DSG zu stärken, entgegenspricht.

Zudem fehlt dem neuen Sanktionsregime eine klare Umschreibung der einschlägigen Tatbestände. Dies dürfte zu grosser Unsicherheit und letztendlich dazu führen, dass seitens der Verantwortlichen (i) aus Angst vor einer Sanktionierung mehr unternommen wird als notwendig (Overengineering), und dadurch (ii) die Informationsflut gegenüber den betroffenen Personen unverhältnismässig umfangreich wird, was dem Ziel der erhöhten Transparenz wohl eher zuwider laufen dürfte.

Es soll ausserdem eine starke *„Pönalisierung“* allfälliger (bewusster oder *„unbewusster“*, leichter oder grober) Verstösse gegen die gesetzlichen Regelungen erfolgen. Der Kreis der neuen (Straf-)Tatbestände wie auch die Höhe der mit diesen verbundenen Strafen ist in vielen Teilen unangemessen und unverhältnismässig sowie nicht zielführend. Bei der Festlegung des *„Pflichtenkatalogs“* der Daten verarbeitenden Person wird nicht bzw. unzureichend berücksichtigt, zu welchen Zwecken und in welchem örtlichen Rahmen Daten verarbeitet werden. Somit hat die Betreiberin eines kleinen *„Onlineshops“*, welche sich ausschliesslich an Kunden in der Schweiz richtet bzw. ihre Produkte ausschliesslich in der Schweiz absetzt, die gleichen (sehr umfassenden und mit Strafe sanktionierten) Regelungen zu beachten und einzuhalten wie ein grösseres Unternehmen, welches mit ihrer Tätigkeit erhebliche Umsätze erzielt oder grenzüberschreitend Handel betreibt. Die Aufwendungen zur Sicherstellung der Einhaltung der (datenschutz)rechtlichen Regelungen können jedoch aus finanziellen und personellen Mitteln bei kleineren und mittleren Unternehmen nicht in gleicher Weise geleistet werden wie in grösseren bzw. grossen Unternehmen.

Es wäre somit wünschenswert, wenn bei der Umschreibung des Pflichtenkatalogs (wie allenfalls auch der Sanktionen bei Pflichtwidrigkeiten) der Daten verarbeitenden Personen noch vermehrt der Situation kleinerer und mittlerer Betriebe Rechnung getragen würde. Wir erachten es bei eingeschränktem örtlichem Tätigkeitsbereich insbesondere auch nicht für zwingend notwendig, die sehr strengen Vorgaben des EU-Rechts *„tel quel“* zu übernehmen.

In Art. 50 Bst. e VE-DSG wird ein neues Unterlassungsdelikt vorgeschlagen. Es ist nicht klar, welche Personen wegen eines Verstosses gegen dieses Unterlassungsdelikt bestraft werden können sollten. Offen ist, welche Personen eine *"allgemeine Garantenstellung"* für die Pflicht zur Meldung von Verletzungen des DSG trifft. Diese Bestimmung, welche keinerlei sachliche und persönliche Einschränkungen enthält, setzt Unternehmen dem Risiko erpresserischer Handlungen bzw. Drohungen aus.

Sie dürfte letztlich auch geeignet sein, das Denunziantentum zu fördern, was schliesslich dem Ziel eines wirksamen und effizienten Datenschutzes wohl gar auch diametral entgegenlaufen wird. Auch die strafrechtliche Sanktionierung einer Missachtung einer Verfügung des EDÖB ist in der Schweizerischen Rechtsordnung grundsätzlich untypisch und schiesst über das Ziel hinaus.

Die Bestimmungen von Art. 50ff. VE-DSG sind nochmals einer kritischen Betrachtung zu unterziehen und maximal die Äquivalenz zum EU-Recht herzustellen.

16. Einwilligung von Kindern nicht geregelt

Ein weiterer, wichtiger Punkt stellt u.E. die **nicht geregelte Einwilligung von Kindern** dar.

In der DSGVO wurde das Mindestalter für die Abgabe einer rechtswirksamen Einwilligung in die Verarbeitung von personenbezogenen Daten von ursprünglich 13 Jahre auf 16 Jahre angehoben.
Die Einwilligung von Kindern ist zwar im Schweizer ZGB grundsätzlich geregelt, sollte jedoch auch im Schweizerischen Datenschutzgesetz geregelt sein.

Wir beantragen, die Einwilligung von Kindern im VE-DSG zu regeln.

Abschliessend möchten wir uns nochmals für die Möglichkeit bedanken, uns zur Revision des Datenschutzgesetzes vernehmen zu lassen.

Für Rückfragen oder ergänzende Auskünfte in diesem Zusammenhang stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

EXPERTsuisse

Dr. Lukas Imark
Präsident der Kommission für Rechtsfragen

lic. iur. Sergio Ceresola
Mitglied der Geschäftsleitung
Regulatorisches & Support

Stellungnahme von

Name / Firma / Organisation	: EXPERTsuisse – Schweizer Expertenverband für Wirtschaftsprüfung, Steuern und Treuhand
Abkürzung der Firma / Organisation	: EXPERTsuisse
Adresse	: Limmatquai 120, 8001 Zürich
Kontaktperson	: Dr. Lukas Imark (Präsident Kommission für Rechtsfragen) und/oder Sergio Ceresola (Regulatorisches & Dienste, Mitglied der Geschäftsleitung)
Telefon	: 058 792 20 30 (Dr. Lukas Imark) / 058 206 05 05 (Sergio Ceresola)
E-Mail	: lukas.imark@ch.pwc.com / sergio.ceresola@expertsuisse.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

Allgemeine Bemerkungen ____ 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ 5

Allgemeine Bemerkungen	
Name/Firma	**Bemerkung/Anregung**
EXPERTsuisse	Der Bundesrat hat das Eidg. Justiz- und Polizeidepartement (EJPD) am 21. Dezember 2016 beauftragt, bei den interessierten Kreisen zum Entwurf des Bundesgesetzes über den Datenschutz ein Vernehmlassungsverfahren durchzuführen. Gemäss der Medienmitteilung vom 21. Dezember 2016 will der Bundesrat primär die jüngsten Entwicklungen im Bereich des Datenschutzes in der EU und beim Europarat berücksichtigen sowie mit der Revision die Grundlage dafür schaffen, dass die Schweiz die Datenschutzkonvention des Europarates ratifizieren und die EU-Richtlinie über den Datenschutz im Bereich der Strafverfolgung übernehmen kann. Damit soll sichergestellt sein, dass die grenzüberschreitende Datenübermittlung weiterhin möglich bleibt. Zudem soll die Transparenz bei der Datenbearbeitung erhöht werden, Informationspflichten der Datenbearbeiter ausgeweitet, das Auskunftsrecht der betroffenen Personen präzisiert und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) mehr Kompetenzen verliehen werden. Überdies sollen die Strafbestimmungen verschärft werden. Gerne nehmen wir zum Vorentwurf Datenschutzgesetz (VE-DSG) wie folgt Stellung: Auch wir sind der Ansicht, dass das neue Datenschutzrecht der Schweiz den Vorgaben auf EU- und Europarats-Ebene möglichst entsprechen muss. In der VE-DSG sind nun aber verschiedene Regelungen enthalten, die über das Ziel hinausschiessen sowie für die in der Schweiz tätigen Unternehmen zu einem unnötigen administrativen und finanziellen Aufwand und – insbesondere für die international tätigen Unternehmen – zu einem Standortnachteil führen würden. Die Totalrevision des Datenschutzgesetzes in der Schweiz darf keinesfalls zur Folge haben, dass der Datentransfer bei grenzüberschreitenden Tätigkeiten der international tätigen Unternehmen erschwert wird. Für die in der Schweiz ansässigen Revisionsgesellschaften, die für einen international tätigen Konzern eine Konzernprüfung durchführen, muss die Zulieferung von Datenmaterial zwischen der Muttergesellschaft und einer Tochtergesellschaft ohne grosse Einschränkung und Aufwand möglich sein. Der Prüfer, der eine Teileinheit überprüft, ist auf diesen Datentransfer zwingend angewiesen. Es ist somit von grosser Wichtigkeit, dass die Möglichkeit, grenzüberschreitende Daten über verschiedene Kanäle auszutauschen, sichergestellt ist. Ferner ist zu erwarten, dass in ein paar Jahren ein massgebender Teil der Software in einer Cloud abgelegt sein wird. Der entsprechende Server würde dann in der Schweiz oder in der EU bzw. möglicherweise sogar einem Staat ausserhalb der EU liegen. Konzerne, die grenzüberschreitend tätig sind, würden ihre Daten in einer solchen Cloud ablegen. In der EU-Datenschutz-Grundverordnung (EU-DSGVO) findet sich der Begriff *„Unternehmensgruppe“* (=herrschende(s) Unternehmen und von diesem abhängige Unternehmen). Art. 47 der DSGVO enthält eine Art **Konzernprivileg,** wonach gruppeninterne

	Datenweitergaben zwischen verbundenen Unternehmen unter erleichterten Voraussetzungen erfolgen. Mittels gruppeninternen vertraglichen Regelungen kann der Mindestinhalt des angemessenen Datenschutzniveaus festgesetzt werden. Es ist im Interesse des Wirtschaftsstandortes Schweiz, sicherzustellen, dass die Äquivalenz zur EU-Regelung gegeben und der grenzüberschreitende Datentransfer mit dem VE-DSG gewährleistet ist. Mit Art. 52 VE-DSG soll der in Art. 321 StGB vorgesehene Schutz der beruflichen Schweigepflicht ausgebaut werden, da dieser durch die zunehmende Spezialisierung und die neuen Informationsbearbeitungsmethoden lückenhaft geworden sei (siehe Erläuternder Bericht). Gemäss Abs. 1 dieser Bestimmung wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (auf Antrag) bestraft, wer vorsätzlich geheime Daten bekannt gibt. Diese Bestimmung ist von überschiessender Tragweite. Es ist auch nicht wirklich eine Begründung für deren Notwendigkeit ersichtlich. Wohl ist klar, dass die erfolgreiche Ausübung der Berufe gemäss Art. 321 StGB ein besonderes Vertrauensverhältnis zum Klienten voraussetzt. Dementsprechend sind Verletzungen von Geheimhaltungspflichten zu sanktionieren. Alle anderen Berufe, bei welchen durchaus ein Geheimhaltungsbedürfnis besteht, sind aber nicht ohne weiteres gleichzusetzen mit den in Art. 321 StGB genannten. Datenschutzrechtlich ist insbesondere das Verhältnis zu Outsourcing-Konstellationen nicht genügend geklärt (gesetzliche und vertragliche Geheimhaltungspflichten verbieten ja ein Outsourcing ohne Einwilligung). Für unsere Mitglieder bzw. die gesamte Branche ist das Revisionsgeheimnis eine der wichtigsten Pflichten, die es strikte einzuhalten gilt. Gemäss Art. 730b Abs. 2 OR muss die Revisionsstelle sowohl das Geheimnis über ihre Feststellungen wahren, soweit sie nicht von Gesetzes wegen zur Bekanntgabe verpflichtet ist. Sie wahrt auch die Geschäftsgeheimnisse der Gesellschaft bei der Berichterstattung, der Erstattung von Anzeigen und bei der Auskunftserteilung an die Generalversammlung. Die spezialgesetzlichen Prüfgesellschaften haben noch andere Gesetzesnormen (z.B. Art. 129 Abs. 1 KAG: Prüfgeheimnis) zu beachten. Ferner sei auf das verbandsrechtliche Berufsgeheimnis hingewiesen (vgl. Standes- und Berufsregeln von EXPERTsuisse). Die Pflicht zur *„unverzüglichen“* Meldung an den EDÖB (Art. 17 VE-DSG) birgt das Risiko, dass aus Angst vor der strengen Strafandrohung in Art. 50 Abs. 2 Bst. d VE-DSG vorschnell Informationen an den EDÖB weitergeleitet werden und dabei (fahrlässig) ein Geschäftsgeheimnis/Berufsgeheimnis verletzt wird. Damit müssen die Unternehmen ihre Prozesse und Systeme deutlich ausbauen, was insbesondere für KMU einen unverhältnismässigen (finanziellen und organisatorischen) Aufwand zur Folge hätte. Im Übrigen gibt es verschiedene Umsetzungsprobleme der geplanten Regelungen in der Praxis. Zu erwähnen ist beispielsweise das Recht der Betroffenen auf Löschung ihrer Daten. Daten können nur in *„live“*-Systemen gelöscht werden. Daten in einem Backup sind allerdings nicht mit einem vernünftigen Aufwand löschbar. Wichtig ist auch, dass Innovationen und Entwicklungen in der digitalen Welt nicht durch das Datenschutzgesetz blockiert oder eingeschränkt werden sowie die Strategie des Bundesrates „Digitale Schweiz“ im Fokus behalten wird.

	Wir beantragen, dass diese Aspekte, insbesondere das Verhältnis zwischen Meldepflicht und Berufsgeheimnis nochmals einer genaueren Betrachtung zu unterziehen sind und bei der Totalrevision des DSG berücksichtigt werden.	

Zum Entwurf des Datenschutzgesetzes stellen wir im Einzelnen folgende Hauptanträge:

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
EXPERTsuisse	VE-DSG	2	1		Gemäss dem VE-DSG soll das Datenschutzgesetz auch auf bereits rechtshängige Zivilprozesse und laufende Strafverfahren Anwendung finden, was bei den Auskunftsrechten zu Missbräuchen führen kann. Damit wird die Beweisbeschaffung über die zivilprozessualen Editionsrechte ausgehebelt. Der Geltungsbereich darf in dieser Hinsicht keinesfalls erweitert werden. **Wir beantragen, dass der Geltungsbereich des VE-DSG nicht auf rechtshängige Zivilprozesse und laufende Strafverfahren erweitert wird.**
EXPERTsuisse	DSG	11a	5	Bst. e	Wie erwartet, orientiert sich der VE-DSG sehr an der EU-DSGVO und es wurden zahlreiche Bestimmungen auf sehr ähnliche Weise übernommen. Es erstaunt daher umso mehr, dass ein wichtiges Element der EU-DSGVO nicht übernommen wurde, nämlich das Institut des internen Datenschutzbeauftragten. Dieser ist im VE-DSG nicht mehr vorgesehen. Weder der, ebenfalls am 21. Dezember 2016 veröffentlichte Erläuternde Bericht, noch eine Stellungnahme des Eidgenössischen Datenschutzbeauftragten erklärt die Löschung des entsprechenden Artikels. Die ersatzlose Streichung ist umso erstaunlicher, weil es sich beim internen Datenschutzbeauftragten um ein Kernelement der EU-DSGVO handelt. Die Streichung führt zu Unsicherheiten und kann u.E. auch zu Problemen im Hinblick auf die Diskussion der Gleichwertigkeit des Schweizerischen Datenschutzes mit demjenigen der EU führen. Gerade im Hinblick darauf, dass eine grenzüberschreitende Datenübermittlung nach wie vor möglich ist, sollte diese Gleichwertigkeit mit dem aktuellen Vorentwurf angestrebt werden. Zumindest auf

					freiwilliger Basis sollten die Unternehmen einen internen Datenschutzbeauftragten einführen 1können und damit von der Meldepflicht im Sinne von Art. 17 VE-DSG an den EDÖB entbunden sein, was insbesondere für grosse Unternehmen, die aufgrund ihres Gesellschaftszweckes viele Daten bearbeiten müssen, eine grosse Erleichterung wäre. **Wir beantragen die Beibehaltung des betriebsinternen Datenschutzbeauftragten, zumindest auf freiwilliger Basis, und unter gleichzeitiger Entbindung von der Mitteilungspflicht im Sinne von Art. 17 VE-DSG.**
EXPERTsuissse	VE-DSG	3		Bst. d	Die Begriffe *"Speichern"* und *"Löschen"* sind unnötig und daher zu löschen. **Wir beantragen die Streichung der Begriffe *„Speichern“* und *„Löschen“.***
EXPERTsuissse	VE-DSG	3	Bst. c	Ziff. 3+4	Die Ausweitung des Begriffs *«besonders schützenswerte 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 des Übereinkommens zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (E-SEV 108). Nach der im VE-DSG vorgeschlagenen Definition wäre beispielsweise künftig jedes Gesichtsfoto als biometrisches Datum erfasst. Die Definition ist entsprechend einzuschränken. **Wir beantragen, die Definition von Art. 3 Bst. c Ziff. 3 und 4 VE-DSG einzuschränken.**
EXPERTsuisse	VE-DSG	3		Bst.f	Der Verzicht auf den Begriff *„Persönlichkeitsprofile“* im VE-DSG ist sehr sinnvoll, da dieser immer zu grossen Unsicherheiten geführt hat und er überdies auch im ausländischen Recht kein bekannter Begriff ist. Neu soll *„Profiling“* verwendet werden. Profiling ist *„jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität“.* Ein Profiling ist nur mit der ausdrücklichen Einwilligung der betroffenen Person zulässig. Wer diese Einwilligung nicht einholt, begeht eine widerrechtliche Persönlichkeitsverletzung (vgl. Art. 23 Abs. 2 Bst. d VE-DSG). Gemäss dem Erläuternden Bericht ist massgebend, dass Daten im Hinblick auf die Untersuchung zentraler Persönlichkeitsmerkmale ausgewertet werden. Die Auswertung der Daten kann automatisiert oder nicht-

					automatisiert erfolgen. Die Definition des Begriffs *„Profiling“* geht zu weit und auch weiter als die EU-DSGVO. Zukünftig wird beispielsweise jede schriftliche Qualifikation eines Mitarbeiters – ohne explizite Einwilligung des Betroffenen – als Persönlichkeitsverletzung betrachtet. Diese neue Bestimmung ist sehr heikel und nach unserem Dafürhalten ein unnötiges *„Swiss Finish“.* Profiling ist auf die automatisierte Bewertung von Personendaten zu beschränken. Ausserdem sind die Bedingungen zu reduzieren und anstatt einer Einwilligung lediglich eine Informationspflicht festzulegen. **Wir beantragen die Einschränkung des Profiling auf *„besonders schützenswerte Personendaten“* und auf die automatisierte Datenauswertung.**
EXPERTsuisse	VE-DSG	3		Bst. i	Die Bestimmung von Art. 3 Bst. i VE-DSG ist zu ungenau und kann zu Missverständnissen führen. **Wir beantragen daher folgende Präzisierung des Wortlautes: *"… im Rahmen eines Rechtsgeschäfts mit dem Verantwortlichen Personendaten bearbeitet, wobei das Vorliegen eines Arbeitsverhältnisses nicht als Rechtsgeschäft im Sinne dieser Regelung gilt".***
EXPERTsuisse	VE-DSG	7	3		Die Zustimmungspflicht im (neuen) Art. 7 Abs. 3 VE-DSG zum Sub-Outsourcing ist fragwürdig. Interessanterweise muss in der Systematik der *„Verantwortliche“* die betroffene Person in der Regel nicht um Zustimmung bitten, wenn er ihre Daten outsourct. Der Outsourcer muss dann aber den Verantwortlichen um Zustimmung bitten, wenn er sub-outsourct.
EXPERTsuisse	VE-DSG	8 + 9			Die Grundidee ist gut, es besteht allerdings das Risiko, dass sie in der Ausführung zu einer Verschärfung des DSG selbst führt. Es fehlen Kontrollmöglichkeiten und Rechtsschutzmechanismen. Auch aus Gründen der Gewaltentrennung sollte die Erstellung der Empfehlungen nicht durch den EDÖB selbst, sondern zwingend durch ein Fachgremium erfolgen. Nur durch den entsprechenden Praxisbezug können sachgerechte Lösungen erarbeitet werden. In der DSGVO wird die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen. **Wir beantragen somit, dass die Empfehlungen der guten Praxis durch ein breit abgestütztes Fachgremium, in welchem neben anderen auch die Wirtschaft vertreten wird, erlassen**

					werden, wobei der EDÖB über eine beratende Stimme verfügt.
EXPERTsuisse	VE-DSG	12			Im geltenden DSG ist Art. 12 VE-DSG ein Teilanspruch des Auskunftsrechts. Positiv zu vermerken ist, dass der VE-DSG eine Vorreiterrolle beim *„Persönlichkeitsschutz"* von verstorbenen Personen einnimmt. Art.12 VE-DSG regelt die datenschutzrechtlichen Gegebenheiten nach dem Tod einer Person. Interessanterweise berücksichtigt dies jedoch die EU-DSGVO nicht, obwohl es hierzu seit Jahren strittige Fälle gibt, z.B. die datenschutzrechtlichen Einstellungen von Facebook, wenn es um die Rechte der Angehörigen nach dem Tode eines Facebook Users geht. Gemäss dieser Regelung sind nebst den (gesetzlichen und eingesetzten) Erben weitere Personen auskunftsberechtigt. Das Auskunftsrecht geht über den Auskunftsanspruch der Erben hinaus, was unseres Erachtens zu weit geht. **Wir beantragen somit, dass das Auskunftsrecht entsprechend der erbrechtlichen Regelungen auf Erben beschränkt wird.**
EXPERTsuisse	VE-DSG	13	1		Nach Art. 13 Abs. 1 VE-DSG muss der Verantwortliche die betroffene Person über die Beschaffung von Personendaten informieren. Diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. Diese Bestimmung soll gemäss dem Erläuternden Bericht vom 21. Dezember 2016 die Transparenz bei der Datenbearbeitung verbessern, was eines der zentralen Ziele der Revision ist. Der Wortlaut der Bestimmung ist zu unklar und der Begriff *„Beschaffen"* wird nicht definiert, auch nicht in Art. 3 VE-DSG. Im Übrigen geht diese Bestimmung über die EU-DSGVO hinaus. Uns stellt sich insbesondere die Frage, ob ein Internet Research und die Verwertung der darin gefundenen Information zu einer Person bereits unter diese Bestimmung fällt und diese Person informiert werden müsste, was natürlich viel zu weit gehen würde. Die Bestimmung führt zu einer grossen Unsicherheit bei den Unternehmen, auch deshalb weil ein Verstoss sanktioniert wird (vgl. Art. 50 Abs. 1, Bst. a und b, Ziff. 1 und 2 VE-DSG). Im geltenden DSG besteht die Informationspflicht nur bei der Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen. Als wesentliche Änderung im VE-DSG soll diese Pflicht nun bei allen Daten gelten. Durch eine solche umfassende Informationspflicht würde nicht mehr Transparenz geschaffen, sondern es würde einfach zu einem Mehr an Information kommen, was letztlich der Transparenz zuwiderlaufen würde (kontraproduktive lnformationsüberflutung). Eine standardisierte Information in Form von AGB oder in einer generellen Datenschutzerklärung muss genügen. Alles andere ginge viel zu weit.

					Wir beantragen daher, dass der Wortlaut nochmals einer kritischen Betrachtung zu unterziehen sei und die Informationspflicht beschränkt wird auf „besonders schützenswerte Personendaten und Persönlichkeitsprofile“.
EXPERTsuisse	VE-DSG	15			Der Bundesrat erachtet die Einführung des neuen Begriffs *„automatisierte Einzelentscheidung“* für notwendig, weil diese Entscheidungen in allen Wirtschaftsbereichen immer häufiger und teilweise auf der Grundlage falscher Daten getroffen werden. Eine automatisierte Einzelentscheidung besteht, wenn ohne menschliches Dazutun eine Auswertung von Daten erfolgt, die zu einer konkreten Entscheidung gegenüber der betroffenen Person führt (siehe Erläuternder Bericht zum Vorentwurf). Dieses Thema ist eine Blackbox, da der Umfang der Informationspflicht unklar ist. Die Übernahme ist aufgrund des E-SEV 108 erforderlich, es wäre allerdings empfehlenswert, den Begriff der *"automatisierten Einzelentscheidung"* in Artikel 3 zu erläutern/definieren. Der völlig uneingeschränkte Äusserungsanspruch geht zudem sehr weit und kann insbesondere auch in kleinen und bescheidenen Verhältnissen zu einem unverhältnismässig und sachlich nicht gerechtfertigten hohen administrativen Aufwand führen. Die Informations- resp. Anhörungspflicht ist eine Einmischung in den zivilrechtlichen Willensbildungsvorgang einer Person bzw. eines Unternehmens. Ein Richtigkeitsgebot würde auch genügen. Auch mit einer allgemeinen Information könnte hier die notwendige Transparenz betreffend die automatisierte Einzelentscheidung erreicht werden, um das effektiv bestehende Bedürfnis nach dem Schutz gegen negative Entscheidfindung mittels falscher Daten zu befriedigen, ohne jedoch die Entwicklung der digitalen Wirtschaft und Gesellschaft übermässig zu behindern. **Wir beantragen, dass der Begriff *„automatisierte Einzelentscheidung“* in Art. 3 VE-DSG zu erläutern ist.**
EXPERTsuisse	VE-DSG	16			Die Datenschutz-Folgenabschätzung ist eine neue Pflicht im VE-DSG, womit die Anforderungen von Art. 8^{bis} Abs. 2 E-SEV 108 sowie die Artikel 27f. der Richtlinie (EU) 2016/680 verwirklicht werden sollen. In der Verordnung (EU) 2016/679 ist eine ähnliche Vorschrift enthalten. Die Datenschutz-Folgenabschätzung soll ein Instrument sein zur Erkennung und Bewertung von Risiken, die den betroffenen Personen durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Ein Verstoss gegen diese Norm wird sanktioniert (vgl. Art. 50 Abs. 1 Bst. c und Art. 51 Abs. 1 Bst. d VE-DSG). Die gesetzliche Umschreibung ist ausserordentlich vage *("voraussichtlich", "erhöht", "Risiko"*) und kann

					infolgedessen angesichts der aus einer Missachtung dieser Regelung resultierenden Folgen seitens der Daten verarbeitenden Person zu erheblichen Unsicherheiten führen. Auch der Erläuternde Bericht vom 21. Dezember 2016 legt sich nicht fest, was das *„erhöhte Risiko"* ist. In Verbindung mit der Regelung in Artikel 17 VE-DSG (Meldung von Verletzungen des Datenschutzes) führt diese Bestimmung zu einer drastischen Verschiebung der Schwelle zu einem inkriminierten Verhalten insbesondere auch zu Ungunsten kleinerer und mittlerer Betriebe bzw. bei einfachen Verhältnissen, wo wohl oft auch *"unbewusste"* Datenverarbeitungen in Unkenntnis der gesetzlichen Regelungen erfolgen (z.B. Onlineshop für Bastelartikel mit ausschliesslich Schweizer Kundschaft). Hier wird sehr oft ein die Strafbarkeit rechtfertigendes Unrechtsbewusstsein fehlen. Die Regelung in Art. 16 Abs. 3 VE-DSG (Benachrichtigung des EDÖB über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen) geht zu weit. Es würde eine Konsultation bei erheblichen Restrisiken genügen. Die geplante Strafbarkeit für private Personen (Busse bis CHF 500'000.-), wenn die Meldung unterlassen wird, ist nicht angemessen (vgl. Art. 51 Abs. 1 Bst. d VE-DSG). Die Dreimonatsfrist für Einwände in Art. 16 Abs. 4 VE-DSG ist viel zu lang. **Wir beantragen, dass der Wortlaut von Art. 16 VE-DSG präzisiert und die unbestimmten Begriffe definiert werden sollen sowie die Reduktion der Frist für Einwände auf ein angemessenes Mass zu reduzieren ist.**
EXPERTsuisse	VE-DSG	17			Art. 17 VE-DSG ist eine neue Bestimmung. Sie verwirklicht (siehe Erläuternder Bericht zum Vorentwurf) die Anforderungen von Art. 7 Abs. 2 E-SEV 108 sowie von Artikel 30 der Richtlinien (EU) 2016/680. In Artikel 33 der Verordnung (EU) 2016/679 ist eine ähnliche Regelung enthalten. Jede Art der unbefugten Bearbeitung, auch die unbefugte Löschung, gilt als Verletzung des Datenschutzes. Die Meldung hat ab Kenntnisnahme unverzüglich zu erfolgen. Ein Verstoss gegen diese Meldepflicht wird sanktioniert (vgl. Art. 50 Abs. 2 Bst. d VE-DSG). Die Übernahme einer solchen Bestimmung ist aufgrund von übergeordnetem Recht (E-SEV 108) erforderlich. Unternehmen werden somit entsprechende Verfahren schaffen müssen. Hier besteht aber der Fehlgedanke, dass der Datenschutz massgeblich verbessert wird, wenn die Unternehmen bei festgestellter Datenschutzverletzung eine staatliche Institution informieren müssen. Wichtig ist, dass man die Ausnahmebestimmung weit auslegt, also rasch annehmen darf, dass kein *„Risiko für die Persönlichkeit und*

					die Grundrechte der betroffenen Person" besteht. Gemäss dem Wortlaut von Art. 17 Abs. 1 VE-DSG hat der Verantwortliche die Meldung *„unverzüglich"* zu machen. Damit enthält die Bestimmung einen unbestimmten Begriff, der zu Verunsicherung führt. Damit besteht auch die Gefahr eines vorschnellen Handelns durch den Verantwortlichen. Nach Abs. 2 von Art. 17 muss der Verantwortliche die betroffene Person informieren, wenn es deren Schutz erfordert oder der EDÖB dies verlangt. Aufgrund der Systematik und dem Wortlaut muss damit zuerst die Meldung an den EDÖB gemacht und erst anschliessend der Betroffene informiert werden. Für die Unternehmen hat diese Meldepflicht einen sehr hohen administrativen und finanziellen Aufwand zur Folge. Für den Verantwortlichen, der diese Meldung machen muss, kommt diese einer zwingenden Selbstanzeige gleich. Unter Umständen muss er sich damit selbst belasten, was nicht angehen kann. **Wir beantragen die Herstellung der Äquivalenz zum EU-Recht. Konkret soll die Meldepflicht auf die Verletzung des Schutzes personenbezogener Daten eingegrenzt werden.**
EXPERTsuisse	VE-DSG	18			Diese neue Regelung soll die Anforderungen von Artikel 8 Ziff. 3 E-SEV 108 sowie von Artikel 20 Abs. 1 der Richtlinie (EU) 2016/680 verwirklichen. Auch in Artikel 25 der Verordnung (EU) 2016/679 ist eine ähnliche Bestimmung enthalten. In Abs. 1 geht es primär darum, Systeme zur Datenbearbeitung technisch und organisatorisch so auszugestalten, dass sie insbesondere den Grundsätzen nach Artikel 4 VE-DSG entsprechen. So kann beispielsweise dafür gesorgt werden, dass Daten in regelmässigen Abständen gelöscht oder standardmässig anonymisiert werden (siehe Erläuternder Bericht zum Vorentwurf). Abs. 2 führt neu die Pflicht zur Verwendung datenschutzfreundlicher Voreinstellungen (*Privacy by Default*) ein. Zwar sind *Privacy by Default* und *Privacy by Design* stets gehörte Begriffe. Aber auch hier sind wir der Auffassung, dass diese für das CH-Recht nicht wirklich eine Neuerung bedeuten. Die geltenden Bearbeitungsgrundsätze sehen bereits entsprechende Pflichten vor. Hier haben wir nun aber eine Normierung, was den Fokus auf die Einhaltung erhöhen, weiteren Aufwand generieren und damit im Ergebnis zu einer massiv geringeren Datenverfügbarkeit führen wird. Dadurch würden die wirtschaftlichen Nutzungsmöglichkeiten stark eingeschränkt.
EXPERTsuisse	VE-DSG	19		Bst. b	Wir regen an, zu Art. 19 Bst. b VE-DSG an geeigneter Stelle festzuhalten, dass an den Nachweis zum *„unverhältnismässigen Aufwand"* keine hohen Anforderungen gestellt werden.

EXPERTsuisse	VE-DSG	20			Das Auskunftsrecht ergänzt die Informationspflicht des Verantwortlichen und bildet die zentrale Grundlage dafür, dass die betroffene Person ihre Rechte nach diesem Gesetz überhaupt wahrnehmen kann. Das Auskunftsrecht ist ein subjektives höchstpersönliches Recht. Ein Verstoss gegen diese Pflicht wird sanktioniert (vgl. Art. 50 Abs. 1 Bst. a VE-DSG). Das alte Auskunftsrecht war bereits umfassend genug. Falls doch an einer Änderung festgehalten werden soll, sollten diese Informationen nur auf Antrag der betroffenen Person mitgeteilt werden müssen. Zudem sollte in Absatz 3 das Wort *„Zustandekommen"* gestrichen werden, da dieser Vorgang in der Regel ein schützenswertes Geschäftsgeheimnis darstellt und für den Empfänger auch nicht sehr aufschlussreich sein dürfte. **Wir beantragen, den Umfang des geltenden Auskunftsrechts auch im VE-DSG beizubehalten.**
EXPERTsuisse	DSG	28			Falls diese Bestimmung vollständig wegfällt, ist es ein Verlust. Es bestand die Möglichkeit, informelle und pragmatische Auskünfte zu erhalten. Die im Erläuternden Bericht zum Vorentwurf zu Art. 43 Abs. 1 VE-DSG erwähnte Beratungsmöglichkeit muss daher unbedingt aufrechterhalten werden. **Es sei daher Art. 28 DSG auch im VE-DSG beizubehalten.**
EXPERTsuisse	VE-DSG	50ff.			Bei den in Art. 50 ff. VE-DSG vorgesehenen Sanktionen handelt es sich um strafrechtliche Sanktionen, die sich direkt gegen die verantwortlichen natürlichen Personen richten. Der maximale Betrag der Busse, der heute gemäss Artikel 106 Abs. 1 StGB bei 10 000 Franken liegt, soll auf 500 000 Franken erhöht werden. Dies ist eine deutliche Verschärfung gegenüber der geltenden Regelung. Gemäss unserer Beurteilung sanktioniert diese vorgeschlagene neue Regelung teilweise reine *"Ordnungsvorschriften"* mit teilweise völlig unverhältnismässig hohen Bussen, welche in keiner Relation zum möglichen Unrechtsgehalt der Daten verarbeitenden Person stehen. Dem EDÖB soll keine Kompetenz eingeräumt werden, Verwaltungssanktionen zu sprechen. Um die Rechtmässigkeit und die Akzeptanz solcher Verfügungen sowie die Wahrung der Verfahrensrechte sicherzustellen, hätte die Organisation des EDÖB verändert werden müssen, beispielsweise analog zur Schweizerischen Wettbewerbskommission. Darauf wurde insbesondere mit Blick auf die Kosten verzichtet.

					Der Bundesrat erachtet es als vorteilhafter, Zuwiderhandlungen im Rahmen eines Strafverfahrens zu ahnden, welches die Garantien des Strafprozessrechts bietet (siehe Erläuternder Bericht vom 21. Dezember 2016). Auch die Empfehlungen EDÖB sollen (nach wie vor) keinen bindenden Charakter haben. Im Vergleich zum europäischen Ausland sind die Befugnisse des EDÖB somit nach wie vor sehr eingeschränkt, was dem Ansinnen, seine Funktion im Zuge der Revision des DSG zu stärken, entgegenspricht. Zudem fehlt dem neuen Sanktionsregime eine klare Umschreibung der einschlägigen Tatbestände. Dies dürfte zu grosser Unsicherheit und letztendlich dazu führen, dass seitens der Verantwortlichen (i) aus Angst vor einer Sanktionierung mehr unternommen wird als notwendig (Overengineering), und dadurch (ii) die Informationsflut gegenüber den betroffenen Personen unverhältnismässig umfangreich wird, was dem Ziel der erhöhten Transparenz wohl eher zuwider laufen dürfte. Es soll ausserdem eine starke *„Pönalisierung“* allfälliger (bewusster oder *„unbewusster“*, leichter oder grober) Verstösse gegen die gesetzlichen Regelungen erfolgen. Der Kreis der neuen (Straf-)Tatbestände wie auch die Höhe der mit diesen verbundenen Strafen ist in vielen Teilen unangemessen und unverhältnismässig sowie nicht zielführend. Bei der Festlegung des *„Pflichtenkatalogs“* der Daten verarbeitenden Person wird nicht bzw. unzureichend berücksichtigt, zu welchen Zwecken und in welchem örtlichen Rahmen Daten verarbeitet werden. Somit hat die Betreiberin eines kleinen *„Onlineshops“*, welche sich ausschliesslich an Kunden in der Schweiz richtet bzw. ihre Produkte ausschliesslich in der Schweiz absetzt, die gleichen (sehr umfassenden und mit Strafe sanktionierten) Regelungen zu beachten und einzuhalten wie ein grösseres Unternehmen, welches mit ihrer Tätigkeit erhebliche Umsätze erzielt oder grenzüberschreitend Handel betreibt. Die Aufwendungen zur Sicherstellung der Einhaltung der (datenschutz)rechtlichen Regelungen können jedoch aus finanziellen und personellen Mitteln bei kleineren und mittleren Unternehmen nicht in gleicher Weise geleistet werden wie in grösseren bzw. grossen Unternehmen. Es wäre somit wünschenswert, wenn bei der Umschreibung des Pflichtenkatalogs (wie allenfalls auch der Sanktionen bei Pflichtwidrigkeiten) der Daten verarbeitenden Personen noch vermehrt der Situation kleinerer und mittlerer Betriebe Rechnung getragen würde. Wir erachten es bei eingeschränktem örtlichem Tätigkeitsbereich insbesondere auch nicht für zwingend notwendig, die sehr strengen Vorgaben des EU-Rechts *„tel quel“* zu übernehmen. In Art. 50 Bst. e VE-DSG wird ein neues Unterlassungsdelikt vorgeschlagen. Es ist nicht klar, welche Personen

					wegen eines Verstosses gegen dieses Unterlassungsdelikt bestraft werden können sollten. Offen ist, welche Personen eine *"allgemeine Garantenstellung"* für die Pflicht zur Meldung von Verletzungen des DSG trifft. Diese Bestimmung, welche keinerlei sachliche und persönliche Einschränkungen enthält, setzt Unternehmen dem Risiko erpresserischer Handlungen bzw. Drohungen aus. Sie dürfte letztlich auch geeignet sein, das Denunziantentum zu fördern, was schliesslich dem Ziel eines wirksamen und effizienten Datenschutzes wohl gar auch diametral entgegenlaufen wird. Auch die strafrechtliche Sanktionierung einer Missachtung einer Verfügung des EDÖB ist in der Schweizerischen Rechtsordnung grundsätzlich untypisch und schiesst über das Ziel hinaus. **Die Bestimmungen von Art. 50ff. VE-DSG sind nochmals einer kritischen Betrachtung zu unterziehen und maximal die Äquivalenz zum EU-Recht herzustellen.**
EXPERTsuisse					Ein weiterer, wichtiger Punkt stellt u.E. die **nicht geregelte Einwilligung von Kindern** dar. In der DSGVO wurde das Mindestalter für die Abgabe einer rechtswirksamen Einwilligung in die Verarbeitung von personenbezogenen Daten von ursprünglich 13 Jahre auf 16 Jahre angehoben. Die Einwilligung von Kindern ist zwar im Schweizer ZGB grundsätzlich geregelt, sollte jedoch auch im Schweizerischen Datenschutzgesetz geregelt sein. **Wir beantragen, die Einwilligung von Kindern im VE-DSG zu regeln.**

Abschliessend möchten wir uns nochmals für die Möglichkeit bedanken, uns zur Revision des Datenschutzgesetzes vernehmen zu lassen.

Für Rückfragen oder ergänzende Auskünfte in diesem Zusammenhang stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

EXPERTsuisse

Amstutz Jonas BJ

Von: Philippe Meier <Philippe.Meier@unil.ch>
Gesendet: Freitag, 24. März 2017 14:31
An: Amstutz Jonas BJ
Betreff: Consultation LPD
Anlagen: Consultation UNIL FDCA LPD(240317).doc

Cher Monsieur,

Dans le délai imparti, je me permets de vous adresser ci-joint la prise de position de la Faculté de droit, des sciences criminelles et d'administration publique de l'Université de Lausanne au sujet de l'avant-projet de révision de la LPD.

En vous remerciant par avance de l'attention que vous lui accorderez, je vous prie de croire, cher Monsieur, à mes sentiments les meilleurs.

Philippe Meier

Docteur en droit, avocat - Professeur ordinaire
Directeur de l'Ecole de Droit, Vice-doyen
Faculté de droit, des sciences criminelles et d'administration publique
Centre de droit privé
Université de Lausanne - Bâtiment Internef
1015 Lausanne-Dorigny (Suisse)
e-mail: philippe.meier@unil.ch

Avis donné par

Nom / société / organisation	: Faculté de droit, des sciences criminelles et d'administration publique, Uni Lausanne
Abréviation de la société / de l'organisation	: FDCA/UNIL
Adresse	: Centre de droit privé / Bâtiment Internef / Bureau 445 / 1015 Lausanne-Dorigny
Personne de référence	: Prof. Dr Philippe Meier, av.
Téléphone	: 021 692 28 38
Courriel	: philippe.meier@unil.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!

Table des matières

Remarques générales 3

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 4

Remarques générales	
nom/société	**remarque / suggestion :**
FDCA/UNIL	La FDCA/UNIL salue la révision générale de la LPD pour assurer une compatibilité de la législation suisse avec la nouvelle réglementation européenne ainsi qu'avec les travaux de révision de la Convention 108. Elle se limitera ici à prendre position sur l'avant-projet de révision de la LPD, ainsi que sur certaines dispositions annexes (CPC, CP).
FDCA/UNIL	De manière générale, la révision tient compte des défis posés par l'évolution technologique et sociétale. Il est heureux que le principe de neutralité technologique de la loi ait été maintenu, pour permettre une adaptation en continu aux nombreux développements encore à venir. Le système des principes généraux, dans un domaine aussi évolutif que celui de la protection des données, a par ailleurs fait ses preuves. Le lien, en matière privée, avec le mécanisme législatif de l'art. 28 CC (illicéité en cas d'atteinte à la personnalité mais levée possible moyennant des motifs justificatifs), avec un certain nombre de précisions, a été maintenu, ce qui doit aussi être salué.
FDCA/UNIL	La FDCA/UNIL exprime néanmoins six regrets (qu'elle aura l'occasion de reprendre dans le commentaire de certaines dispositions individuelles) : 1) le manque d'ambition dans la réflexion qui a accompagné l'élaboration de l'avant-projet. Les travaux du groupe d'accompagnement puis des experts internes sont très largement partis de l'existant, soit d'une conception de la protection des données remontant aux années 70/80. Il est vrai que la nouvelle réglementation européenne en fait de même. Les limites de cette conception (notamment l'importance donnée au couple „notice" and „consent") ont cependant été très clairement identifiées depuis longtemps déjà, notamment dans le cadre de Big Data. Ces débats ne ressortent ni du rapport, ni de l'avant-projet. Le timing est aussi malheureux puisque le programme FNS Big Data est précisément en cours. 2) Sur un certain nombre de points, l'avant-projet va plus loin que les exigences européennes, sans explication particulière. Il serait dommage, en termes économiques, de soumettre les entreprises actives en Suisse à des contraintes plus élevées que leurs homologues européennes, sauf si le besoin s'en fait impérativement ressentir. 3) Certains points qui paraissaient acquis pour la très grande majorité, si ce n'est pour la totalité de la doctrine et des praticiens (tout particulièrement le renforcement de l'arsenal administratif à disposition du préposé) ont passé à la trappe sans raison objective autre qu'un souci budgétaire s'agissant des ressources de l'autorité de contrôle. 4) L'avant-projet ne revient pas du tout sur la question de l'éclatement de la protection des données dans le domaine public ; une harmonisation nécessiterait naturellement une révision de la Constitution fédérale, mais il eût été souhaitable que l'avant-projet puis le Conseil fédéral s'expriment expressément sur ce point et fassent peut-être des propositions alternatives. 5) Même si la prochaine entrée en vigueur du Règlement européen est l'un des moteurs de la révision, on ne trouve pas trace dans le Rapport de la manière dont les deux législations seront mises en œuvre en parallèle (risque pour une entreprise suisse active dans l'Union d'être soumise aux

	règles matérielles des deux ordres juridiques, mais surtout à tous les devoirs liés à la surveillance par l'autorité de contrôle tant dans l'Union qu'en Suisse). 6) La protection des mineurs n'est assurée que très marginalement, à l'art. 24 al. 2 lit. c. On regrette l'absence de réflexion globale sur cette 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

nom/société	loi	art.	al.	let.	remarque / suggestion :
FDCA/UNIL	LPD	1			-
FDCA/UNIL	LPD	2	1	a	L'exclusion des données des personnes morales peut se comprendre en termes d'harmonisation internationale. Elle présente des avantages aussi par rapport aux normes à respecter pour la communication transfrontière. Il ne faut toutefois pas exagérer les effets de cette modification, la protection via les art. 53 et 28 ss CC demeurant garantie. Même une forme de droit d'accès aux données pourrait être fondée sur ces dispositions (soit comme prétention matérielle, soit comme mesure de nature procédurale), sans passer par le droit d'accès LPD.
FDCA/UNIL	LPD	2	2		L'intégration de toutes les procédures dans le champ d'application de la LPD accentue le risque d'abus du droit d'accès. Il faut d'autant plus veiller à donner un cadre strict à ce droit dans les dispositions le concernant spécifiquement.
FDCA/UNIL	LPD	2	3/4		La question de la surveillance ne relève pas du champ d'application au sens ordinaire de l'expression. Les règles spéciales pour les tribunaux devraient figurer aux art. 26 ss. On peut se demander pourquoi les autorités judiciaires indépendantes sont soumises à la surveillance du PFPDT alors que les tribunaux ne le sont pas (les raisons invoquées par le rapport leur seraient pourtant aussi applicables).
FDCA/UNIL	LPD	3			La FDCA/UNIL salue les modifications intervenues dans les définitions et estime que les explications données dans le rapport sont convaincantes. Il en va de même de la terminologie (responsable de

					traitement, sous-traitant). Il est certes dommage d'abandonner une notion finalement aussi pionnière que l'était le profil de la personnalité (malgré ses difficultés d'application, notamment compte tenu de son caractère évolutif : une somme de données se transformant „soudain" en un profil), mais le maintien de cette notion en parallèle à la notion de profilage du droit européen serait source de confusion. Dans la mesure où la LPD s'applique à toute forme de traitement, il ne serait pas opportun de limiter le profilage aux opérations automatisées même si le droit de l'Union apporte cette restriction. En revanche, on comprend mal pourquoi l'utilisation de données non personnelles doit être mentionnée ici, alors que le Règlement européen ne le fait pas. Tant les données utilisées que le résultat doivent constituer une donnée personnelle. Cela dit, vu le caractère très large de la notion même de donnée personnelle, on conçoit mal une opération de profilage basée sur des données non personnelles qui aboutirait à des données personnelles par profilage. Les suppressions apportées dans les définitions sont justifiées (le droit d'accès s'en trouve élargi à toute donnée personnelle, même ne figurant pas dans un fichier, mais le droit général de la personnalité permettait déjà de fonder un tel droit via l'art. 28 CC). Le sort des données pseudonymisées fait l'objet d'interprétations divergentes dans la pratique. Il serait peut-être bon que le projet prévoie une règle précisant les conditions auxquelles ces données, en soi toujours personnelles, pourraient échapper à la loi si elles correspondent à une anonymisation de facto (en reprenant tout ou partie des critères développées par la jurisprudence et la doctrine).
FDCA/UNIL	LPD	4	1-4		Les modifications apportées sont convaincantes. La reconnaissabilité se limite certes aux finalités, mais la transparence de la collecte comme telle découle déjà de la bonne foi (comme sous l'empire du texte originel de la loi) et est désormais consacrée par le devoir d'information de l'art. 13. L'extension aux finalités non incompatibles est justifiée ; il est heureux que le texte ne reprenne pas les précisions de l'art. 6 par. 4 du Règlement (exprimées de façon très complexe), même si certains de ces éléments pourront être utilisés pour l'interprétation. L'al. 4 est particulièrement justifié compte tenu de l'importance du principe de proportionnalité temporelle, notamment sous l'angle de Big Data.
FDCA/UNIL **Fehler! Verweisquelle konnte nicht**	LPD	4	5		La dernière phrase de l'article est curieuse : sur le plan formel (rédaction inhabituelle) et sur le plan matériel. S'il l'on veut dire que les données inexactes doivent être détruites si une rectification ou un complément ne sont pas possibles, il faut le dire ainsi !

gefunden werden.					
FDCA/UNIL	LPD	4	6		La nouvelle formulation met fin aux controverses doctrinales sur le consentement en cas de traitement de données sensibles. Selon la position que l'on soutenait sous le droit actuel, les exigences nouvelles peuvent paraître plus élevées que sous l'empire de la LPD. Mais la nature particulière des données en cause le justifie. Le consentement doit être exprès par rapport au traitement de données lui-même (pas par rapport à l'opération qui pourrait éventuellement donner lieu à un traitement de données). A noter qu'une absence de déclaration peut aussi être un consentement exprès lorsqu'elle qualifiée comme telle entre les parties („si vous ne dites rien, vous consentez").
FDCA/UNIL	LPD	5	1		Le lien entre la menace grave pour la personnalité et le cas du niveau de protection insuffisant est perdu à l'al. 1. L'art. 6 al. 1 doit par conséquent déroger aux al. 2 et 3 de l'art. 5, mais pas à l'al. 1, cas dans lequel la communication est toujours interdite (la balance d'intérêts intervenant dans l'examen du caractère grave de la menace). Notre compréhension est ici différente de celle de D. Rosenthal (Jusletter 20.02.2017, § 37).
FDCA/UNIL	LPD	5	2		L'al. 2 donne à la liste de pays la valeur juridique qui correspond à sa valeur en fait. Il s'agit ici d'un allègement pour le responsable du traitement, qui peut se fier au travail effectué en amont par les autorités spécialisées. C'est un point à saluer.
FDCA/UNIL	LPD	5	3		Si les garanties standardisées doivent être élaborées ou approuvées par le PFPDT puisqu'elles sont précisément destinées à être appliquées de manière générale par un grand nombre de responsables de traitement, il ne saurait en aller de même des BCR, dont seule une *communication* devrait être prévue, comme à l'heure actuelle (art. 6 al. 3 LPD). Il est douteux que la législation suisse puisse être jugée non conforme parce qu'elle irait moins loin que l''art. 57 par. 1 lit s du Règlement. Quant aux garanties spécifiques, elles relèvent à la fois du secret d'affaires et de la responsabilité du responsable de traitement ; elles ne doivent elles aussi qu'être que communiquées (et uniquement sur les points relatifs au transfert à l'étranger). A noter que l'art. 12 al. 5 de la Convention 108 révisée n'exige pas d'approbation, mais une communication (qui n'a pas besoin d'être automatique et spontanée, mais pourrait intervenir sur demande du PFPDT) (cf. aussi art. 12bis al. 2 lit. b de cette même Convention).
FDCA/UNIL	LPD	5	4-6		Les mécanismes doivent être adaptés aux modifications apportées à l'al. 3. A noter que le maintien

					des obligations de l'al. 3 est d'autant moins justifié que les services du PPFPDT seront vite débordés par les demandes, qu'il est préférable qu'ils consacrent leur énergie et leurs ressources à la poursuite des violations importantes et que les délais prévus pour l'approbation (six mois dès que le dossier est jugé complet !!!) sont parfaitement irréalistes pour la pratique.
FDCA/UNIL	LPD	5	7		Fait double emploi avec l'al. 2 ou devrait y être intégré (les modalités relèvent en réalité de l'Ordonnance).
FDCA/UNIL	LPD	6	1		Les modifications apportées à la lit. c et à la lit. f doivent être saluées. Même si la formulation actuelle permet à notre sens d'englober les procédures de nature administrative, la question a donné lieu à beaucoup de controverses dans le cadre de l'affaire des employés de banque/USA. Le texte légal lèvera désormais tout doute.
FDCA/UNIL	LPD	6	2		Pour les raisons juridiques (secret des affaires, responsabilité devant être laissée aux responsables de traitement) et pratiques (surcharge du PFPDT avec des tâches inutiles) déjà exposées en lien avec l'art. 5, l'al. 2 doit être supprimé. On notera ici, mais cela vaut aussi pour l'art. 5, que l'extension des compétences du PFPDT en matière de communication transfrontière ne répond pas aux explications du Rapport (p. 104) selon lequel l'intervention de l'Etat serait „limitée au strict nécessaire, l'idée étant de responsabiliser les auteurs de traitements". Pourtant, cet objectif est correct. Chaque disposition nouvelle proposée devrait être lue en gardant cet objectif à l'esprit !
FDCA/UNIL	LPD	7			La précision de l'al. 3, conforme à la réglementation européenne et à l'avis de la doctrine majoritaire en droit actuel déjà, est à saluer. L'al. 2 in fine est en revanche curieux : la responsabilité du respect des droits de la personne concernée incombe au responsable de traitement à l'endroit duquel ils sont exercés. Quant à l'Ordonnance du Conseil fédéral, dont on peut douter de l'utilité (mais l'inspiration européenne est manifeste), elle devrait se limiter aux questions relatives à la protection des données dans la sous-traitance, et ne pas s'étendre aux obligations du sous-traitant en général. La base légale serait de toute manière insuffisante pour une telle délégation, qui reviendrait à permettre au Conseil fédéral de modifier le droit du contrat de mandat ou du contrat d'entreprise.
FDCA/UNIL	LPD	8			Le système des bonnes pratiques est une manière souple et pragmatique de s'adapter aux besoins de chaque branche d'activité, respectivement aux différentes problématiques de protection des données,

					et de concrétiser les principes généraux autour de laquelle la loi s'articule. Il est également sain de prévoir une compétence concurrente du PFPDT (dont on imagine volontiers qu'il ne disposera pas toujours des ressources nécessaires pour procéder à ce travail) et des milieux intéressés.
FDCA/UNIL	LPD	9			La formulation de la disposition n'est pas adéquate. Mais sur le fond (fiction), une telle disposition ne paraît de toute façon pas nécessaire ni opportune. Il appartient en réalité au PFPDT, respectivement au juge civil ou pénal saisi d'un contentieux, d'apprécier la portée des bonnes pratiques et de leur respect. Il n'en demeure pas moins que celles-ci joueront leur rôle de clarification même sans leur conférer cette curieuse autorité (étant relevé qu'elles ne sont apparemment pas sujettes à recours ni à aucun contrôle étatique), comme le faisaient jusqu'à présent les recommandations du PFPDT. Par définition, ces bonnes pratiques auraient d'ailleurs un caractère beaucoup trop général pour valoir fiction de respect de la protection des données dans chaque cas concret. La marge d'appréciation laissée aux autorités d'application leur permettra aussi de tenir compte de la manière dont le PFPDT – lorsque c'est lui qui adopte les bonnes pratiques – a intégré les préoccupations de la branche. Le PFPDT ne saurait se voir confier ici un rôle quasi législatif.
FDCA/UNIL	LPD	10			Compte tenu des nombreuses tâches nouvelles attribuées au PFPDT, on peut s'étonner que la certification n'y figure pas et que l'on conserve le système des organismes agréés. Mais la solution est probablement raisonnable, faute de quoi les services du Préposé devraient être encore élargis pour cette raison, avec en outre un risque de conflit d'intérêts (celui qui a certifié ne peut plus guère contrôler ensuite). La formule „opérations de traitement" est très vague et laisse entendre qu'une certification individuelle d'opérations individuelles serait possible, ce qui ne paraît pas souhaitable. La terminologie de l'art. 11 al. 1 LPD avec la notion de „système de traitement de données" est meilleure. On peut se demander si la terminologie du Règlement (art. 42 al. 2) doit ici impérativement être reprise. Si la certification est mentionnée, le conseiller indépendant à la protection des données disparaît quant à lui, puisque l'obligation de déclaration des fichiers et les exceptions à cette déclaration, dont l'art. 11a al. 5 lit. e LPD, ont elles aussi disparu. C'est regrettable compte tenu du rôle majeur que ce conseiller peut et doit jouer dans la mise en œuvre de la protection des données. Il est juste de ne pas en imposer la désignation et de renoncer à la réglementation excessivement détaillée des art. 38 ss du Règlement européen. Mais la mention de son rôle et de ses principales obligations (sur la base de l'Ordonnance actuelle) s'impose à notre sens. Que la Convention 108 révisée n'en fasse étonnamment pas mention non plus ne justifie pas ce silence dans l'avant-projet. Il est envisageable de mentionner

					ce rôle dans un article séparé ou de le faire en lien avec les obligations prévues à l'art. 18.
FDCA/UNIL	LPD	11			Pas de remarque : les principes de privacy by default et by design vont au-delà des questions de sécurité. Pour cette raison et vu leur importance, il paraît justifié de leur consacrer un article particulier dans la loi.
FDCA/UNIL	LPD	12			La question des données d'un défunt doit impérativement être traitée au niveau de la loi formelle. Le principe de l'art. 12 se justifie à cet égard. La disposition pose cependant de nombreux problèmes : il ne saurait être question d'écarter l'application des règles sur le secret professionnel au seul motif que la personne concernée est décédée (une pesée des intérêts représenterait un strict minimum); il n'est pas justifié non plus de déroger au principe de l'unanimité des héritiers (puisque ce sont eux, et non plus les proches, qui pourraient réclamer l'effacement des données). Cela dit, on peut se demander s'il est correct de conférer ce droit aux héritiers et pas aux proches, alors qu'il n'en va pas du patrimoine, mais de la personnalité du défaut. Si la question de la mort numérique mérite sans aucun doute une attention particulière, la disposition proposée est loin de répondre aux attentes. Il y aurait probablement lieu d'intégrer la réflexion dans la révision du droit successoral, plutôt que dans la LPD. Ce serait l'occasion de discuter aussi de problèmes dogmatiques : sachant qu'en droit suisse, la personnalité s'éteint à la mort de l'intéressé, il est curieux que la LPD fasse référence aux „intérêts prépondérants" du défunt. Et même qu'elle s'occupe tout court de cette question, puisqu'il n'y a plus de personne physique dont les données devraient être protégées par la LPD.
FDCA/UNIL	LPD	13			La reprise du système du droit européen, déjà largement applicable aux organes fédéraux, n'appelle pas de remarque particulière. Elle permet de renoncer au principe de reconnaissabilité. On se permettra simplement de s'interroger sur l'efficacité actuelle, en termes de protection des données matérielle et pas simplement formelle, de l'information donnée. L'étendue exacte de l'information à donner dépend des circonstances concrètes du cas, ce qui est correct (mais ce caractère par définition vague ne permet naturellement plus de sanctionner pénalement la violation de la loi, contrairement à ce que prévoit l'art. 50). On ne saurait exiger du responsable de traitement qu'il informe d'emblée sur des questions aussi confidentielles que l'identité et les coordonnées d'un sous-traitant. Ce n'est que dans le cadre du droit d'accès, et pour autant que des motifs particuliers le justifient, qu'une telle information doit être donnée

					(l'art. 7bis de la Convention 108 révisée n'exige en aucun cas une disposition telle que l'art. 13 al. 4). Il doit être possible de renvoyer la personne concernée à consulter une notice générale d'information (par ex. sur un site web), pour autant que celle-ci soit accessible et aisément compréhensible (forme et fond). Le texte de l'avant-projet le permet (cf. aussi Rapport p. 54). Il n'est pas nécessaire de le préciser expressément.
FDCA/UNIL	LPD	14			La reprise du mécanisme de l'art. 18b LPD à l'art. 14 al. 5 de l'avant-projet se justifie pleinement. C'était une incohérence de l'art. 14 LPD actuel. A notre sens, la lit. a de l'al. 4 doit être précisée : seule la communication volontaire à un tiers (et non par ex. sur injonction d'une autorité) doit écarter la possibilité de faire valoir les intérêts prépondérants du responsable de traitement.
FDCA/UNIL	LPD	15			Cette solution, malheureusement écartée lors de la révision 2003, est indispensable non seulement pour se mettre en conformité avec la réglementation européenne, mais aussi pour garantir un droit d'intervention personnel de l'individu. La notion de décisions ayant des effets juridiques devra être précisée par la pratique (la délivrance d'un montant au Bancomat, qui a en soi des effets juridiques, puisqu'elle constitue une restitution partielle du dépôt de la personne concernée, ou l'adjudication automatique d'une enchère sur internet ne sauraient ouvrir un droit à s'exprimer de la personne concernée – dans le 1er cas – et de tous les autres enchérisseurs – dans le 2ème cas – ne devraient pas tomber sous le coup de la loi). La 2ème partie de l'art. 15 al. 2 est superflue : ce droit résulte des autres dispositions de la loi. L'art. 15 doit viser uniquement un mode particulier de traitement.
FDCA/UNIL	LPD	16			Une règle sur l'analyse d'impact, moyen pratique important pour garantir la protection des données, se justifie pleinement. Outre que la terminologie pourrait ici être adaptée à la terminologie européenne (puisque l'institution est nouvelle dans le droit suisse), la communication systématique au PFPDT est irréaliste (pour l'entreprise et pour le PFPDT. en termes de charge de contrôle). Seuls les cas les plus problématiques devraient être communiqués (comp. art. 36 du Règlement européen). Le délai de d'objection de trois mois est de toute manière beaucoup trop long, surtout si une obligation générale de communication est maintenue : comme de nombreux traitements vont tomber sous le coup de l'art. 16, les retards pris par les projets en question risquent d'être considérables ... ou la disposition deviendra lettre morte parce qu'on lui a donné une trop large application. A noter encore que le sous-traitant ne peut naturellement procéder à un PIA que pour les opérations de traitement qu'il maîtrise seul.

FDCA/UNIL	LPD	17			Cette disposition, qui concrétise une obligation déjà existante, doit être saluée sur le principe. Elle doit toutefois, comme le Règlement européen (cf. la place des art. 32 et 33 dans le Règlement), être réservée aux violations importantes du principe de sécurité. Elle ne saurait porter sur „tout traitement non autorisé". Les al. 1 et 4 de la disposition ne concordent par ailleurs pas s'agissant des cas à annoncer.
FDCA/UNIL	LPD	18			Il s'agit là de principes aujourd'hui incontournables de la protection des données. Bien que découlant du principe de proportionnalité dans ses différentes composantes, il est important de les mentionner spécifiquement. La terminologie concise choisie tranche (heureusement) avec la lourdeur de l'art. 25 du Règlement européen. L'al. 2 est cependant problématique, car le texte ne fait que répéter le principe de finalité (alors que les explications du Rapport, p. 61, sont quant à elles correctes). Il faudrait dire : „que, par défaut, les données personnelles collectées et les finalités pour lesquelles elles sont traitées soient aussi limitées que possible." Sur l'absence de mention du conseiller à la protection des données dans la loi, cf. le commentaire ad art. 10 ci-dessus.
FDCA/UNIL	LPD	19			La lit. a n'appelle pas de remarque particulière; cette nouvelle obligation permet de renoncer à l'enregistrement des fichiers ou des traitements de personne privée, fort peu respectée et dont les effets sont à peu près nuls. La lit b. fait sens également pour les rectifications, effacements et destructions, pour autant naturellement que l'exception figurant à la fin de la disposition soit interprétée largement, faute de quoi le devoir pourrait mener à des absurdités. En revanche, on n'explique pas pour quelle raison toute violation de la protection des données (de quelque nature et de quelque ampleur que ce soit) devrait être communiquée au destinataire, alors qu'elle ne doit pas nécessairement l'être à la personne concernée (hors de l'art. 17). La communication au destinataire pourrait d'ailleurs être contraire aux intérêts de la personne concernée elle-même ! Il s'agit probablement d'une erreur de conception (même le droit de l'Union ne le prévoit pas, cf. art. 19 du Règlement).
FDCA/UNIL	LPD	20			Le droit d'accès, institution importante s'il en est (en tout cas sur le plan théorique, son usage pratique étant réduit, sauf quand il permet d'atteindre d'autres buts que ceux pour lesquels il a été mis en place,

					notamment des fins d'exploration pré-procédurale) doit être recentré sur son objectif premier : permettre à la personne concernée de savoir si des données sont traitées sur son compte et, dans l'affirmative, vérifier le respect des principes de protection des données. Ce type d'usage doit être limité et encadré. Le recours à l'abus de droit pour s'en prémunir ne suffit pas. L'al. 2 paraît désormais fixer un but à l'exercice du droit d'accès et le met directement en lien avec les droits prévus par la LPD. Il ne saurait donc être invoqué hors desdits buts. Le Rapport ne le dit pas suffisamment clairement. La référence à la transparence du traitement (vague) devrait par ailleurs être supprimée : le premier motif suffit et englobe le second également. Pour le reste, l'al. 2 lit. d doit être salué compte tenu de l'importance de la durée de conservation; la valeur incitative du droit d'accès est ici intéressante. Il en va de même des informations relatives aux décisions individuelles automatisées. En revanche, l'art. 13 al. 5 n'a plus sa place : la personne concernée ne saurait de manière générale avoir accès à l'identité des sous-traitants. Quant à l'al. 4, il doit préciser que c'est „avec l'accord" de la personne concernée qu'un médecin peut être mis en œuvre (l'intéressé conserve le droit d'exiger un accès direct, comme une partie de la doctrine le soutient aujourd'hui déjà concernant l'art. 8 al. 3 LPD). Il est également heureux, compte tenu de l'évolution technologique, que le principe d'une information donnée par des copies écrites ne figure plus dans la loi. En revanche, l'al. 3 va bien au-delà de l'art. 15 lit. h du Règlement européen. Il fait en outre double emploi, en partie, avec l'art. 15 de l'Avant-projet. Il ne saurait par ailleurs valoir pour toute décision (atteinte manifeste au secret des affaires), mais doit être limité, si on veut le garder, aux décisions automatisées. Si la disposition entend permettre un accès aux algorithmes utilisés (ce que le Rapport paraît contester), elle ne prévoit aucune cautèle ni procédure et ne saurait servir à cette fin : pour un domaine si important (notamment à l'ère de Big Data), une simple lecture parallèle des art. 21 et 22 (avec son renvoi à l'art. 14) n'est pas satisfaisante. Il pourrait par exemple être envisagé de recourir à une instance tierce neutre pour examiner le déroulement du processus automatisé et les critères utilisés en présence d'indice d'abus ou de violation des droits de la personne concernée. Une autre solution consisterait simplement à reprendre le texte de l'art. 8 al. 1 lit. c de la Convention 108 révisée. Il est important que le Conseil fédéral puisse comme aujourd'hui définir des exceptions à la gratuité. La disposition doit prévoir une délégation de compétences dans ce sens. On relèvera aussi une erreur en p. 62 du Rapport : il n'existe plus d'interdiction dans le Code civil depuis 2013.

FDCA/UNIL	LPD	21			Pas de remarque.
FDCA/UNIL	LPD	22			Pas de remarque.
FDCA/UNIL	LPD	23			La nouvelle formulation des art. 23 et 24 permet de clarifier le rapport entre la notion d'atteinte, d'illicéité et de motifs justificatifs. Le système matériel quant à lui a largement fait ses preuves. Il n'y a pas de raison de le changer. L'al. 2 lit. d doit cependant être modifié: il mélange à nouveau la notion d'atteinte et les motifs justificatifs. Il n'est pas nécessaire de réserver ici le consentement de l'intéressé (prévu à l'art. 24 al. 1), ni sa forme particulière, prévue à l'art. 4 al. 6.
FDCA/UNIL	LPD	24			La condition supplémentaire tenant à l'âge de la personne prévue à la lit. c est bienvenue ici (même si la prise en compte de l'intérêt des mineurs est largement insuffisante dans l'avant-projet, cf. remaque générale ci-dessus). Il en va de même de l'explicitation des conditions liées à la recherche (lit. e), même si une partie d'entre elles découlent déjà des principes généraux de la loi. On s'étonnera simplement de la modification apportée au texte allemand, alors que le texte français de l'art. 24 al. 2 est pour sa part (à raison) identique à l'art. 13 al. 2 actuel.
FDCA/UNIL	LPD	25			Pas de remarque particulière. Les facilitations procédurales (pas de sûretés, gratuité de la procédure, cf. CPC) doivent être saluées. Avoir renoncé à prévoir en plus un allègement du fardeau de la preuve est un choix politique défendable, de même que le fait de ne pas vouloir régler spécifiquement les actions collectives dans le cadre de la LPD, alors que la problématique est plus large. Mais la nécessité de prévoir de telles actions pour les litiges du droit de la consommation au sens large du terme ne fait à notre sens pas de doute. Il est bon de ne pas avoir consacré de disposition spéciale au „droit à l'oubli" qui, comme le précise à juste titre le Rapport (p. 67), existe aujourd'hui déjà en vertu des principes généraux. Compte tenu de l'importance prise par ce droit dans l'esprit du public, il paraît opportun de le mentionner expressément, sous la terminologie d'effacement, à l'art. 25. Il n'est pas nécessaire d'aller au-delà, ni de prévoir des règles spéciales pour les moteurs de recherche. La mention de la limitation de traitement (déjà possible sous l'empire du droit actuel) se justifie par les

					dispositions parallèles du droit de l'Union, même si la nouvelle Convention 108 n'en parle pas.
FDCA/UNIL	LPD	26			Pas de remarque.
FDCA/UNIL	LPD	27			La technique législative choisie (régler toutes les questions relatives à la base légale exigée) dans une même disposition doit être saluée. On peut en revanche douter que les auteurs du projet aient mesuré les conséquences d'une exigence de base légale formelle pour tout type de décision individuelle automatisée, alors que la notion est extrêmement large (elle couvre les accusés de réception électronique, la facturation électronique des services d'un registre public ou d'une assurance sociale, ou encore les programmes de filtrage et de sécurité dans les communications électroniques). Certains de ces exemples seront probablement exclus de la définition de l'art. 15, mais il serait préférable ici de limiter le champ d'application de l'art. 27 al. 2.
FDCA/UNIL	LPD	28			Pas de remarque.
FDCA/UNIL	LPD	29			Pas de remarque particulière. La suppression des règles spéciales sur la procédure d'appel est justifiée ; la protection ne s'en trouve pas amoindrie, car il s'agit toujours là d'une communication soumise aux autres conditions légales.
FDCA/UNIL	LPD	30			Pas de remarque.
FDCA/UNIL	LPD	31			Pas de remarque.
FDCA/UNIL	LPD	32			Pas de remarque particulière. On ne s'explique cependant pas pourquoi l'al. 1 lit. b ne concernerait que la communication de données sensibles à des personnes privées. La même règle doit valoir pour les organes fédéraux et pour les organes cantonaux et communaux. Le Rapport (p. 70) n'explique pas les raisons de ce choix.
FDCA/UNIL	LPD	33			Pas de remarque.
FDCA/UNIL	LPD	34			Cf. les remarques ad art. 25. L'al. 4 offre un bon compromis entre les intérêts publics et les intérêts privés. Les explications du Rapport (p. 71) sont convaincantes.

FDCA/UNIL	LPD	35			La disposition de coordination fait sens.
FDCA/UNIL	LPD	36			Dans le cadre de l'Etat de droit, le maintien d'une obligation générale de déclaration pour les organes fédéraux est justifié.
FDCA/UNIL	LPD	37			Pas de remarque.
FDCA/UNIL	LPD	38			Pas de remarque. La limitation à une période d'activité maximale de 12 ans est opportune.
FDCA/UNIL	LPD	39			Il est curieux de prévoir une interdiction absolue à al. 1, puis de réserver néanmoins des exceptions à l'al. 2. Cela dit, cet alinéa doit être supprimé : compte tenu de l'importance de la direction du service (avec nombreuses tâches nouvelles qui lui seront confiées), il n'est pas concevable que ce poste permette une activité lucrative accessoire en parallèle (la dérogation paraissant pouvoir porter tant sur une activité lucrative que non lucrative). Comment peut-on politiquement convaincre du sérieux du poste et du domaine s'il permet la poursuite d'une telle activité accessoire lucrative quelconque ? La solution pratiquée jusqu'à peu ne saurait être reconduite.
FDCA/UNIL	LPD	40			Les al. 2 et 3 font sens si l'on veut permettre au PFPDT d'intervenir non seulement dans les processus législatifs portant sur la protection des données, mais aussi dans la mise en œuvre concrète de ces principes par d'autres autorités.
FDCA/UNIL	LPD	41			La nouvelle terminologie („enquête") est justifiée. Il en va de même des conditions matérielles de l'al. 1. On perd toutefois la condition supplémentaire posée par l'actuel art. 29 al. 1 lit a LPD (nombre important de personnes). L'on devrait ajouter : « ... qu'un traitement de données pourrait être gravement contraire à des dispositions de protection des données ou porter atteinte à la personnalité d'un nombre important de personnes ». Il est en effet important d'encadrer de manière minimale les cas de déclenchement d'une enquête. La justification du rapport (p. 73) pour s'écarter du système actuel ne convainc pas : l'art. 1 du Protocole additionnel et l'art. 12bis al. 2 lit. a de la Convention révisée ont la même teneur. La limitation au pouvoir d'investigation (qui a le mérite de la transparence et de la prévisibilité, puisqu'elle est prévue par la loi, et non par des directives internes au service) ne saurait être jugée contraire aux textes du Conseil de l'Europe. L'al. 4 n'est pas compréhensible : ou il y a enquête et donc droit d'investigation, ou pas. Une solution

					différente est envisageable pour les organes fédéraux (cf. l'art. 27 al. 1 actuel), mais pas pour les personnes privées.
FDCA/UNIL	LPD	42			Le transfert de cette compétence au PFPDT est logique. Elle rend d'autant plus incompréhensible le refus de doter le PFPDT d'un pouvoir de sanction administrative (cf. infra). Si l'on veut véritablement renoncer à l'effet suspensif (en dépit des conséquences gravissimes qu'une interdiction injustifiée peut avoir pour l'auteur de traitement privé), il doit au moins pouvoir être restitué par l'autorité de recours (art. 55 al. 3 PA), et cela même si l'on se trouve dans un cas réservé par l'art. 55 al. 5 PA. Cette possibilité doit être mentionnée expressément.
FDCA/UNIL	LPD	43			Le système, à l'origine innovateur mais fruit d'un compromis politique, de la recommandation a vécu : les mesures doivent pouvoir être prononcées par le PFPDT, avec voies de recours ordinaires. A l'al. 2, il faut indiquer que le préposé peut „ordonner la suspension" (comme à l'al. 1), car le PFPDT ne suspend pas la communication lui-même (la terminologie européenne est défaillante sur ce point). La possibilité prévue à l'al. 2 de faire suspendre une communication transfrontière contraire à d'*autres lois fédérales* paraît par ailleurs conférer un pouvoir exorbitant au PFPDT, en lui confiant indirectement un rôle de surveillance dans d'autres domaines que la LPD. Pour ne pas mélanger les rôles, son pouvoir d'intervention devrait être limité aux violations de la LPD. La question de l'échange d'informations entre les autorités concernées et de leur éventuelle coopération est régie par l'art. 40 et par l'art. 47.
FDCA/UNIL	LPD	44			Pas de remarque.
FDCA/UNIL	LPD	45			Pas de remarque.
FDCA/UNIL	LPD	46			Pas de remarque.
FDCA/UNIL	LPD	47			La construction de la disposition doit être complètement revue. Avec le système proposé, l'autorité étrangère obtiendrait des informations sans condition en répondant à une demande d'entraide suisse, alors qu'elle ne les obtiendrait que sous conditions en demandant elle-même l'assistance ! L'autorité ne saurait par ailleurs dévoiler d'emblée par ex. les mesures techniques et organisationnelles d'un auteur de traitement dans le seul but d'obtenir des informations, sans aucune réserve ou protection du secret d'affaires.

FDCA/UNIL	LPD	48			Même si elle n'est pas prévue dans la loi aujourd'hui, la périodicité du rapport (annuel) devrait être introduite dans le projet.
FDCA/UNIL	LPD	49			Pas de remarques.
FDCA/UNIL	LPD	50-51			La voie pénale n'est pas la voie adéquate pour sanctionner des violations des règles de protection des données, comme l'a montré la loi actuelle. Le juge pénal n'est pas l'autorité idoine et la nécessité d'identifier des personnes physiques dans le contexte pénal rend l'arsenal inefficace malgré le nouvel art. 53 proposé par l'Avant-projet (dont la limite maximale d'application torpille toutes les amendes dissuasives prévues aux art. 51 et 52, mais ne met pas pour autant à l'abri les personnes physiques concernées, puisqu'elles ne peuvent évidemment pas *exiger* que cette disposition soit appliquée). Le risque de sanctions pénales pourrait au demeurant paralyser l'action des personnes concernées à l'intérieur des entreprises, alors que c'est au contraire la responsabilité de celles-ci de mettre en place des systèmes et processus conformes aux exigences légales. Le fait d'augmenter les montants d'amende ou le nombre d'infractions poursuivies n'y changera rien. La pratique s'est de longue date montrée favorable à un système de sanctions administratives, déjà pratiqué à l'étranger et désormais uniformisé dans le Règlement européen. Le refus de revoir l'organisation du service du Préposé comme motif justifiant cette voie solitaire est incompréhensible. Le PFPDT peut être facilement déchargé de tâches inutiles que lui confie l'avant-projet (cf. les remarques ci-dessus) pour dégager du temps pour procéder à des enquêtes administratives dans les cas importantes, sur le modèle par ex. de la Comco ou de la Finma. Le chapitre doit donc être complètement revu. Il faudra décider si certaines violations méritent *en plus* une incrimination pénale, ce dont on peut douter. On peut au demeurant se demander si les „mesures administratives" prévues à l'art. 43 de l'avant-projet sont suffisantes pour respecter l'exigence de l'art. 12bis al. 1 lit. c de la Convention 108 révisée, qui demande que l'autorité de contrôle dispose notamment du pouvoir d'infliger des „sanctions administratives". Dans le Rapport (p. 75, ch. 8.1.7.7 § 2), il est indiqué à la fois que l'art. 43 respecte la disposition conventionnelle et que le Conseil fédéral propose de ne pas la respecter ! S'agissant des violations visées par les art. 50 et 51, l'on renvoie aux commentaires faits ci-dessus concernant les dispositions matérielles. La suppression de certains devoirs se justifie d'autant plus que leur violation est sanctionnée (pénalement ou administrativement) même en cas de négligence. L'on notera encore que certaines obligations (par exemple les conditions d'une sous-traitance selon

					l'art. 7 al. 1 et 2, cf. art. 51 al. 1 lit. b, ou ce que recouvre la notion du privacy by design ou by default, art. 18 et art. 51 al. 1 lit. e) sont tellement vagues qu'il serait impossible pour un juge pénal (et contraire au principe *nullum crimen sine lege*) de prononcer la moindre condamnation sauf circonstances d'une gravité extrême (par définition rares). L'auteur du projet a certainement accordé un poids trop important à ces dispositions (comme par ex. à l'art. 16) pour arriver à vouloir sanctionner leur violation par des amendes pénales importantes, susceptibles d'être infligées à des personnes physiques. Il est par ailleurs curieux de sanctionner ici aussi durement la négligence alors que la violation par négligence d'autres secrets n'est pas incriminée pénalement (cf. art. 320-321ter CP en lien avec l'art. 12 al. 1 CP).
FDCA/UNIL	LPD	52			La justification de l'al. 1 lit. b ne convainc pas. On ne voit pas le lien entre le caractère secret des données et leur traitement „à des fins commerciales". Si cette utilisation devait demeurer dans l'avant-projet, il faudrait revenir à la solution actuelle et ne prévoir d'incrimination que lorsque des données sensibles secrètes sont en jeu. Le champ d'application donné à ce nouveau „secret", dont la violation est sanctionnée bien plus sévèrement que sous l'angle de l'art. 35 LPD actuel, paraît excessivement large. La disposition doit impérativement être revue, faute de quoi toute communication de données qui contreviendrait aux règles de la loi constituera une infraction pénale, ce qui n'est certainement pas le but visé. Si l'on avait voulu étendre aussi largement l'application de la disposition, encore eût-il fallu prévoir des mécanismes permettant de déroger au secret, autres que le consentement de l'intéressé (autorisation d'une autorité externe). La portée limitée de l'art. 35 LPD ne requiert en revanche pas un tel mécanisme. En l'absence de tout véritable besoin de révision sur ce point, l'art. 35 LPD pourrait être conservé comme tel.
FDCA/UNIL	LPD	53			Pas de remarque.
FDCA/UNIL	LPD	54			Pas de remarque.

FDCA/UNIL	LPD	55			Pas de remarque.
FDCA/UNIL	LPD	56			Pas de remarque.
FDCA/UNIL	LPD	57			Pas de remarque.
FDCA/UNIL	LPD	58			Pas de remarque.
FDCA/UNIL	LPD	59			Il manque une réflexion générale de droit transitoire. On peut imaginer que le respect de certaines règles (par ex. un système de notification de violations de la sécurité) ou la mise en place d'un droit accès élargi tel que prévu par l'avant-projet demandent un temps d'adaptation pour les auteurs de traitement. L'art. 59 lit. a n'est par ailleurs pas clair: une étude d'impact doit-elle être réalisée pour les traitements en cours, ou l'auteur du traitement doit-il être capable d'en réaliser une dans les deux ans pour les *nouveaux* traitements qui tomberaient sous le coup de l'art. 16 (c'est ainsi que l'on devrait, selon nous, comprendre la disposition) ?
FDCA/UNIL	CPC				Cf. le commentaire ad art. 25 ci-dessus.
FDCA/UNIL	CC	45a			Le Rapport (p. 86) parle de dérogation à l'art. 32 al. 1 à 3. Le texte de l'avant-projet mentionne l'art. 34 al. 1 à 3, ce qui correspond probablement à l'intention de l'auteur de l'avant-projet.
FDCA/UNIL	CP	179novies			L'extension du champ d'application de la disposition ne se justifie pas (cf. les commentaires ci-dessus ad art. 52 LPD).
FDCA/UNIL	CP	179decies			La disposition proposée est adéquate, les concours avec d'autres dispositions étant réservés comme le souligne le Rapport p. 89. Une incrimination pénale permettra également de faire réunir par l'autorité les éléments de preuve parfois difficiles à obtenir.

Fédération des
Entreprises
Romandes

Secrétariat général

Jonas.amstutz@bj.admin.ch

Département fédéral de justice et police
(DFJP)
Mme Simonetta Sommaruga
Conseillère fédérale
Palais fédéral ouest
3003 Berne

Genève, le 4 avril 2017
FER No 38-2016/JD/ikm/bfb

Réponse à la consultation concernant les textes suivants :

- *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 et 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*

Madame la Conseillère fédérale,

La Fédération des Entreprises Romandes (ci-après : FER) a pris connaissance de la procédure de consultation ouverte par le Département fédéral de justice et police, laquelle porte sur les trois objets cités en référence.

I. Remarques générales

Après lecture de 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 (ci-après : AP-LPD), notre Fédération porte à votre connaissance qu'elle refuse le projet tel que proposé.

Les raisons de ce refus sont multiples mais les principales sont les suivantes :

Premièrement, l'AP-LPD va au-delà de ce que nécessite l'harmonisation voulue par la Suisse avec le droit de l'Union européenne ainsi que celui du Conseil de l'Europe.

Deuxièmement, cet avant-projet génère, pour les entreprises, un surcroît de procédures à mettre en place et à respecter, ce qui engendre inévitablement une augmentation des coûts.

Troisièmement, il réduit de manière inadmissible les possibilités pour les parties à un procès de se défendre en justice.

Enfin, cet avant-projet alourdit les sanctions, respectivement les responsabilités, des personnes qui traitent des données personnelles de manière disproportionnée.

S'agissant des deux autres objets soumis à consultation, notre Fédération les accepte. Elle ne s'oppose en effet pas au développement de l'acquis Schengen. La Directive (UE) 2016/680 constitue un développement de l'acquis Schengen. Conformément à l'accord d'association à Schengen, la Suisse est tenue de transposer les exigences de cet acte dans son ordre juridique interne[1]. Notre Fédération ne s'oppose pas non plus à la ratification du projet de modernisation de la Convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Il est en effet dans l'intérêt de la Suisse de pouvoir ratifier la convention modernisée, eu égard notamment à la décision de la Commission européenne, selon laquelle la Suisse dispose d'un niveau de protection des données adéquat[2].

II. Remarques spécifiques relatives à 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

Notre Fédération vous prie de trouver ci-après ses remarques sur les dispositions de l'AP-LPD qui, selon elle, peuvent poser problème.

Ad art. 2 al. 1 - Champ d'application

L'AP-LPD propose de supprimer les personnes morales du champ d'application de la LPD, laquelle ne s'appliquerait plus qu'aux personnes physiques.
Selon le Rapport explicatif[3], cette solution, qui correspond à celle de la majorité des législations étrangères, a pour avantage de ne plus soumettre la communication à l'étranger de données concernant des personnes morales à la condition qu'un niveau de protection adéquat soit garanti dans l'Etat de destination (art. 5 AP-LPD), ce qui devrait favoriser les flux transfrontières.
Le fait que les personnes morales ne bénéficient plus de la protection des données a également des inconvénients. Elles perdent notamment le droit d'accès conféré par la LPD.
Les avantages que les personnes morales ne tombent plus sous le coup de la LPD nous paraissent toutefois supérieurs aux inconvénients que cela implique.
La FER ne s'oppose donc pas à ce que l'avant-projet LPD supprime les personnes morales du champ d'application de la loi fédérale sur la protection des données.

Ad art. 2 al. 2 let. c - Champ d'application

Selon l'AP-LPD, l'exception relative aux procédures pendantes serait modifiée, de sorte que la LPD serait applicable à de telles procédures.
Par cette modification, il deviendrait extrêmement difficile pour une partie citée en justice d'exposer les faits et de produire les moyens de preuve nécessaires. Elle devrait en effet obtenir l'accord préalable de chaque personne tierce mentionnée dans ses écritures judiciaires et ses moyens de preuve, ce qui n'est pas raisonnable. Ceci d'autant plus que ce consentement pourrait se monnayer.

---

[1] Office fédéral de la justice OFJ, 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 21 décembre 2016, Berne, p. 2

[2] Office fédéral de la justice OFJ, 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 21 décembre 2016, Berne, p. 15

[3] Office fédéral de la justice OFJ, 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 21 décembre 2016, Berne, p. 38

Le fait que les tribunaux cantonaux soient soumis à une loi cantonale sur la protection des données cantonale ne règle pas le problème. En effet, les personnes privées (physiques ou morales), assignées en justice, ne sont pas soumises aux lois cantonales sur la protection des données.
Vu ce qui précède, la FER s'oppose à la modification proposée. Autrement dit, notre Fédération demande que, comme c'est le cas aujourd'hui, la loi sur la protection des données ne s'applique pas aux procédures pendantes civiles, pénales, d'entraide judiciaire internationale ainsi que de droit public et de droit administratif (cf. art. 2 al. 2 let. c LPD actuellement en vigueur).

_Ad_ art. 3 let. f - Définitions (Profilage)
L'AP-LPD introduit une nouvelle notion. Il s'agit du « profilage », lequel est défini comme *toute exploitation de données personnelles ou non, consistant à analyser ou prédire les caractéristiques personnelles essentielles d'une personne, notamment son rendement au travail, sa situation économique, sa santé, sa sphère intime, ou ses déplacements* (art. 3 let. f).
Or d'une part le projet de modernisation de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après : P-STE 108) que la Suisse souhaite ratifier ne contient pas cette notion de profilage.
D'autre part, tant l'art. 3 de la Directive de l'Union européenne 2016/680[4], applicable au traitement de données par les autorités (ci-après : Directive (UE) 2016/680), que l'art. 4 al. 4 du Règlement européen 2016/679[5] définissent le profilage comme *toute forme de traitement automatisé de données à caractère personnel* […].
L'art. 3 let. f de l'avant-projet de la loi sur la protection des données va donc au-delà des exigences de l'Union européenne. En effet, à la différence des règles européennes, même le profilage manuel est couvert par l'avant-projet. Et même des données non-personnelles sont couvertes. Ainsi, selon l'avant-projet, si un employé remplit un questionnaire d'évaluation, il faudrait obtenir son consentement exprès, faute de quoi cela constituerait une violation de la loi sur la protection des données.
Partant, cette disposition doit être modifiée en ce sens qu'elle ne doit couvrir que le profilage automatisé et seulement les données personnelles.

_Ad_ art. 5 al. 3 - Communication de données personnelles à l'étranger
L'AP-LPD prévoit qu'*en l'absence d'une décision du Conseil fédéral, des données personnelles peuvent être communiquées à l'étranger lorsqu'un niveau de protection approprié est garanti par des garanties spécifiques, notamment contractuelles, préalablement communiquées au préposé* (art. 3 al. 3 let. b AP-LPD). Dans un tel cas, selon l'AP-LPD, le préposé dispose d'un délai de 30 jours pour communiquer des éventuelles objections au responsable du traitement (art. 5 al. 4 AP-LPD).
L'AP-LPD prévoit en outre qu'*en l'absence d'une décision du Conseil fédéral, des données personnelles peuvent être communiquées à l'étranger lorsqu'un niveau de protection approprié est garanti par des garanties standardisées, notamment contractuelles, préalablement approuvées par le préposé* (art. 5 al. 3 let. c AP-LPD) *ou par des règles d'entreprises contraignantes préalablement approuvées par le préposé* (art. 5 al. 3 let. d AP-LPD). Dans ce cas, le préposé dispose d'un délai de six mois à compter de la réception du dossier complet des garanties standardisées ou des règles d'entreprises contraignantes pour communiquer au responsable du traitement si elles sont approuvées ou non (art. 5 al. 5 AP-LPD).

---

[4] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre du Conseil, JO L 119 du 4.5.2016 p. 89.
[5] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, JO L 119 4.5.2016 p. 1)

Premièrement, la différence entre les garanties spécifiques, notamment contractuelles, au sens de l'art. 5 al. 3 let. b et les règles d'entreprises contraignantes au sens de l'art. 5 al. 3 let. d. mériterait d'être précisée, voire supprimée.
Deuxièmement, les règles d'entreprises contraignantes devraient bénéficier du même régime que les garanties spécifiques, à savoir être communiquées préalablement au préposé, sans devoir faire l'objet d'une approbation.
Troisièmement, prévoir un délai de six mois pour obtenir l'approbation n'est pas raisonnable. Une entreprise ne peut pas attendre six mois avant de pouvoir transférer des données à l'étranger. Ce délai doit être réduit à 30 jours comme le prévoient l'art. 5 al. 4 AP-LPD, respectivement l'art. 6 al. 5 de l'OPLD actuelle.

_Ad_ art. 7 al. 2 - Sous-traitance
L'art. 7 al. 2 AP-LPD indique que *le responsable du traitement doit en particulier s'assurer que le sous-traitant est en mesure de garantir la sécurité des données personnelles et les droits de la personne concernée*.
L'art. 10a al. 2 de la LPD en vigueur actuellement prévoit que le mandant doit en particulier s'assurer que le tiers garantisse la sécurité des données. En revanche, il n'oblige pas le responsable du traitement à garantir les droits de la personne concernée.
Selon le Rapport explicatif[6], cette extension est exigée par la Directive (UE) 2016/680 (art. 22 par. 1). Le Conseil fédéral estime qu'une transposition uniquement sectorielle dans les domaines Schengen ne fait pas de sens, ceci d'autant plus que le Règlement (UE) 2016/679 prévoit une règle similaire (art. 28 par. 1)
Or le projet de Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (P-STE 108) ne prévoit rien concernant la sous-traitance.
Notre Fédération demande donc que l'art. 10a de l'actuelle LPD ne soit pas modifié. Autrement dit que son champ d'application ne soit pas élargi.

_Ad_ art. 7 al. 3 - Sous-traitance
L'art. 7 al. 3 AP-LPD est nouveau. Il prévoit que *le sous-traitant ne peut lui-même sous-traiter un traitement qu'avec l'accord écrit préalable du responsable du traitement.*
Il s'agit là aussi d'une exigence de la Directive (UE) 2016/680, pour les domaines Schengen (art. 22 par. 2). Le Règlement (UE) 2016/679 prévoit une règle similaire (art. 28 par. 2). Le Conseil fédéral a fait le choix de l'appliquer à tous les cas de sous-traitance[7].
Notre Fédération refuse cette extension, le projet de Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (P-STE 108) ne prévoyant rien concernant la sous-traitance.

_Ad_ art. 12 - Données d'une personne décédée
L'art. 12 al. 5 AP-LPD prévoit que *chaque héritier peut exiger que le responsable du traitement efface ou détruise les données personnelles du défunt*.
L'art. 12 al. 5 AP-LPD prévoit deux exceptions : let. a) *si le défunt l'a expressément interdit de son vivant* ou let. b) *si l'effacement ou la destruction va à l'encontre d'intérêts prépondérants du défunt ou de tiers. Les dispositions spéciales d'autres lois fédérales sont réservées* (art. 12 al. 5 AP-LPD).
Cette disposition pose un certain nombre de problèmes. Qu'en est-il si un héritier unique demande à une entreprise de détruire toutes les données d'un ancien employé décédé, et que les délais de prescription ne soient pas échus ? L'art. 12 al. 5 AP-LPD ne permet pas d'invoquer la sauvegarde des moyens de preuve en vue d'un éventuel litige pour refuser la destruction des données.

---

[6] Office fédéral de la justice OFJ, 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 21 décembre 2016, Berne, p. 50
[7] Ibidem

En d'autres termes, tel qu'il est rédigé, l'art. 12 al. 5 AP-LPD ne permet pas au responsable du traitement d'opposer ses propres intérêts privés prépondérants à une demande faite par un héritier de détruire les données du défunt.
L'AP-LPD confère donc plus de droits à l'héritier qu'au titulaire des données, lequel pouvait se voir opposer un intérêt prépondérant du maître du fichier ou le respect d'une obligation légale (par exemple, le devoir de conserver ces données).
Notre Fédération demande donc que les exceptions de l'art. 12 al. 5 AP-LPD soient étendues, premièrement en permettant au responsable du traitement de refuser la destruction des données du défunt en invoquant ses propres intérêts prépondérants et deuxièmement en ajoutant une troisième exception, à savoir le respect d'une obligation légale.

_Ad_ art. 13 - Devoir d'informer lors de la collecte de données personnelles

L'art. 13 al. 2 AP-LPD indique que *: Au plus tard lors de la collecte de données personnelles, il (le responsable du traitement) communique à la personne concernée les informations nécessaires à la mise en œuvre des droits de celle-ci et garantissant la transparence du traitement, notamment :*

a. *l'identité et les coordonnées du responsable du traitement ;*
b. *les données ou catégories de données personnelles traitées ;*
c. *les finalités du traitement.*

Cette disposition est critiquable pour plusieurs raisons :
Tout d'abord, malgré la liste – exemplative – indiquée ci-dessus, le responsable du traitement ne sait pas exactement quelles informations il doit communiquer. Qu'entend-on par « les informations nécessaires à la mise en œuvre des droits » ? Au vu des sanctions pénales prévues par l'AP-LPD en cas de manquement à cette obligation (art. 50 AP-LPD), les responsables du traitement auront tendance à donner beaucoup d'informations. Or trop d'information est contre-productif. On ne les lit plus.
Avec cette disposition, si l'on installe par exemple une caméra de surveillance, l'on devrait alors ajouter un panneau à côté de la caméra pour donner toutes les informations requises par l'AP-LPD[8].
Un devoir de transparence basé sur le risque, comme l'art. 4 LPD le prévoit aujourd'hui, suffit. On évitera ainsi des pages et des pages de textes en petits caractères sur les sites Internet[9].
L'art. 13 al. 4 AP-LPD prévoit en outre que *lorsqu'un traitement est confié à un sous-traitant, le responsable du traitement communique à la personne concernée son identité et ses coordonnées, ainsi que les données personnelles ou les catégories de données personnelles concernées*.
Cette disposition va au-delà du projet de Convention STE 108 du Conseil de l'Europe, laquelle ne traite pas de la sous-traitance. L'art. 13 al. 4 AP-LPD devrait dès lors être supprimé.

_Ad_ art. 14 al. 1 - Exceptions au devoir d'informer et restrictions

L'art. 14 al. 1 AP-LPD prévoit que *le responsable du traitement est délié du devoir d'information au sens de l'art. 13 lorsque la personne concernée dispose déjà des informations correspondantes*.
Selon le Rapport explicatif[10], l'exception au devoir d'informer vaut également lorsque la personne concernée a elle-même rendu les informations accessibles. Cette précision mériterait de figurer expressément dans la loi.
L'art. 14 al. 1 AP-LPD devrait aussi comprendre les cas où le traitement de données résulte de la loi ou des circonstances ou qu'il est reconnaissable par la personne concernée (cf. art. 4 al. 4 actuelle LPD)[11].

---

[8] David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz : Was er bedeutet, in : Jusletter 20 février 2017, p. 18
[9] Ibidem
[10] Office fédéral de la justice OFJ, 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 21 décembre 2016, Berne, p. 55

L'art. 14 al. 3 let. a AP-LPD stipule qu'*il est possible de restreindre, de différer la communication des informations ou d'y renoncer si le responsable du traitement est une personne privée, lorsque ses intérêts l'exigent et à condition qu'il ne communique pas les données personnelles à des tiers.*
Cette dernière phrase « à condition qu'il ne communique pas les données personnelles à des tiers » devrait être supprimée. Deux raisons justifient cette suppression. D'une part, il s'agit de tenir compte des intérêts prépondérants des groupes de sociétés. D'autre part, cela évite de devoir informer toutes les personnes citées dans des moyens de preuve lors de leur collecte en vue d'une éventuelle procédure.

***Ad* art. 16 - Analyse d'impact relative à la protection des données**
L'art. 16 al. 1 AP-LPD prévoit que *lorsqu'un traitement est envisagé et lorsque le traitement envisagé est susceptible d'entraîner un risque accru pour la personnalité et les droits fondamentaux de la personne concernée, le responsable du traitement ou le sous-traitant procède au préalable à une analyse d'impact.*
Notre Fédération a pris bonne note que cette disposition concrétise les exigences posées par le projet de Convention du Conseil de l'Europe STE 108 ainsi que par la Directive européenne 2016/680.
Toutefois, il nous paraît difficile de savoir ce qu'est un risque accru. Le non-respect de l'obligation de procéder à une analyse d'impact du traitement étant sanctionné pénalement (art. 50 al. 1 let. c AP-LPD), cette notion mériterait d'être définie. L'art. 35 du Règlement (UE) 2016/679 est beaucoup plus détaillé. Il donne des exemples dans lesquels l'analyse d'impact est nécessaire et dans lesquels elle ne l'est pas.

L'art. 16 al. 3 AP-LPD prévoit que *le responsable du traitement ou le sous-traitant doit communiquer les résultats de l'analyse au préposé, ainsi que les mesures envisagées.* Le non-respect de cette communication est sanctionné pénalement (art. 51 al. 1 let. d AP-LPD).
Cette information ne figure pas dans le projet de Convention 108 du Conseil de l'Europe. Cette obligation d'information doit donc être supprimée.

L'art. 16 al. 4 AP-LPD stipule que *si le préposé a des objections concernant les mesures envisagées, il en informe le responsable du traitement ou le sous-traitant dans un délai de 3 mois dès la réception de toutes les informations nécessaires.*

Or l'art. 28 de la Directive (UE) 2016/680 prévoit un délai maximum de 6 semaines.
Le délai de trois mois fixé par l'AP-LPD est excessif. Il doit donc être réduit. Le délai de trois mois conduit également à des situations absurdes. En effet, si une autorité étrangère de surveillance demande des documents et impose un délai plus court que trois mois, l'entreprise devra choisir entre violer le droit suisse ou violer le droit étranger[12].Ce délai doit donc être réduit à 30 jours comme cela est prévu pour l'examen par le préposé des garanties contractuelles en cas de communication à l'étranger.

En résumé, les alinéas 4 et 5 de l'art. 16 AP-LPD vont beaucoup plus loin que les exigences internationales. Non seulement par rapport au délai dans lequel le préposé doit se déterminer, mais surtout par rapport à l'obligation d'informer le préposé. Ces deux alinéas devraient donc être supprimés.

---

[11] David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz : Was er bedeutet, in : Jusletter 20 février 2017, p. 19
[12] David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz : Was er bedeutet, in : Jusletter 20 février 2017, p. 29

***Ad* art. 17 al. 1 - Notification des violations de la protection des données (au préposé)**

Cette disposition prévoit que *le responsable du traitement notifie sans délai au préposé tout traitement non autorisé ou toute perte de données personnelles, à moins que la violation ne présente vraisemblablement pas de risque pour la personnalité et les droits fondamentaux de la personne concernée.*

Or la notification de toute perte de données personnelles n'est mentionnée ni dans le Règlement (UE) 2016/678 (art. 33), ni dans la Directive (UE) 2016/680 (art. 30), ni dans le projet de Convention 108 du Conseil de l'Europe (art. 7 par. 2).

La perte de données personnelles doit donc être exclue de l'art. 17 al. 1 AP-LPD.

***Ad* art. 17 al. 2 - Notification des violations de la protection des données (à la personne concernée)**

Selon l'art. 17 al. 2 AP-LPD, le responsable du traitement doit *informer par ailleurs la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le préposé l'exige.*

Cette obligation de s'auto-dénoncer envers la personne concernée n'est pas prévue par le projet de Convention 108 du Conseil de l'Europe.

Cette disposition va également au-delà des exigences européennes. L'art. 34 par. 2 du Règlement (UE) 2016/679, respectivement l'art. 31 de la Directive UE 2016/680, ne prévoient en effet une information à la personne concernée que si la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et les libertés d'une personne physique.

De plus, l'art. 31 de la Directive prévoit plusieurs exceptions au devoir de communiquer la violation à la personne concernée, qui ne sont pas reprises par l'AP-LPD.

Enfin, selon l'AP-LPD, le non-respect de cette obligation de s'auto-dénoncer envers la personne concernée est pénalement répréhensible (art. 50 al. 1 let. b ch. 2 AP-LPD).

En résumé, l'AP-LPD oblige le responsable du traitement à se dénoncer auprès de la personne concernée sans bénéficier d'aucune diminution de peine, voire d'une amnistie, s'il le fait.

Vu ce qui précède, notre Fédération refuse l'obligation de s'auto-dénoncer prévue par l'art. 17 al. 2 AP-LPD. Cette disposition doit être supprimée.

***Ad* art. 19 - Autres obligations**

L'art. 19 let. b AP-LPD prévoit une obligation d'informer les destinataires des données en cas de rectification, d'effacement ou de limitations du traitement.

Or d'une part cette obligation ne figure pas dans le projet de convention STE 108 du Conseil de l'Europe. D'autre part, cette obligation peut être impossible à respecter. En effet, comment un journal peut informer tous ses lecteurs d'une éventuelle rectification de données, alors qu'il ne peut pas déterminer l'ensemble de ses lecteurs ?

L'art. 10 let. b AP-LPD prévoit en outre que le responsable du traitement et le sous-traitant sont tenus d'informer les destinataires auxquels des données ont été communiquées de toute violation de la protection des données.

Cette obligation de s'auto-dénoncer est inadmissible, ce d'autant plus que l'art. 50 al. 3 let. a AP-LPD prévoit une sanction pénale en cas de non-respect de cette obligation. Le principe *nemo tenetur se ipsum accusare, selon lequel nul n'est obligé de s'accuser soi-même,* n'est pas respecté[13].

***Ad* art. 20 - Droit d'accès**

L'art. 20 al. 1 AP-LPD prévoit la gratuité du droit d'accès.

Or ceci va au-delà des exigences du projet de Convention STE 108 du Conseil de l'Europe (art. 8 al. 1 let. b).

---

[13] David Vasella, Jacqueline Sievers, Der « Swiss Finish » im Vorentwurf des DSG, in : digma – Zeitschrift fü Datenrecht und Informationssicherheit, 2017, pp. 44, 47

Le principe de la gratuité, sous réserve d'exceptions, qui figure actuellement à l'art. 8 al. 5 LPD, devrait être maintenu, de même que l'art. 2 OLPD actuellement en vigueur. Celui-ci prévoit en effet qu'une participation équitable aux frais peut exceptionnellement être demandée (au maximum CHF 300.-) lorsque les renseignements désirés ont déjà été communiqués au requérant dans les douze mois précédant la demande, et que ce dernier ne peut justifier d'un intérêt légitime, telle la modification non annoncée des données le concernant; ou lorsque la communication des renseignements demandés occasionne un volume de travail considérable.
L'art. 20 al. 3 AP-LPD prévoit que *lorsque le traitement de données personnelles conduit à une décision, en particulier à une décision individuelle automatisée, la personne concernée reçoit des informations sur le résultat de la décision, la manière dont elle a été obtenue ainsi que sur ses conséquences*.

D'une part, le devoir d'information prévu par cette disposition est beaucoup trop étendu. L'obligation d'information devrait être limitée aux décisions individuelles automatisées.
L'art. 20 al. 3 AP-LPD devrait donc être modifié comme suit : *lorsque le traitement de données personnelles conduit à une décision individuelle automatisée, la personne concernée reçoit des informations sur le résultat de la décision, la manière dont elle a été obtenue ainsi que sur ses conséquences*.
D'autre part, cette information a déjà été donnée au moment du traitement (cf. art. 13 AP-LPD).
Cet art. 20 al. 3 AP-LPD devrait donc être supprimé.

_Ad_ art. 44 al. 3 - Procédure
Cette disposition prévoit que les recours formés contre les mesures provisoires visées à l'art. 42 n'ont pas d'effet suspensif. Or l'absence d'effet suspensif peut être très dommageable pour une entreprise. Cela empêche l'entreprise d'agir, même si elle avait finalement raison.

_Ad_ art. 45 - Obligation de dénoncer
L'obligation faite au Préposé de dénoncer les infractions pénales poursuivies d'office devrait être supprimée. En effet, vu l'art. 17 AP-LPD qui oblige le responsable du traitement à notifier sans délai au Préposé tout traitement non-autorisé ou toute perte de données personnelles, le fait que l'autorité les dénonce pénalement ne va pas encourager les responsables de traitement à s'auto-dénoncer.

_Ad_ art. 50 - Violation des obligations de renseigner, de déclarer et de collaborer
Cette disposition prévoit des sanctions pénales alors que ni le projet de Convention STE 108 du Conseil de l'Europe, ni la Directive UE 2016/680 ne prévoient l'obligation d'instaurer des sanctions pénales. Des sanctions administratives seraient non seulement suffisantes au regard du droit européen, mais aussi beaucoup plus judicieuses.
Notre Fédération demande donc une refonte complète de cette disposition, en supprimant les sanctions pénales. Ce d'autant plus que le responsable du traitement des données a une obligation de s'auto-dénoncer (art. 17 AP-LPD), laquelle est au surplus contraire au principe *nemo tenetur se ipsum accusare*.

_Ad_ art. 51 - Violation des devoirs de diligence
L'art. 51 AP-LPD prévoit également des sanctions pénales en cas de violation des devoirs de diligence alors que, comme déjà indiqué, ni le projet de Convention STE 108 du Conseil de l'Europe, ni la Directive UE 2016/680 ne prévoient l'obligation d'instaurer des sanctions pénales. Des sanctions administratives seraient non seulement suffisantes au regard du droit européen, mais aussi beaucoup plus judicieuses. Notre Fédération demande donc la suppression des sanctions pénales.

***Ad* art. 52 – Violation du devoir de discrétion**
L'art. 52 AP-LPD alourdit la sanction qui est prévue actuellement à l'art. 35 de la LPD. Alors que le droit actuel sanctionne d'une amende la violation du devoir de discrétion, l'art. 52 AP-LPD prévoit une peine privative de liberté de trois ans au plus ou une peine pécuniaire.
Or rien ne justifie l'alourdissement de la sanction en cas de violation du devoir de discrétion.
Aussi l'art. 35 LPD actuellement en vigueur doit-il être maintenu.

***Ad* art. 53 - Contraventions commises dans une entreprise**
Cette disposition indique que *si l'amende ne dépasse pas CHF 100'000.- et qu'il apparaît que l'enquête portant sur des personnes punissables en vertu de l'art. 6 de la loi fédérale du 22 mars 1974 sur le droit pénal administratif implique des mesures d'instruction hors de proportion avec la peine encourue, l'autorité peut renoncer à poursuivre ces personnes et condamner l'entreprise au paiement de l'amende.*
Notre Fédération refuse cette nouvelle responsabilité des entreprises, laquelle est inadmissible. On remarquera que lorsqu'il s'agit du champ d'application personnel, on supprime les personnes morales. Celles-ci ne peuvent donc plus bénéficier des droits qui leur étaient accordés par le droit actuel de la protection des données. Alors que quand il s'agit de sanctionner les personnes morales, on ajoute une disposition.
L'art. 53 AP-LPD doit donc être supprimé.

***Ad* art. 55 - Prescription de l'action pénale pour les contraventions**
L'art. 55 AP-LPD prévoit que l'action pénale pour les contraventions se prescrit par cinq ans à compter de leur commission.
Or l'art. 109 du Code pénal prévoit un délai de prescription de trois ans.
Il n'y a aucune raison de déroger au délai de trois ans prévu par l'art. 109 du Code pénal. Ce dernier devrait donc s'appliquer tel quel aux contraventions prévues par l'AP-LPD.

***Ad* art. 59 - Disposition transitoire**
Un délai transitoire de deux ans, à l'instar de ce qui est prévu dans l'Union européenne, devrait être prévu, de sorte que les responsables de traitements de données puissent se conformer à leurs nouvelles obligations.

III. Conclusions

L'avant-projet de la loi sur la protection des données doit être clairement remanié. Il va parfois beaucoup plus loin que les exigences internationales, sans que cela ne se justifie. Il occasionne un surcroît de travail pour les entreprises. L'on pense notamment au devoir fortement élargi d'informer et de renseigner tant le Préposé que la personne concernée lors de la collecte des informations.
La mise en pratique et les efforts financiers demandés aux entreprises posent problème. Ces aspects concernent en particulier les PME qui devront mettre en place les procédures requises et rédiger les documents nécessaires.

Les tâches du Préposé vont largement augmenter. Cela va nécessiter également des investissements. A ce sujet, il est intéressant de lire dans le Rapport explicatif[14] que, *à ce stade des travaux, il est difficile d'estimer de manière globale les conséquences financières de l'avant-projet sur le parc personnel de la Confédération et en particulier sur les ressources du Préposé.*

[14] Office fédéral de la justice OFJ, 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 21 décembre 2016, Berne, p. 102

Dans le Rapport explicatif[15], il est indiqué également que *les coûts nécessaires au respect des nouvelles obligations introduites par l'avant-projet pour les responsables du traitement devraient être compensés notamment par les avantages découlant du libre transfert des données avec l'Union européenne*. On admet donc que l'AP-LPD engendrera des coûts, sans toutefois être capable de les chiffrer.

Ceux qui profiteront surtout de cette révision, ce seront les avocats, les experts et les spécialistes en protection des données, enfin ceux qui oseront conseiller les entreprises dans ce champ de mines, vu les sanctions pénales prévues[16].

Enfin, notre Fédération considère que la loi devrait être plus accessible. Le jargon technique devra être simplifié de manière à ce qu'un chef d'entreprise puisse comprendre aisément les obligations qui lui incombent et dans quelles situations celles-ci lui incombent, sans devoir obligatoirement recourir à un expert.
Enfin, cette loi augmente la densité normative, ce qui est hautement regrettable.

Nous vous remercions pour l'attention que vous porterez à ce courrier.

Veuillez croire, Madame la Conseillère fédérale, à l'assurance de notre parfaite considération.

Blaise Matthey
Secrétaire général

Juliette Jaccard
Secrétaire juriste
FER Genève

[15] Office fédéral de la justice OFJ, 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 21 décembre 2016, Berne, p. 104
[16] David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz : Was er bedeutet, in : Jusletter 20 février 2017, p. 44

fga
TV Internet Telefon

Eidg. Justiz- und Polizeidepartement
- 6. April 2017
No.

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

BA Justiz
E - 6. April 2017
Act

31. März 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 fga Fernsehgenossenschaft Aarburg gerne wahr.

fga Fernsehgenossenschaft Aarburg 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

Fernsehgenossenschaft Aarburg ▪ Lindengutstrasse 4 ▪ 4663 Aarburg
Fon: 062 791 06 62 ▪ Fax: 062 791 36 45 ▪ info@fganet.ch ▪ www.fganet.ch

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 an-

---

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.

wesenden 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 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
	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 Voraus*setzungen 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 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
	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.
[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.	**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:	**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 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:	

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. [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. [4] Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten. [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. 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. **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. **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. **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

Thomas Balmer
Präsident fga

Amstutz Jonas BJ

Von: Knecht Liliane <liliane.knecht@fmh.ch>
Gesendet: Dienstag, 4. April 2017 08:47
An: Amstutz Jonas BJ
Betreff: Totalrevision Datenschutzgesetz - Stellungnahme
Anlagen: 170404_FMH-Stellungnahme_Totalrevision-Datenschutzgesetzes.doc

Sehr geehrte Frau Bundesrätin
Sehr geehrter Herr Amstutz

Im Anhang lassen wir Ihnen die Stellungnahme der FMH zur Vernehmlassung über die Totalrevision des Datenschutzgesetzes zukommen.

Wir bedanken uns für die Kenntnisnahme und den Einbezug ins Vernehmlassungsverfahren.

Freundliche Grüsse

Liliane Knecht
Direktionsassistentin
Abteilung Zentrales Sekretariat

FMH

FMH · Verbindung der Schweizer Ärztinnen und Ärzte
Fédération des médecins suisses
Elfenstrasse 18 · Postfach 300 · 3000 Bern 15
Telefon +41 31 359 11 11 · Fax +41 31 359 11 12
liliane.knecht@fmh.ch · www.fmh.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 : FMH Verbindung der Schweizer Ärztinnen und Ärzte

Abkürzung der Firma / Organisation : FMH

Adresse : Postfach 300, 3000 Bern 15

Kontaktperson : Gabriela Lang, Hanspeter Kuhn

Telefon : 031 359 11 11

E-Mail : gabriela.lang@fmh.ch; hanspeter.kuhn@fmh.ch

Datum : 20170404

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
FMH	1. Das Bestreben nach einer Stärkung des Datenschutzes für die Betroffenen ist grundsätzlich zu begrüssen, ebenso die Weiterentwicklung des Datenschutzgesetzes zur Anpassung an die technologischen und gesellschaftlichen Entwicklungen. Es muss allerdings darauf geachtet werden, dass nicht über das Ziel hinaus geschossen wird, was insbesondere bei den Sanktionen von Verletzungen gilt. Zudem ist zu verhindern, dass den Ärzten und Ärztinnen durch die Gesamtrevision weiterer administrativer Mehraufwand entsteht, der bekanntlich tariflich in keiner Weise entschädigt wird. Es ist in besonderem Mass darauf zu achten, dass bei den einer Schweigepflicht unterstehenden Personen keine Friktionen zwischen den Pflichten nach DSG und nach anderen gesetzlichen Vorschriften entstehen. Dies gilt einerseits für

	die Strafbestimmungen (Art. 321 StGB und Art. 50 ff. VE-DSG), aber auch für weiteren beruflichen Pflichten wie beispielsweise die Aufbewahrungspflicht aufgrund gesetzlicher Pflichten. 2. Zu klären ist die Rechtslage bezüglich der Datenerhebungen des Bundes (BFS, BAG) im Gesundheitswesen (MAS, MARS etc.): Im Rahmen von MARS verlangt das BFS vom Leistungserbringer unter anderem die Lieferung von verschlüsselten Personendaten, insbesondere auch von Gesundheitsdaten, die nach dem VE-DSG besonders schützenswerten Personendaten darstellen. Die Verschlüsselung dieser Daten zum Zweck der Weitergabe und insbesondere die Weitergabe der Daten an das BFS stellt eine Bearbeitung von Personendaten gemäss Art. 3 lit. d VE-DSG dar („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;"). Der Arzt muss den Patienten über diese Datenbearbeitung und den Zweck informieren (Art. 4 Abs. 3 und Art. 13 Abs. 1 VE-DSG). Für die Bearbeitung von besonders schützenswerten Personendaten muss der Patient sogar seine ausdrückliche Einwilligung geben (Art. 4 Abs. 6 VE-DSG). Gemäss Art. 3 lit. a VE-DSG sind Personendaten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Wenn es darum geht zu ermitteln, ob die betroffene Person bestimmbar ist, bleibt der VE-DSG bei der durch die bundesgerichtliche Rechtsprechung bestätigten „relativen" Methode. Danach genügt es nicht, dass der Aufwand zur Identifizierung objektiv gering genug ist, dass ein Interessent ihn nach allgemeiner Lebenserfahrung auf sich nimmt. Wesentlich ist ebenso, welches Interesse der Datenbearbeiter oder ein Dritter mit Zugang zu den Daten an der Identifizierung hat, was vom konkreten Fall abhängig ist. (BGE 136 II 508 E. 3.2). Aufgrund des Detaillierungsgrads der vom Arzt an das BFS gelieferten verschlüsselten Daten des einzelnen Patienten (es handelt sich nämlich nicht um gruppierte Daten) ist nicht auszuschliessen, dass je nach Zusatzwissen oder durch zulässige Verknüpfungen des Datenempfängers (BFS, BAG, Versicherer) eine Re- oder direkte Identifizierung des einzelnen Patienten möglich wäre. Die Möglichkeit einer Identifizierung wird dadurch erhöht, dass das BFS die vom Leistungserbringer erhaltenen verschlüsselten Daten gemäss Art. 59a Abs. 3 KVG unter anderem auch den Versicherern je Leistungserbringer zur Verfügung stellen soll. Damit handelt es sich gemäss Art.3 lit. a VE-DSG um Personendaten („Personendaten: alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;") und nicht mehr um verschlüsselte Daten. Dieser Zweck war für die Patienten bei Erhebung der Daten nicht erkennbar (wie es Art. 4 VE-DSG verlangt). Der Arzt konnte die *in der Vergangenheit* behandelten Patienten bei der Datenbeschaffung nicht über diesen Zweck informieren (wie es Art. 13 VE-DSG verlangt), der Zweck der aktuellen Erhebung ist überdies noch nicht deutlich konkretisiert. Auch konnte der Arzt beim Patienten nicht dessen ausdrückliche Einwilligung einholen (wie es Art. 4 Abs. 6 VE-DSG bei besonders schützenswerten Personendaten verlangt). Der Arzt müsste wegen den von ihm nicht verschuldeten Unterlassungen mit strafrechtlichen Sanktionen rechnen. Diese Rechtsunsicherheit muss und darf für den Arzt nicht bestehen. Auch für die in *Zukunft* zu behandelnden Patienten muss geklärt sein, ob der Arzt ihr ausdrückliches Einverständnis für die Datenlieferungen

	bezüglich der Datenerhebungen des Bundes einholen muss. Falls dies bejaht werden sollte, muss geklärt werden, was gilt, wenn der Patient die Einwilligung verweigert. Zudem ist die Übermittlung detaillierter verschlüsselter Patientendaten an den Bund nicht „ausdrücklich im Gesetz" vorgesehen, vgl. dazu den bloss allgemein gehaltenen Art. 23 KVG („Das Bundesamt für Statistik erarbeitet die notwendigen statistischen Grundlagen zur Beurteilung von Funktions- und Wirkungsweise dieses Gesetzes. Es erhebt zu diesem Zweck bei den Versicherern, den Leistungserbringern und der Bevölkerung die notwendigen Daten") und die Formulierung in Art. 59a KVG („Anzahl und Struktur der Patientinnen und Patienten in anonymisierter Form."). Gemäss Art. 27 Abs. 2 VE-DSG brauchen Bundesorgane, welche besonders schützenswerte Personendaten bearbeiten, eine Grundlage dafür in einem Gesetz im formellen Sinn. 3. 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. (David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017, Rz 13) 4. Es ist undiskutabel, dass die schweizerische Gesetzgebung den Anforderungen im europäischen Raum entsprechen muss und die Schweiz ihre Gesetze diesbezüglich anzupassen hat. Eine buchstabengetreue Umsetzung der europäischen Datenschutzregelungen ist jedoch nicht erforderlich, damit die Schweiz auch weiterhin als Staat mit einem «angemessenen Datenschutzniveau» gilt. Verlangt wird lediglich ein angemessener Schutz. Die Befürchtung, dass die Schweiz durch die EU nicht mehr als Staat mit einem «angemessenen Datenschutzniveau» betrachtet werden könnte, scheint doch etwas übertrieben. Die neue DSGVO hält die Kriterien klar fest, wann ein Staat einem «angemessenen Datenschutzniveau» entspricht (vgl. Art. 45 Abs. 2 DSGVO). Hierbei geht es um grundlegende Werte wie Rechtsstaatlichkeit und gelebte Schutzmechanismen, über welche die Schweiz seit Jahrzehnten verfügt. Ausserdem ist die Schweiz seit 6. Mai 1963 Mitglied des Europarates mit entsprechenden Verpflichtungen zur Einhaltung der Grundrechte und des Datenschutzes. Dies wird sich auch in Zukunft nicht ändern. 5. Möchte man «das Verantwortungsbewusstsein der privaten Personen, die Daten bearbeiten, fördern und diese zur Einhaltung nicht verbindlicher Instrumente ermutigen» (wie dies im Begleitschreiben des EJPD steht), müsste das künftige DSG eigentlich weniger streng ausgestaltet sein, als dies mit dem vorliegenden VE-DSG der Fall ist. 6. Der VE-DSG enthält teilweise strengere Bestimmungen als auf europäischer Ebene gefordert (beispielsweise die Umsetzung von Art. 13 – Informationspflicht für die Beschaffung und Art. 17 VE-DSG Meldung von Verletzungen des Datenschutzes). Auf einen teuren Swiss Finish ist zu verzichten.

	7. An die Bearbeitung (u.a. Erhebung, Dokumentation und Weitergabe) der für die medizinische Behandlung notwendigen Informationen darf das Gesetz keine höheren Anforderungen stellen als an die medizinische Behandlung selbst. 8. Die Krankengeschichten werden im Rahmen personalisierter Medizin immer häufiger sowohl genetische Daten wie Daten zum Phänotyp enthalten (Hinweis Prof. J. Blaser, Präsident Schweiz. Gesellschaft für Medizinische Informatik). Für die Medizin ist eine kohärente Regelung der Weiterleitung von Daten an Angehörige und Erben notwendig. Die Revision des DSG ist für diese Fragen mit der Revision des Bundesgesetzes über Genetische Untersuchungen am Menschen GUMG zu koordinieren.[1] . So halten D. Rosenthal und I. Kessler in ihrem Gutachten „Datenschutzrechtliche Aspekte im Rahmen der Totalrevision des GUMG“ vom 18. November 2015 an den Bund fest: *„Die Abgrenzung [des GUMG] zu anderen Gesetzen, die den Umgang mit Informationen über das menschliche Erbgut regeln, ist unzureichend, weil sie Fragen aufwirft. Dieselben Informationen die aus derselben Probe stammen können, können je nach Verwendung unter das GUMG wie auch das Humanforschungsgesetz (HFG) fallen. Im gleichen Zuge ist auch der Anwendungsbereich des GUMG auszuweiten, um nicht nur die Vornahme von Untersuchungen zu erfassen, sondern auch den Umgang mit den dabei entstehenden Daten.“ Wo und wie auch immer die Frage geregelt wird: für den Arzt muss klar sein, welche Grundsätze für die Mitteilung von Daten aus seiner Krankengeschichte an den Patienten, aber an auch an Angehörige und nach seinem Tod an Erben gilt.“* 9. Für die Medizin ist unbedingt zu klären, dass angesichts der bereits bestehenden gesetzlichen Datenbearbeitungs- und Dokumentationspflicht im Gesundheits- und Sozialversicherungsrecht auf eine «Datenschutz-Folgenabschätzungen» gemäss VE-DSG für die KG-Führung bei Behandlung und bei klinischer Forschung (hier sind die Anträge durch die Ethikkommission zu bewilligen und die Forschung ist gemäss HMG zu dokumentieren) verzichtet werden kann. 10. Mitteilung jeder Änderung, Löschung etc. an Dritte Unsinnig und für die Medizin nicht umsetzbar ist die Regelung, wonach im Falle einer jeder 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, es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich. Wer Informationen in der Krankengeschichte korrigiert oder nach Ablauf der gesetzlichen Aufbewahrungsfrist von 10 Jahren die KG-Einträge löscht, darf nicht verpflichtet sein, dies allen nachbehandelnden Gesundheitsfachpersonen mitzuteilen, denen er einen Bericht oder Befund mit dieser Information geschickt hatte. Die Informationspflicht ist auf die Fälle zu begrenzen, in denen die

[1] Der Vorentwurf des GUMG von 2015 sah in Art. 23 Abs. 4 vor: „Wird die Zustimmung [gemeint: vom Patienten um dessen KG es geht] verweigert, kann die Ärztin oder der Arzt bei der zuständigen kantonalen Behörde nach Artikel 321 Absatz 2 des Strafgesetzbuchs die Entbindung vom Berufsgeheimnis beantragen, sofern dies zur Wahrung überwiegender Interessen der Verwandten, der Ehegattin oder des Ehegatten, der Partnerin oder des Partners notwendig ist. Die Behörde kann die Expertenkommission um eine Stellungnahme ersuchen.“

	betroffene Person ein schützenswertes Interesse hat. Mit der Einführung des elektronischen Patientendossiers gemäss EPDG wird zudem die Kommunikation in der Medizin zunehmend *ungerichtet* erfolgen. Dies bedeutet, dass der Arzt, der Daten ins Elektronische Patientendossier des Patienten einstellt, gar nicht wissen wird, welche Gesundheitsfachpersonen aufgrund der vom Patienten erteilten Berechtigungen diese Daten lesen bzw. herunterladen werden. Wenn er diese Information später korrigiert oder löscht, wird er deshalb gar nicht in der Lage sein, die Personen zu erreichen, die die ursprüngliche Information aus dem EPD gelesen oder heruntergeladen haben. 11. Der VE-DSG gibt dem EDÖB Verfügungskompetenz und ausgebaute Untersuchungsmöglichkeiten. Theoretisch führt dies zu einer Stärkung der Stellung. Doch binden diese Verfahren erheblich Ressourcen. Wenn die Politik nicht deutlich mehr Mittel für den EDÖB zur Verfügung stellt, könnte dies dazu führen, dass im Ergebnis die Datenschutzaufsicht weniger erreichen kann als mit den heutigen schlankeren Verfahren (vgl. dazu auch den Hinweis bei Rosenthal, Rz 126). 12. Art. 3 Begriffe; lit. c Ziff. 3 und 4: Ziff. 3 genetische Daten, Ziff. 4 biometrische Daten, die eine natürliche Person eindeutig identifizieren. Es ist zu begrüssen, dass unter den besonders schützenswerten Personendaten neu auch die genetischen und biometrischen Daten, mit welchen eine Person eindeutig identifiziert werden kann, ausdrücklich erwähnt werden. Wie schon die Diskussion zum Vorentwurf der Revision des Bundesgesetzes für die Untersuchung genetischer Daten am Menschen zeigt, ist allerdings die Abgrenzung genetischer von anderen medizinischen Daten schwierig.[2] 13. Zu klären ist der Umgang mit Fotos: Gemäss VE DSG soll jedes Gesichtsfoto als besonders schützenswertes Personendatum gelten. Gemäss Erläuterungen S. 43 soll hingegen Fotos nur dann „unter den Begriff der biometrischen Daten [fallen], wenn sie mit spezifischen

[2] Aus der FMH-Stellungnahme vom 26. Mai 2015 zur Totalrevision des GUMG:
„Neu sollen Untersuchungen von somatischen Eigenschaften (d.h. Erbguteigenschaften, die nicht an Nachkommen weitergegeben werden) den Regelungen des GUMG unter-stellt werden. Dazu zählen auch genetische Untersuchungen, die zur Diagnosestellung, Prognoseabschätzung und Vorhersage eines Therapieansprechens an Tumorzellen durchgeführt werden.
• Diese Ergebnisse bilden die Grundlage einer erfolgreichen Anwendung – sogenannter. gezielter Therapien (targeted therapy) – im Rahmen der personalisierten Medizin bei Krebserkrankungen.
• Die Analyse prädiktiver und prognostischer Marker auf der DNA und RNA Ebene gehört heute zur pathologischen Routinediagnostik von Tumorerkrankungen.
• Die Untersuchungen werden durch den Pathologen in Abhängigkeit von der vorliegenden Erkrankung indiziert und durchgeführt, mit dem Ziel einer sicheren und umfassenden Diagnostik für Patienten.“
Vgl. auch im Gutachten 2015 von Rosenthal/Kessler zur GUMG-Revision (op.cit.) die Empfehlung auf S. 12: „Es ist festzulegen, wann die Regelungen des GUMG auch auf Daten zum Erbgut einer Person Anwendung finden, die nicht im Rahmen des GUMG erhoben wurden oder davon sonst nicht erfasst sind. Die Schnittstellenproblematik besteht allerdings nicht nur im Verhältnis GUMG und HFG, sondern bei jeder vom GUMG nicht erfassten Erhebung genetischer Daten.“

	technischen Mitteln so bearbeitet werden, dass eine eindeutige Identifizierung oder Authentisierung eines Individuums möglich ist". Die Formulierung des Gesetzes sollte dieser Absicht angepasst werden. (so ebenfalls Rosenthal Rz 9) 14. Die Pflicht zur Information und Anhörung der betroffenen Person bei automatisierten individuellen Entscheidungen wird begrüsst (Art. 20 Abs. 2 lit. e und Abs. 3) (zu denken ist z.B. an eine Ablehnung eines Antrags nach einer Datenanalyse mit einem Algorithmus im VVG). 15. Der Verzicht auf die Datenportabilität wird begrüsst. 16. Begrüsst werden die beiden folgenden neuen bzw. ausgeweiteten Strafnormen: • Art. 179novies StGB soll ausgeweitet werden und stellt neu jeden auf Antrag unter Strafe, der «unbefugt» Personendaten beschafft, «die nicht für jedermann zugänglich sind». Die Redaktion des Artikels sollte klarer auf Hacking fokussiert werden.*„… 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. …"* (Rosenthal Rz 122) • In Art. 179decies StGB neu eingeführt werden soll schliesslich eine Bestimmung zur strafrechtlichen Ahndung des Identitätsmissbrauchs. 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. 17. Begrüsst wird die neue Kompetenz des EDÖB, 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). 18. Nicht überzeugend ist dabei hingegen, dass Beschwerden gegen vorsorgliche Massnahmen per se keine aufschiebende Wirkung haben sollen (Art. 44 VE DSG). 19. 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 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). (Rosenthal Rz 124)

	20. Funktion und Aufgaben des Datenschutzverantwortlichen sind im heute geltenden DSG sowie in den aktuellen und künftigen europäischen Datenschutzgesetzen anders geregelt als im VE-DSG. Hier verbleibt wieder eine (unnötige) Unsicherheit, welche weder privaten Organisationen wie Spitälern noch den betroffenen Personen bzw. dem Schutz der Privatsphäre dient. 21. *« 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. »* (Frédéric Erard, Dominique Sprumont, IDS) 22. *« 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. »* (Frédéric Erard, Dominique Sprumont, IDS) 23. Der persönliche, strafrechtliche Charakter der Sanktionen ist unverhältnismässig und widerspricht dem berechtigten heutigen Anspruch an selbstlernende und sichere Unternehmenskulturen und ist ein Rückfall in frühere Zeiten, wo die Barrierenwärterin verurteilt wurde, wenn das Sicherheitsdispositiv der Eisenbahn fehlerhaft war
FMH	

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
FMH	VE DSG	1			**Zweck** Die juristischen Personen sind neu vom Schutzbereich des DSG ausgenommen. Der Schutz des DSG soll jedoch auch in Zukunft für die juristischen Personen gelten. Für Arztpraxen macht es keinen Sinn, zwischen der selbständig erwerbenden Berufstätigkeit des Arztes (für die der Schutz der natürlichen Person gemäss VE-DSG auch für die Arztpraxis greifen würde) und der Berufsausübung in einer als juristischen Person organisierten Arztpraxis (für die der Schutz gemäss DSG entfallen würde) zu unterscheiden. Auch aus gesetzessystematischer Sicht wäre die Unterscheidung nicht konsequent, denn *„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."* (David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017, Rz 5)
FMH	VE-DSG	3		c	**Begriffe** Es ist zu begrüssen, dass unter den besonders schützenswerten Personendaten neu auch die genetischen und biometrischen Daten, mit welchen eine Person eindeutig identifiziert werden kann, ausdrücklich erwähnt werden. Die Umschreibung erscheint uns korrekt.
FMH	VE-DSG	3		f	Das Profiling wird zunehmend wichtiger, auch bei Daten-Verknüpfungen, die in den entsprechenden Gesetzen nicht explizit vorgesehen werden. Indessen ist der Begriff „Profiling" noch ungenügend umschrieben. In der Praxis wird dies den Rechtsanwendern zunehmend Mühe bereiten, insbesondere da an diese Begrifflichkeiten Sanktionen und Rechtfertigungsgründe anknüpfen. Das ist entsprechend zu

					präzisieren. Siehe zum Profiling auch die Ausführungen der FMH zu Art. 4 Abs. 6 VE-DSG.
FMH	VE-DSG	4	3 und 4		**Grundsätze** *„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.“* [Rosenthal Rz 22] Die Pflicht zur Aufbewahrung von Personendaten kann sich nicht nur aus dem Zweck der Bearbeitung, sondern aus anderen Vorschriften ergeben. Die meisten kantonalen Gesundheitsgesetze sehen beispielsweise die Pflicht zur Aufzeichnung und Aufbewahrung während zehn Jahren vor. Dokumente im Laborbereich und für Blut und Blutprodukte haben gar längere Aufbewahrungsfristen. Deshalb ist in Art. 4 Abs. 4 der Vorbehalt von gesetzlichen Vorschriften aufzunehmen, welche die Aufbewahrung konkret regeln.
FMH	VE-DSG	4	6		Art. 4 Abs. 6 VE-DSG sieht vor, dass für die Bearbeitung von besonders schützenswerten Personendaten und das Profiling eine ausdrückliche Einwilligung der betroffenen Person vorliegen muss. Gemäss dem erläuternden Bericht muss eine ausdrückliche Einwilligung durch eine 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. Um Schwierigkeiten im medizinischen Praxisalltag zu vermeiden, ist unbedingt zu klären, wie die Forderung nach einer „ausdrücklichen Einwilligung“ im medizinischen Bereich, in welchem die Einwilligung eines Patienten auch stillschweigend oder konkludent gegeben werden kann, zu verstehen ist. Gemäss Art. 4 Abs. 6 VE-DSG muss eine ausdrückliche Einwilligung auch beim Profiling, ein neu aufgenommener Begriff im DSG, vorhanden sein. Gemäss dem erläuternden Bericht wird das Profiling definiert als jede Auswertung von Personendaten oder nicht-personenbezogenen Daten, um wesentliche

					persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Der VE-DSG führt in Art. 3 lit. f als Beispiele dafür persönliche Merkmale, die analysiert werden können, die Arbeitsleistung, die wirtschaftliche Lage, die Gesundheit, die Intimsphäre oder auch die Mobilität auf. Gemäss David Rosenthal (Rz 7) ist diese Definition extrem weit gefasst, „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." Wenn jede Datenbearbeitung, welche die Analyse oder die Vorhersage von wesentlichen Persönlichkeitsmerkmalen beinhaltet, z.B. die Gesundheit, als ein Profiling betrachtet wird, so fiele jede diagnostische Tätigkeit in der Medizin darunter. Es ist somit zu klären, wie die medizinische Behandlung zu qualifizieren ist. Zudem ist die Koordination mit der Pflicht zur Führung einer Krankengeschichte sicherzustellen. Die Einwilligung zur Behandlung selbst kann ja in der Medizin stillschweigend erteilt werden, und wenn der Patient nicht ansprechbar ist, sind die nötigen Behandlungen durchzuführen – und über die durchgeführten Behandlungen besteht die Aufzeichnungspflicht in den Krankengeschichten gestützt auf Art. 400 OR und die kantonalen Gesundheits- und Spitalgesetze. Insbesondere bei der notfallmässigen Einweisung des Patienten in ein Spital kann die Weitergabe der verfügbaren Informationen lebensrettend sein, doch wird dafür nur die mutmassliche Einwilligung des Patienten vorliegen und keine ausdrückliche. Auch hier gilt: **An die Bearbeitung (u.a. Erhebung, Dokumentation und Weitergabe) der für die medizinische Behandlung notwendigen Informationen darf das Gesetz keine höheren Anforderungen stellen als an die medizinische Behandlung selbst**. Für die Bearbeitung besonders schützenswerter Daten und für das Profiling im Rahmen der Patientenbehandlung ist daher auf die explizite Einwilligung zu verzichten; diese würde die Medizin lähmen und könnte bei nicht ansprechbaren Patienten deren Gesundheit gefährden.
FMH	VE-DSG	6	1	d	**Bekanntgabe ins Ausland in Ausnahmefällen** Es ist zu begrüssen, dass dieser Ausnahmefall ausdrücklich Eingang ins Gesetz findet. Da ein medizinischer Notfall vorliegen muss, kann der Entscheid, ob im konkreten Fall eine Bekanntgabe zulässig ist, den Ärzten überlassen werden. Der Schutz des Betroffenen ist durch die Mitteilung gemäss Abs. 2 gewährleistet.

FMH	VE-DSG	7			**Auftragsdatenbearbeitung** Es besteht ein grundsätzlicher Klärungsbedarf bezüglich der Pflichten, welche der VE-DSG dem Auftragsbearbeiter auferlegt. In der DSGVO werden die Auftragsbearbeiter nicht in gleicher Weise in die Pflicht genommen (z.B. 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."* [Rosenthal Rz 11] Gemäss Art. 7 darf die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen werden, wenn u.a. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. In der Medizin ist zuweilen eine Auftragsdatenbearbeitung notwendig. Insbesondere sollten unseres Erachtens gerade aus Sicherheitsgründen auch Patientendaten georedundant aufbewahrt werden. Sollen die Patienten des Unispitals um Einwilligung gefragt werden, bei welchem Datenbearbeiter die Sicherheitskopie gelagert wird? Der Vorbehalt der gesetzlichen Geheimhaltungspflicht ist vor diesem Hintergrund ein Problem.
FMH	VE-DSG	8			**Empfehlungen der guten Praxis** Die Empfehlungen der guten Praxis, zu erlassen in erster Linie durch den eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, sind ein neues Instrument. Nachvollziehbar ist, dass ein Bedürfnis besteht, die gesetzlichen Vorschriften zu konkretisieren und den Branchenbedürfnissen anzupassen. Dass auch die einzelnen Branchen („interessierten Kreise") selber Empfehlungen ausarbeiten und vom Beauftragten genehmigen lassen können, entspricht diesem Konzept. Allerdings darf nicht übersehen werden, dass diese Empfehlungen zwar grundsätzlich unverbindlich sein sollen, ihnen jedoch in der Praxis eine erhebliche Bedeutung zukommen wird. Das im Gesetz enthaltene Verfahren („Er zieht die interessierten Kreise bei …") reicht aus diesem Grund rechtsstaatlich nicht aus. Es ist im Gegenteil ein formelles Recht auf Wahrung des rechtlichen Gehörs der betroffenen Kreise vorzusehen. Zudem sollen sich auch interessierte Kreise, die vom Beauftragten nicht in ein Anhörungsverfahren einbezogen werden, zu einem in Bearbeitung stehenden Thema unaufgefordert äussern können und ein formelles Recht haben, dass diese Äusserungen vom Beauftragten berücksichtigt werden. Nur so kann gewährleistet

					werden, dass die Interessen sämtlicher von einer Empfehlung Betroffenen rechtzeitig in Empfehlungen einfliessen. Zu klären ist die Rechtslage, wie betroffenen Personen sich wehren können, wenn sie mit einer Datenbearbeitung nicht einverstanden sind, die im Einklang mit einer Empfehlung der guten Praxis vorgenommen wird. Wie David Rosenthal (Rz 108 f.) festhält, *„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. (…) Weil der EDÖB inoffiziell «Beschützer» betroffener Personen ist, werden seine Empfehlungen der guten Praxis „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.“*
FMH	VE-DSG	12	1 und 3		**Daten einer verstorbenen Person** Neu wird vorgesehen, dass ein allfälliges Amts- oder Berufsgeheimnis nicht geltend gemacht werden kann, wenn die Voraussetzungen für die Einsichtnahme nach Art. 12 vorliegen. Unklar ist, ob das Datenschutzgesetz neu dem Strafgesetzbuch vorgehen soll. Wenn dies der Fall wäre, würde das bedeuten, dass bei einer entsprechenden Anfrage nicht mehr eine Entbindung vom Berufsgeheimnis einzuholen wäre. Die Interessenabwägung müsste damit in jedem Fall vom Geheimnisträger (z.B. Arzt) selber vorgenommen werden, ohne dass er sich bei der Aufsichtsbehörde rückversichern könnte. Daraus entsteht das latente Risiko, dass sich ein Ermessensentscheid rückblickend als falsch erweist, was zu empfindlichen Sanktionen für die Auskunft erteilende Person führen kann. Für den ärztlichen Alltag kann sich die Bestimmung in dieser Form als heikel erweisen. Denn Anfragen über die Herausgabe von Daten einer verstorbenen Person haben bekanntlich oft den Zweck der Verfolgung berechtigter oder unberechtigter eigener Interessen. Es kann nicht die Aufgabe eines Arztes sein, in der ihm zur Verfügung stehenden Zeit vertiefte Interessensabklärungen zu treffen. Damit sich die Patienten vorbehaltlos ihrem Arzt anvertrauen können, MUSS das Berufsgeheimnis grundsätzlich auch gegenüber Angehörigen und

					potentiellen Erben gelten, auch nach dem Tod. In unproblematischen Fällen ist nichts dagegen einzuwenden, dass der Arzt die Interessenabwägung selbst vornimmt. Doch muss er die Möglichkeit haben, in für ihn unklaren Fällen oder bei Interessenkonflikten die gemäss Art. 321 StGB zuständige kantonale Behörde entscheiden zu lassen. Der Vorbehalt des Berufsgeheimnisses ist daher auch im Zusammenhang mit der Einsichtnahme in Daten Verstorbener weiterhin vorzusehen bzw. ist Absatz 3 in diesem Sinne wie folgt zu ändern: ~~Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.~~ *Die einem Berufsgeheimnis unterstehende Person kann in Zweifelsfällen den Fall der kant. Behörde gemäss Art. 321 StGB zum Entscheid vorlegen.* Zudem sind in Art. 12 Abs. 1 lit b analog zu Art. 14 Abs. 4 lit. a die überwiegenden eigenen Interessen des Datenverantwortlichen zu ergänzen: b. keine überwiegenden Interessen der verstorbenen Person, ~~oder~~ von Dritten *oder des Verantwortlichen* entgegenstehen. In jedem Fall sind die Regeln des DSG betreffend den Umgang mit Daten verstorbener Personen zu koordinieren mit der Rechtsstellung der Verwandten in der Revision des Bundesgesetzes über genetische Untersuchungen beim Menschen (GUMG), vgl. vorstehend bei den Allgemeinen Bemerkungen Ziff. 8.
FMH	VE-DSG	12	4		Auch beim Antrag des Erben auf Datenlöschung sind die gesetzlichen Aufbewahrungspflichten vorzubehalten. In jedem Fall sind die Regeln des DSG betreffend die Rechte der Erben zu koordinieren mit der Rechtsstellung der Verwandten in der Revision des Bundesgesetzes über genetische Untersuchungen beim Menschen (GUMG), vgl. vorstehend bei den Allgemeinen Bemerkungen Ziff. 8.
FMH	VE-DSG	13			**Informationspflicht bei der Beschaffung von Personendaten** Diese Bestimmung ist strenger als auf europäischer Ebene gefordert (vgl. Entwurf SEV 108 und Richtlinie

					(EU) 2016/680); dies sollte optimiert werden. Die Information gemäss Art. 13 VE-DSG muss nämlich „aktiv“ erfolgen. Dies wird aus europäischer Sicht gar nicht verlangt. So formuliert führt es zu unnötigem Mehraufwand und Kosten sowie einer entsprechenden Informationsflut, was wiederum nicht sachdienlich ist. Die Information hat zudem spätestens bei der Beschaffung, also bei Entgegennahme der Personendaten, zu erfolgen. Auch dieser Zeitpunkt ist eine unnötige zusätzliche Anforderung. Für die Ärzteschaft stellt sich die Frage, was aktive Information in casu bedeutet: reicht eine Info auf der Webseite, Wartesaal etc. oder muss die Ärztin / der Arzt jeden Patienten wirklich aktiv mündlich (Sprechstunde) oder schriftlich (mit Schreiben oder auf der Rechnung) informieren? Das wäre ein administrativer Aufwand, der kaum zu bewältigen wäre. Überdies stellt sich die Frage, was mit all den Patienten passiert, die mit der Weitergabe der eigenen Daten und der damit verbundenen Aushöhlung des Patientengeheimnisses nicht einverstanden sind. Ein erheblicher gesetzlicher Klärungsbedarf besteht bezüglich der Datenerhebungen des Bundes (BFS, BAG) im Gesundheitswesen (MAS, MARS etc.): Im Rahmen von MARS verlangt das BFS vom Leistungserbringer unter anderem die Lieferung von verschlüsselten Personendaten, insbesondere auch von Gesundheitsdaten, die nach dem VE-DSG besonders schützenswerten Personendaten darstellen. Die Verschlüsselung dieser Daten zum Zweck der Weitergabe an das BFS stellt eine Bearbeitung von Personendaten gemäss Art. 3 lit. d VE-DSG dar. Der Arzt muss den Patienten über diese Datenbearbeitung und den Zweck informieren (Art. 4 Abs. 3 und Art. 13 Abs. 1 VE-DSG). Für die Bearbeitung von besonders schützenswerten Personendaten muss der Patient sogar seine ausdrückliche Einwilligung geben (Art. 4 Abs. 6 VE-DSG). Gemäss Art. 3 lit. a VE-DSG sind Personendaten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Wenn es darum geht zu ermitteln, ob die betroffene Person bestimmbar ist, bleibt der VE-DSG bei der durch die bundesgerichtliche Rechtsprechung bestätigten „relativen“ Methode. Danach genügt es nicht, dass der Aufwand zur Identifizierung objektiv gering genug ist, dass ein Interessent ihn nach allgemeiner Lebenserfahrung auf sich nimmt. Wesentlich ist ebenso, welches Interesse der Datenbearbeiter oder ein Dritter mit Zugang zu den Daten an der Identifizierung hat, was vom konkreten Fall abhängig ist. (BGE 136 II 508 E. 3.2). Aufgrund des Detaillierungsgrad der vom Arzt an das BFS gelieferten verschlüsselten Daten des einzelnen Patienten (es handelt sich nämlich nicht um gruppierte Daten) ist nicht auszuschliessen, dass je nach Zusatzwissen oder durch zulässige Verknüpfungen des Datenempfängers (BFS, BAG,

					Versicherer) eine Re- oder direkte Identifizierung des einzelnen Patienten möglich wäre. Die Möglichkeit einer Identifizierung wird dadurch erhöht, dass das BFS die vom Leistungserbringer erhaltenen verschlüsselten Daten gemäss Art. 59a Abs. 3 KVG unter anderem auch den Versicherern je Leistungserbringer zur Verfügung stellt. Damit handelt es sich gemäss Art.3 lit. a VE-DSG um Personendaten („Personendaten: alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;“) und nicht mehr um verschlüsselte Daten. Dieser Zweck war für die Patienten bei Erhebung der Daten nicht erkennbar (wie es Art. 4 VE-DSG verlangt). Der Arzt konnte die Patienten bei der Datenbeschaffung nicht über diesen Zweck informieren (wie es Art. 13 VE-DSG verlangt), der Zweck der aktuellen Erhebung ist überdies noch nicht deutlich konkretisiert. Auch konnte der Arzt beim Patienten nicht dessen ausdrückliche Einwilligung einholen (wie es Art. 4 Abs. 6 VE-DSG bei besonders schützenswerten Personendaten verlangt). Der Arzt müsste wegen den von ihm nicht verschuldeten Unterlassungen mit strafrechtlichen Sanktionen rechnen. Diese Rechtsunsicherheit muss und darf für den Arzt nicht bestehen. Zudem ist die Übermittlung detaillierter verschlüsselter Patientendaten an den Bund nicht „ausdrücklich im Gesetz“ vorgesehen, vgl. dazu den bloss allgemein gehaltenen Art. 23 KVG („Das Bundesamt für Statistik erarbeitet die notwendigen statistischen Grundlagen zur Beurteilung von Funktions- und Wirkungsweise dieses Gesetzes. Es erhebt zu diesem Zweck bei den Versicherern, den Leistungserbringern und der Bevölkerung die notwendigen Daten“) und die Formulierung in Art. 59a KVG („Anzahl und Struktur der Patientinnen und Patienten in anonymisierter Form.“). Gemäss Art. 27 Abs. 2 VE-DSG brauchen Bundesorgane, welche besonders schützenswerte Personendaten bearbeiten, eine Grundlage dafür in einem Gesetz im formellen Sinn.
FMH	VE-DSG	13	2 und 5		*„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.“ [Rosenthal Rz 46] Des Weiteren wird in Art. 13 Abs. 2 lit. b VE-DSG in der „oder-Formulierung“ von Kategorien der bearbeiteten Personendaten gesprochen. Die Formulierung „Kategorie“ erinnert an die Schwammigkeit von Art. 59a KVG. Beim Auskunftsrecht in Art. 20 Abs. 2 hingegen, kann die Person unter lit. b die bearbeiteten Personendaten einsehen – hier wird nicht mehr von Kategorien gesprochen. Es bleibt aber eine aktive Pflicht der betroffenen Person. Es wird kaum möglich sein, alle Daten genau zu benennen, um der Informationspflicht nach Art. 13 gesetzeskonform nachzukommen. Gemäss Art. 13 Abs. 5 VE-DSG muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden, wenn die Personendaten nicht bei der betroffenen Person beschafft werden. Damit würde jede Fremdanamnese in der Medizin verunmöglicht. Auch die Konsultation des EPD ist eine Datenbeschaffung bei Dritten, bei der der Patient nicht in jedem Fall vorgängig informiert werden kann. Der VE-DSG geht auch hier über die europäische Verordnung hinaus, die eine Monatsfrist für die Mitteilung vorsieht.
FMH	VE-DSG	14			**Ausnahmen von der Informationspflicht** Der Leistungserbringer ist im Umfeld von gesetzlich vorgeschriebenen Datenbearbeitungen im Gesundheits- oder Sozialversicherungsrecht von den Verpflichtungen, was die Information gegenüber dem Patienten anbelangt, ausdrücklich auszunehmen.
FMH	VE-DSG	15			**Automatisierte Einzelentscheidung ist zu weit gefasst** Es ist nicht ersichtlich, warum im VE-DSG ohne Einschränkung auch besonders schützenswerte Personendaten und Daten von Kindern entsprechend bearbeitet werden dürfen.

FMH	VE-DSG	16			**Datenschutz-Folgenabschätzung** Die Pflicht des Verantwortlichen (bzw. des Auftragsbearbeiters) eine Datenschutz-Folgenabschätzung durchzuführen, wenn die vorgesehene Datenbearbeitung „voraussichtlich zu einem erhöhten Risiko“ für die Persönlichkeit oder die Grundrechte der betroffenen Person führt sowie die Pflicht, den EDÖB über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen zu informieren, bedarf für die Ärzteschaft einer Klärung. Gemäss Erläuterungen soll die Bearbeitung von besonders schützenswerten Personendaten oder ein Profiling bereits Indiz für ein «erhöhtes» Risiko sein. Da die Ärzteschaft mit besonders schützenswerten Daten zu tun hat, ist wohl davon auszugehen, dass diese diese Bestimmung auf die Ärzteschaft zur Anwendung kommen würde. Für die Medizin ist deshalb unbedingt zu klären, dass angesichts der bereits bestehenden gesetzlichen Datenbearbeitungs- und Dokumentationspflicht im Gesundheits- und Sozialversicherungsrecht auf eine «Datenschutz-Folgenabschätzungen» gemäss VE-DSG für die KG-Führung bei Behandlung und bei klinischer Forschung (hier sind die Anträge durch die Ethikkommission zu bewilligen und die Forschung ist gemäss HMG zu dokumentieren) verzichtet werden kann. Ungeeignet erscheint weiter, dass gemäss Vorentwurf nicht nur der Verantwortliche die Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung trifft, sondern auch den Auftragsbearbeiter. Letzter wird aber in der Regel gar nicht in der Lage dazu sein und es ist auch nicht seine Aufgabe. [Rosenthal Rz 86]
FMH	VE-DSG	17			**Meldung von Verletzungen des Datenschutzes** Auch diese Bestimmung ist strenger als auf europäischer Ebene gefordert (vgl. Entwurf SEV 108 und Richtlinie (EU) 2016/680): Eine Meldung soll gemäss Art. 17 VE-DSG bei jeglicher (!) unbefugten Datenbearbeitung oder Verlust von Daten erfolgen. Auf europäischer Ebene beschränkt sich die Meldung an die Datenschutzbehörden auf «Verstösse gegen die Datensicherheit» (vgl. Art. 7 Abs. 2 Entwurf SEV 108). Ausserdem ist Art. 17 VE-DSG zu unklar formuliert: - Was bedeutet «Risiko»? In der Richtlinie (EU) 2016/680 ist zumindest von einem «hohen Risiko»

					für die Rechte und Freiheiten natürlicher Personen die Rede. - Wann spricht man von einem «Verlust von Daten»? Betrifft dies z.B. auch aus Versehen gelöschte Daten? David Rosenthal bringt in seinem Beitrag die Folgen dieser Meldepflicht auf den Punkt: *„Die im Vorentwurf vorgesehene Meldepflicht bringt 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, da der EDÖB seinerseits eine Anzeigepflicht hat. 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).“* [Rosenthal Rz 97] Aus Sicht der FMH ist in der Medizin eine angstfreie Kommunikation zwischen den Mitarbeitern und dem internen Datenschutzverantwortlichen der Institution Voraussetzung für einen möglichst wirksamen Datenschutz. Sinnvoll erscheint zudem, wie David Rosenthal vorschlägt, *„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.“* (Rosenthal Rz 98) *„Die Meldepflicht sollte zudem in zeitlicher Hinsicht relativiert werden. Statt einer «unverzüglichen » Meldung sollte eine Meldung ohne unnötigen Verzug stattfinden.“* [Rosenthal Rz 99]
FMH	VE-DSG	19	3		**Weitere Pflichten - Mitteilung jeder Änderung, Löschung etc. an Dritte** Der Leistungserbringer ist im Umfeld von gesetzlich vorgeschriebenen Datenbearbeitungen und

					Dokumentationspflichten im Gesundheits- oder Sozialversicherungsrecht von den weiteren Pflichten ausdrücklich auszunehmen. Unsinnig und für die Medizin nicht umsetzbar ist die Regelung, wonach im Falle *jeder* 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, es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich. Wer Informationen in der Krankengeschichte korrigiert oder nach Ablauf der Aufbewahrungsfrist von 10 Jahren die KG-Einträge löscht, darf nicht verpflichtet sein, dies allen nachbehandelnden Gesundheitsfachpersonen mitzuteilen, denen man gestützt auf die nun gelöschten Daten einen Bericht oder Befund geschickt hatte. Die Informationspflicht ist auf die Fälle zu begrenzen, in denen die betroffene Person ein schützenswertes Interesse hat. Mit der Einführung des elektronischen Patientendossiers gemäss EPDG wird zudem die Kommunikation in der Medizin zunehmend *ungerichtet* erfolgen. Dies bedeutet, dass der Arzt, der Daten ins Elektronische Patientendossier des Patienten einstellt, gar nicht wissen wird, welche Gesundheitsfachpersonen aufgrund der vom Patienten erteilten Berechtigungen diese Daten lesen bzw. herunterladen werden. Wenn er diese Information später korrigiert oder löscht, wird er deshalb gar nicht in der Lage sein, die Personen zu erreichen, die die ursprüngliche Information aus dem EPD gelesen oder heruntergeladen haben. *„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.“* [Rosenthal Rz 69]
FMH	VE-DSG	20	1		**Kostenloses Auskunftsrecht** Das Auskunftsrecht ist grundsätzlich kostenlos. Während in der bisherigen Fassung des Artikels über das

					Auskunftsrecht vorgesehen war, dass der Bundesrat die Ausnahmen regelt, enthält der Vorentwurf diese Möglichkeit nicht mehr. Gemäss Art. 2 der VO DSG kann unter anderem dann eine angemessene Kostenbeteiligung verlangt werden, wenn die Auskunftserteilung mit einem besonders grossen Arbeitsaufwand verbunden ist. Der Bundesrat soll auch weiterhin Ausnahmen von der Kostenlosigkeit vorsehen können, weshalb Art. 20 Abs. 1 entsprechend zu ergänzen ist. Dies ist gerade in Fällen wichtig, wo Fotokopien von Dokumenten zur Herausgabe erstellt werden müssen, die (noch) nicht elektronisch vorhanden sind. David Rosenthal hält in Rz 57 zur im Vorentwurf vorgesehenen ausnahmslosen Kostenlosigkeit fest: *"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."*
FMH	VE-DSG	20	3		**Auskunftsrecht – Entscheidungen, insb. automatisierte Einzelfallentscheidungen** Auch diese Bestimmung ist strenger als auf europäischer Ebene gefordert (vgl. Entwurf SEV 108 und Richtlinie (EU) 2016/680): Art. 20 Abs. 3 – Auskunftsrecht bzgl. «Entscheidungen» (insb. automatisierte Einzelfallentscheidungen) VE-DSG fordert umfassende Erklärungspflichten für den Verantwortlichen (z.B. Arzt, Arztpraxis, Spital). Dies geht ebenfalls weiter als erforderlich und bedeutet einen entsprechenden Mehraufwand.
FMH	VE-DSG	21			**Einschränkung des Auskunftsrechts – persönliche Notizen** Der Verantwortliche kann gemäss Art. 21 Absatz 1 VE-DSG die Auskunft unter den Voraussetzungen nach Artikel 14 Absätze 3 und 4 des VE verweigern, einschränken oder aufschieben. Falls der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies gemäss Absatz 2 entsprechend begründen. Als Gründe kommen grundsätzlich nur die Voraussetzungen nach Artikel 14 Absätze 3 und 4 in Frage. […]. Aufgrund der Begründung muss die betroffene Person überprüfen können, ob die Auskunft zu Recht

					verweigert, eingeschränkt oder aufgeschoben worden ist. Von Arztseite her wird gewünscht, die Rechtslage bezüglich persönlicher Notizen des Arztes zu klären; gewisse kantonale Gesundheits- oder Spitalgesetze räumen dem Patienten ein grundsätzliches Auskunftsrecht ein, nehmen aber die persönlichen Notizen des Arztes davon aus (z.B. Art. 55 As. 2 LSanté GE, und diverse andere Gesundheits- und Spitalgesetze).
FMH	VE-DSG	25	1	c	**Klagen zum Schutz der Persönlichkeit: Löschung oder Vernichtung von Personendaten** Für die Medizin ist wichtig zu klären, wie dieser Löschungsanspruch mit der Pflicht zur Führung einer Krankengeschichte, mit der in den meisten kantonalen Gesundheitsgesetzen vorgesehenen Aufbewahrungsfristen und im Spital mit der Pflicht zum Angebot eines Elektronischen Patientendossier zu koordinieren ist. Zudem ist darauf hinzuweisen, dass im Zeitalter der elektronischen Krankengeschichten eine Löschung technisch oft nicht möglich ist: die Löschung wird als solche im System dokumentiert.
FMH	VE-DSG	50 ff.			**Strafbestimmungen** Die Strafbestimmungen sind zu ungenau formuliert (Art. 50 ff. VE-DSG). Zum Beispiel in Bezug auf die «Datenschutz-Folgenabschätzung» (Art. 16 VE-DSG): «Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit…» - Was bedeutet «voraussichtlich»? - Was bedeutet «erhöht»? - Aber: Busse bis CHF 500'000.- sollte keine Datenschutz-Folgenabschätzung vorgenommen worden sein (Art. 51 Abs. 1 Bst. d VE-DSG). Dies widerspricht dem Grundsatz «nulla poena sine lege» (keine Strafe ohne Gesetz bzw. keine Strafe bei unklaren Bestimmungen). Keine Verwaltungsbussen durch den EDÖB, jedoch strafrechtliche Sanktionen gegen einzelne verantwortliche natürliche Personen:

					- anders als in den neuen europäischen Datenschutzbestimmungen hat der VE-DSG in erster Linie die verantwortlichen «natürlichen Personen» für strafrechtliche Sanktionen im Visier, statt Unternehmen bzw. Institutionen (juristische Personen). - Warum? Offenbar aufgrund fehlender Ressourcen beim EDÖB. Dies kann kein ernsthaftes Argument sein und ist keineswegs zielführend. - Der persönliche, strafrechtliche Charakter der Sanktionen ist unverhältnismässig und widerspricht dem berechtigten heutigen Anspruch an selbstlernende und sichere Unternehmenskulturen und ist ein Rückfall in frühere Zeiten, wo die Barrierenwärterin verurteilt wurde, wenn das Sicherheitsdispositiv der Eisenbahn fehlerhaft war.[3] David Rosenthal hält die möglichen Auswirkungen des persönlichen, strafrechtlichen Charakters der Sanktionen eindrücklich fest: *„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, 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.“* [Rosenthal Rz 116] *„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.“* [Rosenthal Rz 117]

[3] Martin Schubarth. Sicherheitsdispositiv und strafrechtliche Verantwortlichkeit im Eisenbahnverkehr, SJZ 1996 S. 37-41. Siehe auch Schubarth, Kommentar I zum StGB, 1982, Art. 117, N.2: „Bestraft werden, mangels eines individuellen konkreten Schuldvorwurfs oder auch aus Bequemlichkeit der Strafverfolgungsbehörden dagegen diejenigen nicht, die durch unzweckmässige Dispositionen zu unfallträchtigen Situationen beigetragen haben.“

FMH	VE-DSG	50			**Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten** Der Vorentwurf DSG sieht generell bei Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten eine massive Erhöhung der möglichen Bussen vor, von bisher CHF 10‘000.00 (106 Abs. 1 StGB) auf bis zu CHF 500‘000.00 bei vorsätzlicher Tatbegehung bzw. bis CHF 250‘000.00 bei fahrlässiger Tatbegehung. Dagegen ist grundsätzlich nichts einzuwenden, da das DSG damit mehr Biss erhält. Allerdings muss zwischen vorsätzlicher und fahrlässiger Tatbegehung deutlich stärker unterschieden werden. . Angesichts der auf den einzelnen Mitarbeiter gerichteten Strafdrohung mussdie mögliche Bussenhöhe bei Fahrlässigkeit viel tiefer angesetzt werden als bis CHF 250‘000.00 Zum Vergleich: Die fahrlässige Verletzung des Amts-, Anwalts- oder Arztgeheimnisses (Art. 321 StGB) ist nicht strafbar. Aufgrund der Bussenerhöhungen ist es zudem umso wichtiger, die Pflichten konkret zu klären (siehe vorne zu klärende Frage).
FMH	VE-DSG	51			**Verletzung der Sorgfaltspflichten** Es muss zwischen vorsätzlicher und fahrlässiger Tatbegehung deutlich stärker unterschieden werden, siehe oben bei Art. 50.
FMH	VE-DSG	52			**Verletzung der beruflichen Schweigepflicht** Die Strafdrohung gemäss DSG sollte tiefer bleiben als Art. 321 StGB um die besondere Vertrauenswürdigkeit dieser Berufe klar zu positionieren.
FMH	VE-DSG	55			**Verfolgungsverjährung für Übertretungen** Die Verfolgungsverjährungsfrist bei Übertretungen beträgt gemäss Art. 109 StGB 3 Jahre. Es sind keine sachlichen Gründe ersichtlich, weshalb sie beim Datenschutz 5 Jahre betragen soll. Es ist daher aus Gründen der Rechtssicherheit nach dem allgemeinen Massstab des StGB von einer Verjährungsfrist von 3 Jahren auszugehen.

FMH	VE-DSG	59			**Übergangsbestimmung** Eine Übergangsfrist von zwei Jahren nach Inkrafttreten des DSG wird nur gewährt für: - die Einführung einer Datenschutz-Folgeabschätzung gemäss Art. 16 VE-DSG; - für die Erstellung der Dokumentation der zum Zeitpunkt des Inkrafttretens des revidierten DSG bereits bestehenden Datenbearbeitungen (Art. 19 VE-DSG); - die Einführung des „Privacy by Default“ und „Privacy by Design“ für zum Zeitpunkt des Inkrafttretens des revidierten DSG bereits bestehenden Datenbearbeitungen (Art. 18 VE-DSG). Weshalb die Übergangsfrist nur auf diese Bestimmungen beschränkt ist, ist nicht nachvollziehbar. Sinnvoller wäre es, eine Übergangsfrist von zwei Jahren für die Umsetzung des ganzen DSG vorzusehen. Auch die DSGVO sieht eine generelle Übergangsfrist von zwei Jahren für alle Bestimmungen vor. (vgl. Rosenthal Rz 127-129)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Forum PME
KMU-Forum
Forum PMI

CH-3003 Berne, Forum PME

Par courriel

jonas.amstutz@bj.admin.ch
Office fédéral de la justice
Bundesrain 20
3003 Berne

Spécialiste: mup
Berne, 04.04.2017

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

Madame, Monsieur,

Notre commission extraparlementaire s'est penchée, lors de sa séance du 23 février 2017, sur l'avant-projet de révision totale de la loi sur la protection des données (LPD). Nous remercions Mme Monique Cossali de votre office d'avoir participé à cette séance et d'y avoir présenté les différents aspects du projet. Conformément à son mandat, notre commission l'a examiné du point de vue des petites et moyennes entreprises (PME).

Tout comme le Conseil fédéral, les membres de notre commission sont favorables à l'adoption de mesures susceptibles de moderniser les dispositions légales de protection des données, afin de faire face au développement fulgurant des nouvelles technologies. Il s'agit non seulement de protéger la personnalité et les droits fondamentaux des personnes dont les données font l'objet de traitements, mais également de maintenir et de renforcer la compétitivité de la Suisse, en créant un environnement propre à faciliter les flux transfrontières de données et en favorisant l'émergence de nouvelles activités économiques en lien avec la société numérique. Les données constituent la matière première d'une économie et d'une société numériques, nous sommes pour cette raison de l'avis que **notre pays devrait se positionner comme un lieu attractif pour la création de valeur au moyen des données**.

Nous craignons cependant que le projet mis en consultation ne permette pas d'atteindre ce but de manière satisfaisante. Les nouvelles dispositions proposées risquent à notre avis de compliquer à l'excès, par de nombreuses obligations et charges administratives, la tâche des entreprises concernées, en particulier celle des PME. Les coûts auxquels ces dernières devront faire face sont à notre avis trop importants. Vous trouverez, dans le formulaire ci-joint, nos commentaires de détail et nos demandes d'adaptations concernant les différentes dispositions concernées. Notre commission est de l'avis, de manière générale, qu'**aucune nouvelle obligation ne devrait être introduite dans la LPD, si elle n'est pas absolument nécessaire en vue de garantir le maintien par l'UE de sa décision de reconnaissance**

Forum PME
Holzikofenweg 36, 3003 Berne
Tél. +41 58 464 72 32, Fax +41 58 463 12 11
kmu-forum-pme@seco.admin.ch
www.forum-pme.ch

de l'adéquation de notre réglementation dans ce domaine (qui garantit le libre accès au marché européen). **Nous sommes opposés à tout swiss finish** ayant pour conséquence une augmentation des charges administratives et coûts pour les entreprises suisses, auxquels les entreprises européennes ne sont pas confrontées. Nous demandons pour cette raison que les règles et notions plus simples développées dans l'UE soient reprises telles quelles dans notre ordre juridique, en particulier en ce qui concerne le profilage. Notre commission estime par ailleurs que des exigences différenciées devraient autant que possible être prévues, en fonction du type et de la taille des entreprises. Il s'agira en particulier de prévoir une réglementation davantage différenciée et allégée pour les petites et moyennes entreprises (cf. nos propositions concernant les art. 16 et 19 AP-LPD).

Le projet mis en consultation est très vaste. Il est difficile d'en appréhender, même après un examen approfondi des dispositions et du rapport explicatif, tous ses enjeux. Le degré élevé de complexité et le caractère technique de la matière nécessitent à notre avis une analyse encore plus poussée des différents impacts de la révision. Notre commission a reçu, en 2011, le mandat exprès du Conseil fédéral[1] de vérifier, lors de procédures de consultation, que les offices aient procédé, lors de l'élaboration de projets législatifs, à une mesure des coûts de la réglementation ainsi qu'à une analyse de leur compatibilité PME (du point de vue des charges administratives, etc.). Nous saluons le fait que votre office ait réalisé une analyse d'impact de la réglementation approfondie, en collaboration avec le SECO, sur ce sujet complexe. Nous vous rendons cependant attentifs au fait que **les informations figurant actuellement dans le rapport explicatif sont en partie insuffisantes**. Le chapitre sur les conséquences économiques du message devra contenir des informations détaillées et chiffrées concernant les impacts de la révision sur les différents groupes concernés[2], notamment sur les intermédiaires financiers, les fiduciaires, les avocats et notaires, les services informatiques, l'industrie pharmaceutique et biotechnologique, les professions médicales, etc.

Plusieurs nouvelles règles et notions sont introduites dans l'avant-projet, sans que leur signification ne soit toujours clairement fournie dans le rapport explicatif. Certaines de ces nouvelles notions, qui ont été introduites en vue d'adapter notre réglementation à celle de l'UE, ne sont, paradoxalement, pas identiques à celles du Règlement général sur la protection des données de l'Union européenne (RGPD). **Les explications figurant dans le rapport explicatif ne répondent pas à toutes les questions qui se posent**, en particulier en ce qui concerne le devoir d'informer et le type de consentement requis lors du traitement de données en cas de profilage. Nous demandons pour cette raison que le texte du rapport explicatif soit complété et que le futur message contienne des informations beaucoup plus détaillées afin de réduire l'insécurité juridique pour les entreprises et autres acteurs concernés.

En ce qui concerne la définition du champ d'application de la loi révisée, nous sommes de l'avis que **le Législateur devrait opter plus clairement pour le principe de primauté des lois spéciales** et demandons que le texte de l'article 2 précise quels seront les rapports de la future loi révisée avec les réglementations spéciales (comme p.ex. la loi relative à la recherche sur l'être humain et ses ordonnances). Les indications fournies dans le rapport explicatif contredisent en partie ce principe et sont susceptibles d'avoir des impacts très négatifs

---

[1] Mesure 2 du rapport du Conseil fédéral du 24.08.2011 "Allégement administratif des entreprises: bilan 2007-2011 et perspectives 2012-2015".

[2] Conformément au point 3.2 des directives du Conseil fédéral du 15.09.1999 sur l'exposé des conséquences économiques des projets d'actes législatifs fédéraux.

sur certaines activités économiques en Suisse, comme par exemple sur l'industrie pharmaceutique et biotechnologique ou sur les intermédiaires financiers (cf. nos explications y-relatives dans le formulaire).

Dans ce contexte de grande insécurité juridique, **nous sommes opposés au renforcement des dispositions pénales**, dont les montants proposés vont jusqu'à 250'000 francs en cas d'infraction commise par négligence. Les entreprises seront, dans ces conditions, ne sachant pas exactement ce qu'elles doivent faire, obligées de prendre de nombreuses mesures superflues (et inutiles du point de vue de la protection des données), afin de se prémunir contre d'éventuelles poursuites pénales. Les coûts de la réglementation devraient par conséquent être très élevés et dépasser les bénéfices escomptés. **Nous demandons pour cette raison qu'un système de sanctions administratives à l'encontre des entreprises soit prévu, comme dans l'UE, en lieu et place des sanctions pénales** prévues aux articles 50 ss du projet (qui, quant à elles, vont principalement à l'encontre des personnes physiques). Alternativement, nous demandons qu'en cas d'infractions commises par négligence, aucune amende ne soit prévue, à l'instar de la réglementation actuellement en vigueur.

Espérant vivement que nos recommandations seront prises en compte, nous vous prions d'agréer, Madame, Monsieur, nos meilleures salutations. Nous nous tenons volontiers à votre disposition pour toute question éventuelle.

Jean-François Rime
Co-Président du Forum PME
Conseiller national

Dr. Eric Jakob
Co-Président du Forum PME
Ambassadeur, Chef de la promotion économique du Secrétariat d'Etat à l'économie

Copie à:

Commissions des affaires juridiques du Parlement

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 : **Commission extraparlementaire « Forum PME »**

Abréviation de la société / de l'organisation : Forum PME

Adresse : Holzikofenweg 36, 3003 Berne

Personne de référence : M. Pascal Muller, secrétaire de la commission

Téléphone : 058 464 72 32

Courriel : kmu-forum-pme@seco.admin.ch

Date : 04.04.2017

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

Remarques générales 3

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 5

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 9

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel 9

Rapport explicatif (excepté chap. 8 « Commentaire des dispositions») 10

Rapport explicatif : chap. 8 « Commentaire des dispositions » 10

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 :
Forum PME	Tout comme le Conseil fédéral, les membres de notre commission sont favorables à l'adoption de mesures susceptibles de moderniser les dispositions légales de protection des données, pour faire face au développement fulgurant des nouvelles technologies. Il s'agit non seulement de protéger la personnalité et les droits fondamentaux des personnes dont les données font l'objet de traitements, mais également de maintenir et de renforcer la compétitivité de la Suisse, en créant un environnement propre à faciliter les flux transfrontières de données et en favorisant l'émergence de nouvelles activités économiques en lien avec la société numérique. Les données constituent la matière première d'une économie et d'une société numériques. Nous sommes pour cette raison de l'avis que **notre pays devrait se positionner comme un lieu attractif pour la création de valeur au moyen des données**. Nous craignons cependant que le projet mis en consultation ne permette pas d'atteindre ce but de manière satisfaisante. **Les nouvelles dispositions proposées risquent à notre avis de compliquer à l'excès, par de nombreuses obligations et charges administratives, la tâche des entreprises concernées, en particulier celle des PME**. Les coûts auxquels ces dernières devront faire face sont à notre avis trop importants. Notre commission est de l'avis, de manière générale, qu'**aucune nouvelle obligation ne devrait être introduite dans la LPD, si elle n'est pas absolument nécessaire en vue de garantir le maintien par l'UE de sa décision de reconnaissance de l'adéquation de notre réglementation** dans ce domaine (qui garantit le libre accès au marché européen). **Nous sommes opposés à tout swiss finish** ayant pour conséquence une augmentation des charges administratives et coûts pour les entreprises suisses (auxquels les entreprises européennes ne sont pas confrontées). Nous demandons pour cette raison que les règles et notions plus simples développées dans l'UE soient reprises telles quelles dans notre ordre juridique, en particulier en ce qui concerne le profilage (cf. infra nos demandes y-relatives). Notre commission estime par ailleurs que **des exigences différenciées devraient autant que possible être prévues**, en fonction du type et de la taille des entreprises. Il s'agira en particulier de prévoir une réglementation davantage différenciée et allégée pour les petites et moyennes entreprises (cf. nos propositions concernant les art. 16 et 19 AP-LPD).
Forum PME	Le projet mis en consultation est très vaste. Il est difficile d'en appréhender, même après un examen approfondi des nouvelles dispositions et du rapport explicatif, tous ses enjeux. Le degré élevé de complexité et le caractère technique de la matière nécessitent à notre avis une analyse encore plus poussée des différents impacts de la révision. Nous saluons le fait que votre office ait réalisé une analyse d'impact de la réglementation approfondie, en collaboration avec le SECO, sur ce sujet complexe. Nous vous rendons cependant attentifs au fait que **les**

	informations figurant actuellement dans le rapport sont en partie insuffisantes. Le chapitre sur les conséquences économiques du message devra contenir des informations détaillées et chiffrées concernant les impacts de la révision sur les différents groupes concernés[1], notamment sur les intermédiaires financiers, les fiduciaires, les avocats et notaires, les services informatiques, l'industrie pharmaceutique et biotechnologique, les professions médicales, etc. Plusieurs nouvelles règles et notions sont introduites dans l'avant-projet, sans que leur signification ne soit toujours clairement fournie dans le rapport explicatif. Certaines de ces nouvelles notions, qui ont été introduites en vue d'adapter notre réglementation à celle de l'UE, ne sont, paradoxalement, pas identiques à celles du Règlement général sur la protection des données de l'Union européenne (RGPD). **Les explications figurant dans le rapport explicatif ne répondent pas à toutes les questions qui se posent**, en particulier en ce qui concerne le devoir d'informer et le type de consentement requis lors du traitement de données en cas de profilage. Nous demandons pour cette raison que le texte du rapport explicatif soit complété et que le futur message contienne des informations beaucoup plus détaillées afin de réduire l'insécurité juridique pour les entreprises et autres acteurs concernés.
Forum PME	En ce qui concerne la définition du champ d'application de la loi révisée, nous sommes de l'avis que **le Législateur devrait opter plus clairement pour le principe de primauté des lois spéciales** et demandons que le texte de l'article 2 précise quels seront les rapports de la future loi révisée avec les réglementations spéciales (comme p.ex. la loi relative à la recherche sur l'être humain et ses ordonnances). Les indications fournies dans le rapport explicatif contredisent en partie ce principe et sont susceptibles d'avoir des impacts très négatifs sur certaines activités économiques en Suisse, comme par exemple sur l'industrie pharmaceutique et biotechnologie ou sur les intermédiaires financiers (cf. infra nos explications y-relatives).
Forum PME	Dans ce contexte de grande insécurité juridique, **nous sommes opposés au renforcement des dispositions pénales**, dont les montants proposés vont jusqu'à 250'000 francs en cas d'infraction commise par négligence. Les entreprises seront sinon, dans ces conditions, obligées de prendre de nombreuses mesures superflues (et inutiles du point de vue de la protection des données), afin de se prémunir contre d'éventuelles poursuites pénales ; les coûts de la réglementation seront dans ce cas très élevés et dépasseront les bénéfices escomptés.

[1] Conformément au point 3.2 des directives du Conseil fédéral du 15.09.1999 sur l'exposé des conséquences économiques des projets d'actes législatifs fédéraux.

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 :
Forum PME	LPD	1			<u>But de la loi :</u> nous demandons que le texte de l'article 1 AP-LPD soit complété par le deuxième alinéa suivant : *En outre* [la loi]*, elle poursuit les buts suivants:* *a. aménager des conditions favorables à l'émergence de nouvelles activités économiques en lien avec la société numérique;* *b. faciliter les flux transfrontières de données.*
Forum PME	LPD	2			<u>Champ d'application / autre droit applicable :</u> nous demandons que le texte de l'article 2 (et celui du message) précisent quels seront les rapports de la future LPD révisée avec les lois et ordonnances spéciales (comme par exemple la loi relative à la recherche sur l'être humain et ses ordonnances). Nous demandons que le texte de l'article 2 soit, dans cette optique, complété par l'alinéa 5 suivant : *« Sont réservées les dispositions spéciales d'autres lois et ordonnances fédérales ».* Selon la doctrine et la jurisprudence du Tribunal fédéral, il n'est pas exclu qu'une règle spéciale cède le pas à une règle générale, selon sa place dans l'ordre juridique, la date de son adoption ou encore les intentions de ses auteurs. Il est pour cette raison nécessaire que le Législateur fournisse autant que possible des indications claires concernant ces relations. Nous sommes de l'avis que le Législateur devrait opter pour le principe « *lex specialis derogat generali* » et non pour le principe « *lex posterior derogat anteriori* ». Ce principe a pour conséquence que les normes relatives à la protection des données contenues dans d'autres réglementations trouvent pleine et entière application, qu'elles aient été adoptées avant ou après l'entrée en vigueur de la LPD révisée. Les indications fournies à la page 37 du rapport explicatif (en relation avec le postulat Béglé 16.3384) contredisent en partie ce principe de primauté des lois spéciales. Elles mentionnent notamment que : « *L'AP prévoit toute une série de nouvelles obligations à charge du responsable du traitement et du sous-traitant qui s'appliqueront donc aussi aux données médicales (art. 13, 15, 16, 17, 18 et 19)* ». Les règles de la loi relative à la recherche sur l'être humain doivent à notre avis absolument garder leur primauté, raison pour laquelle nous vous demandons de corriger les indications figurant à la p. 37. Une modification

					des règles en la matière est susceptible d'entraver gravement la recherche sur l'être humain en Suisse. Les risques que les conditions cadre deviennent défavorables et que la Suisse soit nettement moins attractive en comparaison internationale sont importants. Une simple modification des règles (qui ont été minutieusement élaborées avec tous les acteurs concernés au cours d'un processus ayant duré plusieurs années) est susceptible d'avoir un impact très négatif sur l'industrie pharmaceutique ainsi que sur les secteurs de la biotechnologie et du génie biomédical suisses.
Forum PME	LPD	3		f	Profilage : nous demandons que cette notion soit définie de la même manière que dans le RGPD et qu'elle se limite, par conséquent, aux cas d'exploitation automatisée de données personnelles (et non pas, en outre, comme prévu à la lettre f, aux cas d'exploitation non-automatisée ainsi qu'aux cas d'exploitation de données non personnelles). Nous sommes en effet opposés à tout swiss finish ayant pour conséquence une augmentation des charges administratives et coûts pour les entreprises suisses concernées (auxquels les entreprises européennes ne sont, elles, pas confrontées).
Forum PME	LPD	5	5		Communication de données personnelles à l'étranger : nous demandons que le délai dans lequel le préposé doit communiquer sa réponse au responsable du traitement soit fixé à 30 jours et non pas à six mois, comme proposé. Un délai aussi long entraverait inutilement les entreprises dans leurs activités économiques.
Forum PME	LPD	8	1		Recommandations de bonnes pratiques : nous sommes de l'avis que la tâche du préposé devrait se limiter à approuver les recommandations élaborées par les milieux intéressés (si elles sont conformes aux dispositions de protection des données). Comme dans l'UE, le préposé ne devrait pas élaborer lui-même ces recommandations (voir art. 40 RGPD). Les milieux économiques sont en effet mieux à même de le faire, car ils connaissent mieux que quiconque leurs domaines d'activités.
Forum PME	LPD	13	4		Devoir d'informer lors de la collecte de données personnelles : l'al. 4 prévoit que lorsqu'un traitement est confié à un sous-traitant, le responsable du traitement communique à la personne concernée son identité et ses coordonnées ainsi que les données ou les catégories de données personnelles concernées. Une telle obligation n'est pas prévue dans le RGPD. Nous demandons que cet alinéa soit tracé, car il engendrerait des charges et coûts trop importants pour les entreprises concernées en Suisse.

Forum PME	LPD	13	5		L'alinéa. 5 arrête le moment où la personne concernée doit être informée lorsque les données personnelles ne sont pas collectées auprès d'elle. L'information doit lui parvenir au plus tard lors de leur enregistrement ou lors de la première communication à des tiers. Cette obligation est beaucoup plus stricte que la solution retenue dans le RGPD. Nous demandons que cet alinéa soit tracé ou qu'une solution identique à celle du RGPD (voir art. 14) soit prévue. Selon cet article, le responsable du traitement doit fournir les informations non pas dès l'enregistrement des données personnelles, mais dans un délai raisonnable (ne dépassant toutefois pas un mois).
Forum PME	LPD	16	1		Analyse d'impact relative à la protection des données : L'art. 16 instaure une obligation de procéder à une analyse d'impact « *lorsque le traitement envisagé est susceptible d'entraîner un risque accru pour la personnalité et les droits fondamentaux de la personne concernée* ». Nous demandons qu'une telle analyse (comme le prescrit l'art. 35 RGPD) ne soit obligatoire que dans les cas où le traitement envisagé est susceptible d'engendrer un « risque élevé ».
Forum PME	LPD	16	4		Nous demandons que le délai dans lequel le préposé doit communiquer ses éventuelles objections au responsable du traitement ou au sous-traitant soit fixé à 30 jours et non pas à trois mois, comme proposé. Un délai aussi long entraverait inutilement les entreprises dans leurs activités économiques.
Forum PME	LPD	16	5		Nous demandons que l'alinéa 5 ci-après soit ajouté à l'article 16 : « *Le Conseil fédéral prévoit des simplifications pour les petites entreprises* ». Par petites entreprises, il faut comprendre toutes celles qui ont jusqu'à 49 emplois à plein temps en moyenne annuelle. Nous sommes de l'avis que les petites entreprises devraient être exemptées de l'obligation d'établir chacune individuellement une analyse d'impact, comme cela est déjà prévu p.ex. dans le droit des denrées alimentaires (voir l'art. 26, al. 3 de la loi révisée sur les denrées alimentaires, relatif aux obligations d'autocontrôle, ainsi que l'art. 80 de l'ordonnance révisée sur les denrées alimentaires et les objets usuels). Des guides de bonnes pratiques, développés par les associations de branche (p.ex. des médecins, des avocats, des banques ou des gérants de fortune), remplaceraient les analyses d'impact individuelles des entreprises membres de ces associations. Cette solution permettrait de décharger les PME sans pour autant sacrifier aux exigences en matière de protection des données. Les guides recenseraient les principales activités exercées dans la branche et les analyseraient du point de vue de leurs impacts sur la protection des données (risques spécifiques induits et mesures à prendre). Les

					petites entreprises n'auraient ainsi pas à refaire chacune individuellement une nouvelle analyse d'impact (pour les mêmes processus), mais pourraient, par le biais des guides, se conformer aux exigences de l'art. 16. Les responsables du traitement ou les sous-traitants (pour autant qu'il s'agisse de petites entreprises) seraient ainsi exemptés de la lourde obligation de réaliser eux-mêmes des analyses d'impacts. Cela permettrait de réduire sensiblement les coûts de la réglementation pour une proportion importante d'entreprises, tout en assurant un niveau élevé de protection des données. A noter encore que ce système d'analyses d'impacts réalisées par les associations de branche serait compatible avec la règle de l'art. 35 RGPD ; les analyses d'impacts réalisées par les associations de branche dans le domaine du droit des denrées alimentaires sont considérées compatibles avec le droit de l'UE.
Forum PME	LPD	19		a	L'art. 19, let. a oblige le responsable du traitement et le sous-traitant à documenter leurs traitements de données. Selon l'art. 30 RGPD, cette obligation ne s'applique pas aux entreprises comptant moins de 250 employés (sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées). Nous vous demandons de prévoir également une telle exception dans la LPD.
Forum PME	LPD	50 51	1, 2 et 3 1		<u>Dispositions pénales</u> : nous demandons qu'un système de sanctions administratives à l'encontre des entreprises soit prévu, comme dans l'UE (art. 83 RGPD), en lieu et place des sanctions pénales prévues aux articles 50 ss AP-LPD (qui vont à l'encontre des personnes physiques). Alternativement, nous demandons qu'en cas d'infraction commise intentionnellement, l'amende soit fixée à 50'000 francs au plus et non pas à 500'000 francs comme cela est prévu dans le projet.
Forum PME	LPD	50 51	4 2		Nous demandons qu'en cas d'infractions commises par négligence (à l'instar des articles 34 et 35 de la loi en vigueur), aucune amende ne soit prévue.
Forum PME	LPD	59			Nous demandons que les responsables du traitement et les sous-traitants disposent d'un délai de deux ans (dès la date d'entrée en vigueur de la loi) pour mettre en œuvre toutes les nouvelles obligations introduites par la LPD révisée (et non pas uniquement celles prévues aux lettres a et b du projet).

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 :

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 :

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 (excepté chap. 8 « Commentaire des dispositions»)		
nom/société	**chap. n°**	**remarque / suggestion :**
Forum PME	9.4	Conséquences économiques : notre commission a reçu, en 2011, le mandat exprès du Conseil fédéral[2] de vérifier, lors de procédures de consultation, que les offices aient procédé, lors de l'élaboration de projets législatifs, à une mesure des coûts de la réglementation ainsi qu'à une analyse de leur compatibilité PME (du point de vue des charges administratives, etc.). Nous saluons le fait que votre office ait réalisé une analyse d'impact de la réglementation approfondie, en collaboration avec le SECO, sur ce sujet complexe. Nous vous rendons cependant attentifs au fait que **les informations figurant actuellement dans le rapport sont en partie insuffisantes**. Le chapitre sur les conséquences économiques du message devra contenir des informations détaillées et chiffrées concernant les impacts de la révision sur les différents groupes concernés[3], notamment sur les intermédiaires financiers, les fiduciaires, les avocats et notaires, les services informatiques, l'industrie pharmaceutique et biotechnologique, les professions médicales, etc.

Rapport explicatif : chap. 8 « Commentaire des dispositions »		
nom/société	**art.**	**remarque / suggestion :**
Forum PME	4, al. 6	Les indications relatives au consentement en cas de profilage ne permettent pas de savoir dans quels cas une déclaration écrite ou orale est nécessaire. Nous demandons que le futur message contienne des informations détaillées relatives à cette question, afin de réduire l'insécurité juridique y-relative.

[2] Mesure 2 du rapport du Conseil fédéral du 24.08.2011 "Allégement administratif des entreprises: bilan 2007-2011 et perspectives 2012-2015".
[3] Conformément au point 3.2 des directives du Conseil fédéral du 15.09.1999 sur l'exposé des conséquences économiques des projets d'actes législatifs fédéraux.

Amstutz Jonas BJ

Von: Florence Bettschart <f.bettschart@frc.ch>
Gesendet: Dienstag, 4. April 2017 16:35
An: Amstutz Jonas BJ
Betreff: FRC - Prise de position Révision de la LPD
Anlagen: FRC_Prise de position révision LPD.doc

Cher Monsieur,

Je vous prie de trouver, ci-joint, la position de la Fédération romande des consommateurs relative à la révision de la Loi sur la protection des données.

En vous en souhaitant bonne réception, je vous prie de croire, cher Monsieur, à l'expression de mes sentiments les meilleurs.

Florence Bettschart
Responsable Politique & Droit, Avocate

LA FEDERATION ROMANDE DES CONSOMMATEURS
LE POUVOIR D'AGIR
Rue de Genève 17, case postale 6151,1002 Lausanne, Suisse
T. +41 (0)21 331 00 90 I +41 (0) 76 347 08 87 I www.frc.ch I Facebook I Twitter

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 romande des consommateurs

Abréviation de la société / de l'organisation : FRC

Adresse : 17, rue de Genève, Case postale 6151, 1002 Lausanne

Personne de référence : Florence Bettschart, Responsable Politique & Droit, Avocate

Téléphone : 021 331 00 90

Courriel : f.bettschart@frc.ch

Date : 4 avril 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

Remarques générales _____ 3

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 _____ 7

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 _____ Fehler! Textmarke nicht definiert.

Projet de modernisation de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel _____ Fehler! Textmarke nicht definiert.

Rapport explicatif (excepté chap. 8 « Commentaire des dispositions»)_____ Fehler! Textmarke nicht definiert.

Rapport explicatif : chap. 8 « Commentaire des dispositions » _____ Fehler! Textmarke nicht definiert.

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.FRC	La FRC soutient globalement le projet de loi proposé. Les avancées technologiques de ces dernières années nécessitent une révision de la Loi fédérale sur la protection des données, afin que le particulier dispose d'un niveau de sécurité suffisant sur ses propres données. Le responsable de fichier (ou de traitement selon la nouvelle terminologie) doit assurer transparence et proportionnalité lors du traitement de données.
Fehler! Verweisquelle konnte nicht gefunden werden.FRC	Un exemple récent, qu'il faut mieux légiférer en Suisse sur la protection des données, est le suivant: Swisscom a informé ses clients, en février 2017, que leurs données allaient être transmises à des tiers. La communication qui a été faite aux clients Swisscom était peu transparente et n'expliquait pas les enjeux au niveau de la transmission des données, ni le destinataire de celles-ci. Les clients qui voulaient refuser devraient être pro-actifs pour s'opposer à l'utilisation de leurs données. Une simple opposition ne suffisait pas: il fallait passer par une procédure compliquée d'opt-out sur le site internet de Swisscom.. Pour les clients qui n'avaient pas le courage ou la possibilité de se lancer dans cette procédure, cela signifie que leurs données allaient être transmises à des tiers, certains étant aussi à l'étranger. Une procédure de ce type n'est pas acceptable du point de vue du client. La protection des données devrait être guidée par le principe du opt-in. Gage de confiance accrue entre entreprises et consommateurs, il faut pouvoir exiger des firmes un «opt-in actif»: ainsi, le consommateur donne ainsi son accord explicite à l'échange d'informations. L'opt-out passif, plus sournois, contraint le client à demander à être retiré d'un fichier où il a été enregistré d'office. La FRC considère que l'utilisation des données, sans contrepartie pour le consommateur, doit être faire en tous les cas l'objet d'un opt-in.
Fehler! Verweisquelle konnte nicht gefunden werden.FRC	Si certaines compétences du Préposé fédéral à la protection des données et à la transparence (PFPDT) sont élargies, il lui manquera toutefois toujours un pouvoir de sanctionner. Cela signifie qu'il faudra continuer à passer par le biais de procédures judiciaires pour voir reconnaître ses droits, ce qui est évidemment beaucoup plus lourd et compliqué pour un consommateur. S'il n'y a pas de sanction, il faudrait au moins donner la possibilité au PFPDT d'agir comme médiateur lorsqu'un consommateur a un litige, sur le même modèle que l'Ombudscom, par exemple. Cela serait très utile en particulier pour des procédures qui demandent de faire cesser l'atteinte, plutôt que d'agir en justice, ce qui est souvent compliqué et coûteux pour le consommateur.

Fehler! Verweisquelle konnte nicht gefunden werden.FRC	S'agissant des amendes qui peuvent être infligées, il est regrettable que le projet prévoie que ce sont les personnes privées qui peuvent être sanctionnées et non les entreprises.
Fehler! Verweisquelle konnte nicht gefunden werden.FRC	La FRC regrette que le projet de LPD, contrairement au droit européen, ne prévoit pas de droit à la portabilité qui permette de récupérer ses données dans un format standard pour se tourner vers un autre fournisseur. Cela aurait permis un meilleur contrôle sur ses données, favorisé leur réutilisation et le développement de nouveaux services.
Fehler! Verweisquelle konnte nicht gefunden werden.FRC	L'avant-projet ne prévoit pas de renversement du fardeau de la preuve en faveur de la personne dont les données sont traitées. En cas de procédure judiciaire, c'est donc à celui qui allègue un fait de le prouver. Un renversement aurait obligé le responsable du traitement à démontrer qu'il traite les données de manière licite.
Fehler! Verweisquelle konnte nicht gefunden werden.FRC	Aucune action collective n'est prévue, le Conseil fédéral préférant mettre cela en œuvre par le biais d'une modification générale du Code de procédure civile. Un regroupement des procédures devant le PFPDT aurait simplifié le travail aussi bien pour les responsables du traitement que pour les personnes concernées.
Fehler! Verweisquell	Plusieurs interventions parlementaires (Postulat Schwaab, 16.3682 ; Motion Savary, 12.3578 ; Question Comte, 12.1084) se sont penchées sur la problématique **des fichiers de solvabilité**. Ces fichiers tiennent des informations sur la solvabilité des personnes privées, donnent des

e konnte nicht gefunden werden.FRC	renseignements commerciaux, voire même des notes sur des particuliers, sans que l'on sache d'où viennent les données et comment elles sont traitées. Moyennant finance, n'importe qui peut avoir accès à ces données. Souvent, les personnes fichées ne savent même pas qu'elles le sont. Et si elles le savent, elles peinent à savoir à quelles entreprises s'adresser. En résumé, il règne une immense opacité qui ne correspond pas aux principes de la loi sur la protection des données. En outre, se pose le problème de la véracité des données inscrites. Les renseignements sont souvent inexacts, les créances douteuses ou il y a confusion dans les noms (homonymie). De bons payeurs, des enfants parfois se retrouvent sur ces listes. Bref la population tout entière peut être victime d'un fichage abusif. Les conséquences de ces données disponibles dans les registres de solvabilité et à disposition de quiconque souhaite les consulter peuvent être graves. Le système de notation appliqué par les sociétés de recouvrement (la note A est la note maximale) peut être consulté par toute personne ou entreprise souhaitant se renseigner sur un citoyen. Cela a un impact quotidien sur la vie des gens (abonnement de téléphonie, bail, contrat de travail, petit crédit ou encore assurance refusés). Cela peut porter une grave atteinte à la vie privée des gens, inadmissible dans la plupart des cas. Aucune indication de durée n'est préconisée pour la conservation des données, aucune définition n'est arrêtée pour préciser qui est un bon ou un mauvais payeur. Il n'est pas rare d'avoir une mauvaise note sur la base d'un simple retard de paiement. La procédure pour demander l'effacement et la suppression des données n'est souvent pas claire, voire inexistante. Ces fichiers, à l'inverse du registre des poursuites et de l'IKO (fichier lié à la loi sur le crédit à la consommation), n'ont aucune base légale. Ils doivent être interdits dans la LPD. En 2012, une pétition de la FRC et de ses consoeurs de l'Alliance des organisations de consommateurs (SKS et ACSI), réunissant plus de 4000 signature, demandait au Conseil fédéral l'interdiction de ficher les personnes privées en matière de solvabilité dans des fichiers autres que le registre des poursuites et l'IKO, centre suisse de renseignements pour le crédit à la consommation. Pour sortir de ces fichiers, il faut souvent une longue procédure d'opt-out. Le Conseil fédéral avait répondu, notamment dans le cadre de la motion Savary et de la question Comte, qu'une législation complémentaire à ce sujet devrait être examinée dans le cadre de la révision de la LPD. Or, ce point n'a pas du tout été traité par la révision de la LPD. Il n'est même pas évoqué dans le rapport. Le problème se pose également avec les maisons de recouvrement qui transmettent les données récoltées à des sociétés de renseignements économiques, sans que l'on connaisse les critères de transmission. La FRC estime que la question doit être réglée dans le cadre de la révision de la LPD : le principe devrait être que ces fichiers, mis à part le Registre des poursuites et l'IKO, sont interdits.
FRC	La FRC se réjouit que les données génétiques et les données biométriques qui identifient un individu de façon unique figurent explicitement dans cette révision de la LPD. 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. Lorsque la personne fait un don d'échantillon biologique à des fins de recherche, il est difficile de prévoir toutes les conséquences que pourrait avoir ce geste dans plusieurs années. Aussi, il nous semble primordial d'encadrer strictement le traitement de ces données. Le projet de révision de la LPD devrait mieux prendre en compte les risques liés à cette question. Il nous semble également utile de préciser que le concept d'anonymisation des données doit être appréhendé de manière très prudente. Avec le développement des techniques génétiques et physiologiques, il est actuellement aisé de relier un échantillon biologique à un individu. 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.
FRC	La FRC considère que la LPD devrait aussi pouvoir s'appliquer à des entreprises n'ayant pas de siège en Suisse mais procédant à des traitements ayant des effets en Suisse. Celles-ci devraient avoir un répondant en Suisse.
FRC **Fehler! Verweisquelle konnte nicht gefunden werden.**	En résumé, la FRC, même si elle n'est pas entièrement satisfaite par la révision de la LPD telle que proposée, car trop légère, soutient cette révision. Elle demande par contre que soient ajoutés à la loi les points suivants : - Principe en matière de protection des données : Procédure d'opt-in - Droit à la portabilité - Renversement du fardeau de la preuve - Pouvoir de sanction administrative du PFPDT, ce qui impliquerait des moyens financiers supplémentaires pour le PFPDT - Action collective - Interdiction des fichiers de solvabilité, excepté les registres de poursuites et l'IKO, centre de renseignement suisse sur les crédits à la consommation - Amendes à l'égard des entreprises et non des personnes privées - Application de la LPD à des entreprises, n'ayant pas de siège en Suisse mais dont l'utilisation de données ont des effets en Suisse.

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 :
FRC	LPD	2	1	a	Le rapport du Conseil fédéral ne définit pas clairement ce qu'il entend par « personne privée ». S'agit-il uniquement de personnes physiques ou s'agit-il des personnes physiques et morales ? L'acception pour nous doit être celle des personnes physiques et morales. Si tel n'est pas le cas, la portée de la révision de la LPD n'est pas suffisante.
FRC	LPD	3		c	L'introduction spécifique des points 3. et 4. est saluée, soit les données génétiques, et les données biométriques qui identifient un individu de façon unique.
Fehler! Verweisquelle konnte nicht gefunden werden.FRC	LPD	4	2		L'exigence d'un traitement conforme au principe de la proportionnalité est essentielle et est saluée. Le principe de la minimisation des données doit conduire à un traitement approprié des seules données nécessaires au but recherché.

Fehler! Verweisquelle konnte nicht gefunden werden.FRC	LPD	4	3		La formulation de l'article 3 ne garantit aucune protection adéquate. Cela ne suffit pas, que le but du traitement soit clairement reconnaissable. Ce qui est déterminant, c'est que la personne concernée doit être informée explicitement au moment de la collecte des données. Il doit d'abord être informé de la collecte des données elle-même. D'autre part, le but du traitement des données doit être clairement expliqué. Le cas des données marketing transmises à des tiers est particulièrement criant, notamment celles transmises à des pseudo partenaires. Il ne devrait pas être possible de transmettre ces données sans accord exprès de la personne concernée. Proposition : Les données personnelles doivent être collectées pour des finalités déterminées et en informant du but recherché la personne concernée ;…. La deuxième partie de la phrase de l'article 4 dans la version française ne correspond pas à la version allemande, ce qui porte à confusion.
FRC	LPD	4	6		Cet alinéa doit être complété par le principe du opt-in. En effet, la FRC estime que c'est un accord explicite qui doit guider les relations entre les parties pour que la confiance soit garantie entre les entreprises et les particuliers.
FRC	LPD	5	1		Selon cet alinéa, aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée. Cette limitation à la gravité de la menace est en opposition avec les autres alinéas de l'art. 5 et doit être clairement refusée.
FRC	LPD	5	2		Nous ne voyons pas très bien comment le Conseil fédéral pourra constater qu'un autre Etat dispose d'une législation assurant un niveau de protection suffisant, quels seront les critères pour déterminer cela.
FRC	LPD	6	1	e	La lettre e de l'art. 6 al. 1 AP-LPD prévoit que des données peuvent exceptionnellement être communiquées à l'étranger lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement. La notion d'accessibilité n'est pas suffisante dans le monde numérique actuel. Il faudrait dès lors compléter cette notion par le terme publiquement. Par ailleurs, la collecte de données doit également être protégée par

					cette article. Nous proposons donc la formulation suivante pour la lettre e : La personne concernée a rendu les données personnelles accessibles publiquement à tout un chacun et n'est pas opposée expressément à la collecte.
FRC	LPD	8			La publication de recommandations de bonnes pratiques par le PFPDT est à saluer. Néanmoins, le fait que celles-ci ne soient pas contraignantes restreint la portée de cette article et risque parfois de porter à confusion : s'agit-il d'un objectif idéal ou du minimum légal à atteindre ? Comme le montre l'exemple de Swisscom, le PFPDT a proposé une procédure d'opt-in, ce qui n'a pas été suivi par l'opérateur, qui a uniquement mis en place une procédure d'opt-out.
FRC	LPD	10	1		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 certification « obligatoire ». Ceci permettrait 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 ; *les organisations qui, de par la loi, sont amenées à traiter des données sur la santé.* »
Fehler! Verweisquel le konnte nicht gefunden werden.FRC	LPD	12	3		Si l'on peut saluer le fait d'avoir voulu régler dans la LPD la question de la mort numérique, il apparaît en revanche que l'alinéa 3 de cet article est inacceptable. Les données médicales ou juridiques sont notamment protégées par les dispositions relatives au secret professionnel (art. 321 CP) et au secret de fonction (art. 320 CP). Le secret professionnel poursuit plusieurs intérêts, en particulier. - La protection de la sphère intime et privée du particulier, qui doit pouvoir se fier entièrement à la discrétion du professionnel en vue de lui livrer toutes les informations qui lui permettront de recevoir le traitement le plus adapté. - L'intérêt de l'Etat à ce que les professions protégées par le secret professionnel puissent être exercées correctement et sans entrave, dans la mesure où ces professions ne peuvent être exercées que si elles inspirent au public une confiance suffisante, moyennant de sérieuses garanties de discrétion. - L'intérêt du professionnel à ce qu'un rapport de confiance existe, de manière à pouvoir exercer son métier efficacement. - La protection des informations qui concernent des tiers et qui auraient été divulguées. Selon la jurisprudence, le secret médical continue de déployer ses effets après la mort du patient (ATF 87 IV 105). Même si la personnalité finit par la mort (art. 31 CC), il n'apparaît en effet pas dépourvu de sens de garantir aux justiciables qu'après leur décès, les renseignements figurant dans leur dossier médical demeureront couverts par le secret médical et ne seront divulgués *sans un contrôle sévère* (arrêt du Tribunal fédéral du 3 novembre 1989, RDAF 1990 p. 45, c. 4b). L'article 12 AP-LPD ouvre une brèche inacceptable au maintien du secret médical ou juridique après la mort du patient. Si le défunt n'a pas de son vivant interdit expressément la consultation de son dossier après sa mort, cette disposition permettrait en effet à tout tiers présentant un intérêt légitime de

					consulter son dossier si aucun intérêt prépondérant du défunt ou d'un tiers l'en empêche. Cette disposition est problématique à plusieurs titres : - L'article 12 AP-LPD supprime au responsable du traitement le droit d'invoquer le secret professionnel ou de fonction. De ce fait, il remet en cause l'existence même du secret médical ou juridique après la mort du patient. Cela est propre à entamer la confiance nécessaire que le public doit placer dans ces professions afin de garantir le bon exercice de ces dernières. Le secret professionnel, le cas échéant de fonction, doit être maintenu après la mort du patient. - Le dossier médical ou juridique d'une personne décédée peut contenir des données très sensibles que le défunt ne souhaitait pas divulguer aux membres de sa famille, même après sa mort. Ces données nécessitent une protection particulière, que l'article 12 AP-LPD n'assure pas suffisamment. - L'article 12 AP-LPD présume l'existence d'un intérêt légitime en faveur des personnes en lien de parenté directe avec le défunt ou mariées, en partenariat enregistré ou en concubinage. Or, le secret professionnel vaut précisément à l'égard de ces proches et il doit être maintenu par principe après la mort du patient. L'accès aux données médicales ou juridiques par les proches après la mort du patient est rendu ici trop aisé. - Les garde-fous prévus par l'article 12 al. 1 AP-LPD, à savoir que le défunt n'a pas de son vivant interdit expressément la consultation et qu'aucun intérêt prépondérant du défunt ou d'un tiers ne l'empêche, constituent des protections insuffisantes en matière de secret professionnel. Il paraît en effet douteux que l'ensemble des particuliers soient informés, au début de chaque relation avec celui soumis au secret professionnel, de leur droit de s'opposer à la divulgation de leurs données après leur mort. Nous reconnaissons que la consultation de données médicales d'une personne décédée doit pouvoir être accordée dans des circonstances particulières, notamment en cas de suspicion d'erreur médicale ayant conduit à la mort d'un patient ou en cas de maladie génétique. Toutefois, même dans cette hypothèse, la transmission d'informations aux proches doit être strictement encadrée et se limiter aux seules informations nécessaires.

					En conséquence, l'article 12 al. 3 AP-LPD ne peut pas subsister sous la forme proposée.
FRC	LPD	13	1-5		L'article 13 prévoit un devoir d'informer la personne concernée de la collecte de données. La collecte de données en elle-même représente déjà un traitement des données. Comme déjà dit, la FRC demande le respect du principe du opt-in: le traitement de données ne doit se faire qu'avec le consentement exprès de la personne concernée. Il faut donc que cette notion soit intégrée à l'article 13. Cela vaut d'autant plus à l'alinéa 3 relatif à la communication de données à des tiers ou à des catégories de destinataires. Il est nécessaire que les tiers soient facilement identifiables et expressément nommés et notifiés aux consommateurs. La simple acceptation de conditions générales par un clic ne suffit pas à définir cette acceptation comme un accord exprès. Il faut que la personne concernée soit rendue particulièrement attentive au traitement de ses données. Par ailleurs, la transmission de données à des fins marketing, notamment à des pseudo-partenaires, doit être particulièrement cadrée et ne peut être permise sans une acceptation expresse par le consommateur.
FRC	LPD	14	1		Selon cet alinéa, le responsable du traitement est délié du devoir d'information au sens de l'art. 13 lorsque la personne concernée dispose déjà des informations correspondantes. La FRC refuse cet alinéa qui amène trop d'insécurité juridique. Selon les circonstances, ces informations ont été données il y a très longtemps. Cela signifie qu'il y a une sorte de procuration en blanc au traitement des données lorsque l'information a été donnée une fois. Il faudrait dès lors que le responsable du traitement informe lors de chaque changement la personne concernée.
FRC	LPD	15	1		La formulation, qui prévoit que le responsable du traitement informe la personne concernée lorsqu'une décision qui a des effets juridiques sur elle ou qui l'affecte de manière significative est prise exclusivement sur la base d'un traitement automatisé, n'est pas suffisante. La plupart des décisions de ce type ont des effets juridiques : cela signifie que cela laisse une importante marge d'interprétation. Le Conseil fédéral devrait définir de manière plus claire ce que sont ces décisions qui ont des effets juridiques.

FRC	LPD	18	1		La FRC salue cet article qui va dans le bon sens. Néanmoins, le respect des principes de protection des données par défaut et dès la conception ne doit pas seulement être une obligation du responsable du traitement, cela doit aussi être une obligation des constructeurs, fabricants, développeurs. Si l'on pense à un logiciel informatique, à une caméra, un téléphone portable ou une voiture connectée, ce n'est pas le responsable du traitement (qui sera souvent l'utilisateur) qui pourra respecter ces principes, mais c'est le fabricant qui doit les appliquer et permettre leur application dès la conception / fabrication. La protection des données dès la conception n'est pas suffisante et une interdiction doit être faite aux fabricants et développeurs de prévoir des portes dérobées (backdoors) et toutes autres mesures permettant un accès aux données à l'insu de la personne concernée. De plus, la terminologie utilisée (« mesures appropriées », « prévenir les atteintes ») pour cet article réduit sa portée. Nous proposons donc une modification de l'article 18 al. 1 : Dès la conception du traitement, le responsable du traitement et le sous-traitant, notamment le développeur, le constructeur ou le fabricant, doivent prendre toutes les mesures qui assurent qu'il n'y ait pas d'atteinte à la personnalité et aux droits fondamentaux de la personne concernée.
FRC	LPD	18	2		Le principe de la protection par défaut (privacy by default) est ancré dans cet alinéa. Revendication de longue date des organisations de consommateurs, cet alinéa répond aux besoins matériels d'une loi moderne sur la protection des données, applicable au monde numérique. La FRC soutient dès lors tout particulièrement cet alinéa. Dans le cas de données personnelles qui ne sont pas nécessaires à la finalité du traitement, les fabricants doivent prévoir une procédure d'opt-in pour tout transfert de données à des tiers.
FRC	LPD	20	1		L'article 20 de l'avant-projet prévoit un droit d'accès très large pour le consommateur. Il pourra notamment demander gratuitement l'identité et les coordonnées du responsable du traitement, les données traitées, la finalité du traitement, la durée de conservation ou les critères pour fixer cette

					dernière et les informations disponibles sur l'origine des données. Cela est à saluer.
FRC	LPD	20	5		Selon l'art. 20 al. 5, le sous-traitant doit fournir les renseignements demandés, s'il ne révèle pas l'identité du responsable du traitement. Il n'y aucune justification à ce que le sous-traitant ne puisse pas révéler qui traite les données de la personne concernée. Au contraire, celle-ci doit avoir le droit de savoir par qui ses données sont traitées. Cela va de plus à l'encontre de l'art. 13 al. 4 AP-LPD. La partie de la phrase «s'il ne révèle pas l'identité du responsable du traitement » doit dès lors être biffée.
FRC	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.
FRC	LPD	23	3		L'art. 23 al. 3 devrait reprendre la formulation proposée à l'art. 6 al. 1 lit. e) : En règle générale, il n'y a pas d'atteinte à la personnalité lorsque la personne concernée a rendu les données personnelles accessibles publiquement à tout un chacun et ne s'est pas opposée expressément à la collecte.
FRC	LPD	25	1	c	S'agissant des prétentions qu'un consommateur pourra faire valoir, il a été ajouté, par rapport à la loi actuelle, la mention du droit à l'effacement. Cela correspond à la revendication du droit à l'oubli et c'est un point à saluer.
FRC	LPD	27	3	b	L'art. 27 al. 3 lit. b devrait reprendre la formulation proposée à l'art. 6 al. 1 lit. e) : la personne concernée y a consenti ou a rendu ses données personnelles accessibles publiquement à tout un chacun et ne s'est pas opposée expressément à la collecte.
FRC	LPD	29	2	d	L'art. 29 al. 2 lit. d devrait reprendre la formulation proposée à l'art. 6 al. 1 lit. e) : la personne concernée a rendu ses données personnelles accessibles publiquement à tout un chacun et ne s'est pas opposée expressément à la collecte.
LPD	50	Ss			Des instruments légaux sont nécessaires pour mettre de la pression pour une application effective du droit. L'élargissement du catalogue des infractions, de même qu'une augmentation importante des amendes est dès lors à saluer.

					Par contre, deux éléments importants doivent être corrigés : 1. Seules les personnes privées peuvent être amendées, soit selon notre interprétation les personnes physiques. Si tel est le cas, il s'agit d'une limitation qui n'est pas acceptable. Les sociétés doivent également pouvoir être poursuivies. Dans le monde numérique, ce sont évidemment les personnes morales qui sont responsables du traitement et non des personnes physiques. La limitation aux personnes privées des poursuites pénales est bien évidemment un affaiblissement important de l'effet préventif de ces dispositions. La poursuite pénale doit dès lors être élargie aux personnes morales. 2. Les art. 50ss ne prévoient pas de renvoi à l'art. 4 AP-LPD, qui pose les principes de la loi. Or, si des violations des principes de la loi sont constatés, celles-ci doivent également pouvoir faire l'objet d'une sanction. Le catalogue des infractions devrait dès lors être élargi à l'art. 4.
FRC	CPC	99 113 114	3 2	d g f	La FRC salue particulièrement les modifications des articles du CPC qui prévoient de ne pas percevoir de sûretés ou de frais judiciaires concernant les litiges relevant de la loi sur la protection des données. En effet, il s'agit d'un domaine où la valeur litigieuse est difficilement calculable. Les frais judiciaires empêchent souvent que le particulier ouvre action, alors que celle-ci est totalement justifiée.

Amstutz Jonas BJ

Von: Richard Lins <rli@ftargeting.ch>
Gesendet: Dienstag, 4. April 2017 11:25
An: Amstutz Jonas BJ
Betreff: Stellungnahme zur Vernehnlassung vom neuen DSG
Anlagen: Formular-fuer-Stellungnahme_de_VE-DSG (2).doc

Guten Tag Herr Amstutz

Unsere Stellungnahme zum DSG-Entwurf finden Sie im Anhang.

Freundliche Grüsse
Richard Lins

FutureTargeting.ch
Bright strategies for new target groups
Schachenstrasse 82
8645 Rapperswil-Jona
Tel: +41 (0)55 511 25 25
Fax: +41 (0)55 212 19 30
future-targeting.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 : Future Targeting GmbH / Geschäftsleitung

Abkürzung der Firma / Organisation : FtargetingGL

Adresse : Schachenstrasse 82, 8645 Rapperswil-Jona

Kontaktperson : Richard Lins

Telefon : 055 511 25 25

E-Mail : rli@ftargeting.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 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 4

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 5

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten 5

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") 6

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" 6

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
FtargetingGLFtargetingGL	Das CH-Gesetzt strenger als das EU-DSGVO zu gestalten, ist ein Schuss ins eigene Bein und wird sehr viele Arbeitsplätze in der digitalen Zukunftsbranche kosten. Ökonomische Nachteile für CH Unternehmen in Kauf zu nehmen, erachten wir als sehr bedenklich.
FtargetingGL FtargetingGL	Der erhöhte administrative Aufwand ist für Grossunternehmen kein Problem. Jedoch für kleine Firmen nicht tragbar.
FtargetingGL FtargetingGL	Die Gesetzesverschärfung wird sogenannte "schwarze Schafe", die vom Ausland aus arbeiten nicht treffen. Deshalb wird der Frust des Konsumenten mit dem neuen DSG nicht sinken.
FtargetingGL FtargetingGL	Wir bedauern sehr, dass nicht mehr Wirtschaftsvertreter in der Kommission waren. Dieses Gesetz trifft die Schweizer KMU's in verschiedenen Branchen sehr hart, obwohl sich die grosse Mehrheit bereits jetzt stark an das geltende Datenschutzrecht hält.
FtargetingGL	
FtargetingGL	
FtargetingGL	

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
FtargetingGL FtargetingGL	DSG				Persönlichkeitsprofile und Profiling: Wir verstehen nicht, wieso die betreffende Person der Adresse ihre Zustimmung geben muss, wenn die Daten für Marketingzwecke genutzt werden. Eine Verstärkung des Personenschutzes macht hier keinen Sinn.
FtargetingGL	DSG	51			Besonders schützenswerte Daten müssen wie bisher geschützt werden. Wieso Profilbildung sanktioniert werden sollen verstehen wir nicht.
FtargetingGL	DSG	50			Da Strafverfolgung auf Private und nicht auf das Unternehmen abzielt, wird die Kosten für den operativen Betrieb signifikant erhöhen. Die Löhne der Verantwortlichen werden stark ansteigen. Präventive Anwaltskosten werden Kleinfirmen nicht bezahlen können.
FtargetingGL					
FtargetingGL					
FtargetingGL					

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
FtargetingGL	
FtargetingGL	
FtargetingGL	

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

Name/Firma	Bemerkung/Anregung
FtargetingGL	
FtargetingGL	
FtargetingGL	

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**
FtargetingGL		
FtargetingGL		
FtargetingGL		

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"		
Name/Firma	**Art.**	**Bemerkung/Anregung**
FtargetingGL		
FtargetingGL		
FtargetingGL		

Amstutz Jonas BJ

Von: Michel Meier <m.meier@b3m.ch>
Gesendet: Freitag, 31. März 2017 10:06
An: Amstutz Jonas BJ
Cc: 'Florian Leupold MD'; 'Meier Lukas Dr.'
Betreff: Vernehmlassung zum VE DSG
Anlagen: 20170331095103751.pdf

Sehr geehrter Herr Amstutz

Anbei überlasse ich Ihnen fristgerecht die Stellungnahme der Gesellschaft der Ärztinnen und Ärzte des Kantons Solothurn zum Vorentwurf DSG. Wir haben bewusst auf das Formular verzichtet, sollte eine Rückmeldung dafür unerlässlich sein, bedanke ich mich, wenn Sie mir dies kurz mitteilen würden.

Ansonsten bin ich Ihnen verbunden, wenn Sie unsere Anliegen und Erwägungen prüfen und berücksichtigen können, zumal diese mit einem hohen praxisbezogen Wert hinterlegt sind.

Freundliche Grüsse

Michel Meier

GESELLSCHAFT DER ÄRZTINNEN UND ÄRZTE DES KANTONS SOLOTHURN (GAESO)

RECHTSBERATER
LIC. IUR MICHEL MEIER
Rechtsanwalt

C/O BONT BITTERLI MEIER
DORNACHERSTRASSE 26
POSTFACH
4600 OLTEN
TEL: +41 62 212 10 30
FAX: +41 62 212 76 30
EMAIL: M.MEIER@B3M.CH

Diese E-Mail ist allein für den bezeichneten Adressaten bestimmt. Wenn Sie diese E-Mail irrtümlich erhalten haben, informieren Sie bitte unverzüglich den Absender per E-Mail und löschen Sie diese E-Mail von Ihrem Computer, ohne Kopien anzufertigen. Vielen Dank.
Le présent courriel s'adresse exclusivement au destinataire indiqué. Si vous avez reçu ce message par erreur, nous vous prions de bien vouloir en informer immédiatement l'expéditeur et supprimer le présent e-mail de votre ordinateur sans en faire de copies. Merci beaucoup.
Il presente mail è indirizzato esclusivamente al destinatario indicato. Se Lei ha erroneamente ricevuto questo messaggio la preghiamo di volere informare immediatamente il mittente e cancellare il presente e-mail dal Suo computer senza farne alcuna copie. Grazie.
This email is for the exclusive use of the addressee. If you have received this message in error, please notify the sender by email immediately and delete the message from your computer without making any copies. Thank you.

Bitte denken Sie an unsere Umwelt, bevor Sie diese E-Mail drucken.

GESELLSCHAFT DER ÄRZTINNEN UND ÄRZTE DES KANTONS SOLOTHURN (GAESO)

per Mail (pdf)
jonas.amstutz@bj.admin.ch
Bundeamt für Justiz
3000 Bern

Olten, 31. März 2017

Vernehmlassung zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz der Gesellschaft der Ärztinnen und Ärzte des Kantons Solothurn (GAeSO)

Sehr geehrter Damen und Herren Bundesräte
Sehr geehrter Herr Amstutz
Sehr geehrte Damen und Herren

Gerne und zeitgerecht bediene ich Sie – namens der GAeSO – mit der begründeten Stellungnahme zur rubrizierten Vernehmlassung und danke Ihnen für die Möglichkeit der Mitwirkung.

1. Grundsätzliche Bemerkungen

Die nachfolgende Vernehmlassung erfolgt aus der Optik der medizinischen Leistungserbringer, vorwiegend im ambulanten Bereich, aber nicht nur. Dabei werden auch konkrete Überlegungen zu den laufenden Datenerhebungen gezogen und mit der künftigen Gesetzgebung geprüft. Zur besseren Übersicht und Darstellung unserer Begründung, haben wir auf die Ausfüllung des Vernehmlassungsformulars verzichtet.

Das Co-Präsidium und die grosse Mehrheit der GAeSO stehen der titelvermerkten Vorlage kritisch gegenüber, wenn auch offenkundig ist, dass gewisse Anpassungen im DSG nötig sind. Solche Anpassungen dürfen aber nicht zu Rechtsunsicherheiten führen, aber gerade im Bereich des Gesundheitsrechts fehlt es an Legiferierungssubstrat im VE-DSG und die Lücken dürften langwierige Prozesse nach sich ziehen, die nicht nötig wären. Dabei werden sowohl die Datenerhebungen und der Datenschutz der Leistungserbringer und der Patienten im VE-DSG ungenügend oder gar nicht berücksichtigt. Diese Unzulänglichkeit ist mit entsprechenden Anpassungen bzw. Korrekturen, zu bereinigen. Die Gründe und die Lösungsansätze legen wir Ihnen nachfolgend dar:

c/o Bont Bjtterli Meier
Dornacherstrasse 26
Postfach
4603 Olten

Tel: +41 62 212 10 30
Fax: +41 62 212 76 30

Email: m.meier@b3m.ch

Grundsätzlich geht die Revision in die richtige Richtung. Zur Internationalisierung und zur länderübergreifenden Amtshilfe können wir uns nicht äussern. Indessen unterstützungswürdig sind die geschaffenen Leitlinien nach Ziffer 1.4.1 der Botschaft. Allen voran der risikobasierte Ansatz und die Stärkung der betroffenen Person. Dabei darf aber nicht darüber hinwegtäuschen, dass in der Gesamtkonstruktion des Entwurfs, grundsätzlich immer nur ein betroffener Datenherr und eine erhebende bzw. sammelnde Datenstelle besteht. Gerade im Gesundheitsbereich werden die Leistungserbringer zu „Zwischenstellen" bzw. möglicherweise zu Auftragsbearbeiter, welche einerseits Daten ihrer Patienten sammeln und mit eigenen Daten ergänzen müssen, welche dann, als besonders schützenswerte Personendaten, gestützt auf ein Gesetz im formellen Gesetz, weitergegeben werden müssen. Dieser Doppelrolle wird im Revisionsentwurf zu wenig oder gar kein Gewicht beigemessen. Dies wird anhand der sechsten Leitlinie besonders deutlich, wo die Stärkung der betroffenen Personen gleichzeitig die Pflichten der Verantwortlichen präzisiert. Ein Leistungserbringer in seiner Doppelrolle kann diese beiden Erwartungen nicht gleichzeitig erfüllen.

Wichtig erscheint der Hinweis, dass die vorherrschenden Unschärfen der aktuellen Gesetzgebung nun ausgeräumt werden und der fortschreitenden Technologie Rechnung zu tragen, ohne die Re- oder direkte Identifikation zu ermöglichen. Ein exemplarisches Beispiel dazu findet sich auch in der Botschaft auf Seite 43 zu 8.1.1.3 Art. 3 zur Definition der Begriffe: *„Wie auch nach dem aktuellen Recht reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei bestimmbar. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Die zur Verfügung stehenden technischen Möglichkeiten werden in Bezug darauf geprüft, wie hoch der zeitliche und finanzielle Aufwand für ihre Anwendung ist. Mit Blick auf die immer gezielteren Technologien zur Datenauswertung und deren konstante Weiterentwicklung verschwimmt die Grenze zwischen Personendaten und anderen Daten indes zusehends. Daten, bei denen heute noch eine rein theoretische Möglichkeit der Identifizierung anzunehmen ist, können morgen vielleicht bereits einer bestimmbaren Person zugeordnet werden."* Dieser technischen Erweiterungsmöglichkeit ist in der Gesetzesvorlage genügend Gewicht beizumessen, insbesondere in den gesetzlichen Bestimmungen, wo gegenwärtig mit anonymisierten Personendaten gearbeitet werden soll. Diese Begrifflichkeiten sind mit gruppenbasierten Personendaten zu ersetzen, soweit kein gesetzlicher Anknüpfungspunkt in einem Gesetz im formellen Sinn besteht und der Verwendungszweck konkret und nachvollziehbar auf gleicher Normstufe ausgeführt wird.

II. Abschreibung Postulat Béglé:

Postulat Béglé 16.3384 «Elektronische medizinische Daten. Eine geschützte, transparente und zielgerichtete Datenerhebung im revidierten Bundesgesetz über den Datenschutz sicherstellen». Das Datenschutzgesetz gilt für medizinische Daten, soweit nicht ein Spezialgesetz etwas anderes vorsieht. Der VE-DSG sieht verschiedene Pflichten des Verantwortlichen und des Auftragsbearbeiters vor, die auch für medizinische Daten gelten (Art. 13, 15, 16, 17, 18 und 19 VE-DSG) und den Forderungen des Postulats entsprechen. Weitere Massnahmen wie beispielsweise die Präzisierung der Anforderungen für die Einwilligung (Art. 4 Abs. 6) sowie die Erarbeitung von Empfehlungen der guten Praxis, sollten auch im Bereich der medizinischen Daten zu einem verbesserten Schutz führen.

Hier stellt sich, wie nachfolgend auch noch, die Frage, welche Funktion im gesetzlichen Sinne für die Ärzteschaft vorgesehen ist. Soweit die Erhebung- und Datenweiterleitungspflicht der Ärztinnen und Ärzte keine weiteren Pflichten, insbesondere Aufklärungspflichten vorsieht (vgl. dazu Interpretation und Fragen D, Artikeln 13 ff VE-DSG, nachfolgend), ist der Bestimmungsgrad und die das Postulat erfüllt. Dabei ist weiter zu berücksichtigen, dass der Datenschutz, auch für die Ärzte vollumfänglich gilt und frühzeitig greift. Das sind mitunter zwei der erklärten Ziele dieser Revision. Der Entwurf sieht dies noch nicht in der nötigen Klarheit vor. Demnach ist der Entwurf dahingehend zu ergänzen, als dass in Artikel 27 konkret festgehalten wird, dass die Leistungserbringer Gesundheitsdaten nur erheben und weiterleiten müssen, wenn dies in einem Gesetz in formellen Sinne ausdrücklich vorgesehen und dem Zweck nach genügend bestimmt ist. Im Übrigen ist der Leistungserbringer im Umfeld von Datenerhebungen im Gesundheitsrecht von den Verpflichtungen was die Information gegenüber dem Patienten anbelangt (Art. 14 VE-DSG), von den Datenschutz-Folgeabklärungen (Art. 16 VE-DSG) und den weiteren Pflichten (Art. 19 VE-DSG) ausdrücklich auszunehmen.

Erst wenn alle diese offenen Punkte rechtsgenüglich geklärt und im VE-DSG aufgenommen sind, kann das Postulat Béglé effektiv abgeschrieben werden.

III. Konkrete Problemstellung für Ärztinnen und Ärzte

(kursiv Gesetzestext aus dem Entwurf, ganz oder auszugsweise)

A. Artikel 2 VE-DSG

1. Ausgangslage und Gesetzestext

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[3], 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 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.

2. Bemerkungen

Selbstredend ist bei der gesetzlichen Aufzeichnungs- und Aufbewahrungspflicht der Patientendaten durch den Leistungserbringer nicht von einem persönlichen Gebrauch auszugehen, genau so wenig, wie wenn es um die Weiterleitung dieser Daten gestützt auf ein Gesetz im formellen Sinn geht, wie

es aktuell mit der Datenerhebung MARS bzw. MAS umgesetzt wird. Dabei stellt sich aber die Frage, was mit den juristischen Personen, welche gestützt auf das Bundesstatistikgesetz eine UID erhalten, aber nach Art. 36a KVG als (Medizinal- oder Gruppen-)Praxis als Institution ausgestaltet sind. Dieser Widerspruch zwischen UID und juristische Person nach Art. 52 ff ZGB wird im VE-DSG nicht ausgeräumt. Nach vorgenanntem Art. 2 VE-DSG ist der Geltungsbereich nur noch für natürliche Personen (und Bundesorgane) vorgesehen. Juristische Personen gehören nicht mehr in den Geltungsbereich, ob sich bei der MARS bzw. MAS Erhebung eine Bearbeitung der Daten durch ein Bundesorgan supponieren lässt und damit die Erhebung durch eine Gruppenpraxis als juristische Person argumentativ umgehen lässt, darf durchaus bezweifelt werden. Hier ist unbedingt Klarheit zu schaffen. Mit Blick auf das Postulat Béglé, welches als erfüllt angesehen wird, kann ja nicht ernsthaft gefolgert werden, dass das DSG für die Erhebung MARS bzw. MAS nicht gilt, da hier die Leistungserbringer gemäss UID befragt werden. Hier besteht Handlungs- bzw. Klärungsbedarf.

B. Artikel 3 VE-DSG

1. Ausgangslage und Gesetzestext

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,
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;
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;
i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auf-trag des Verantwortlichen Personendaten bearbeitet.

2. Bemerkungen

Diese Bestimmung nimmt einen zentrale Funktion im DSG ein, wonach mittels guten und korrekten Definitionen griffige und frühzeitige Klärung geschaffen wird. Das gilt insbesondere für die besondere schützenswerten Personendaten und über das „Profiling". Dieses wird zunehmen wichtiger, auch bei Daten-Verknüpfung die in den entsprechenden Gesetzten nicht explizit vorgesehen sind. Indessen ist der Begriff „Profiling" noch ungenügend umschreiben. In der Praxis wird dies den Rechtsanwendern zunehmend Mühe bereiten, insbesondere da an diese Begrifflichkeiten Sanktionen und Rechtefertigungsgründe (vgl. lit. C zu Art. 4 VE-DSG nachfolgend) anknüpfen. Das ist entsprechend zu präzisieren.

Wenig verständlich ist, warum von „guter Praxis" nach Art. 8 und 9 VE-DSG keine Definition vorliegt. Dies wäre dienlich und auch sachgerecht. Entsprechend ist der Artikel 3 VE-DSG zu ergänzen. Mit Blick auf den erläuternden Bericht (vgl. dazu Ziffer 8.1.2.6), erscheint die dort gemachte Erklärung als taugliche Adaption für die beantragte Definition der guten Praxis und ist daher entsprechend in Artikel 3 aufzunehmen.

C. Artikel 4, 12 und 23 VE-DSG

1. Ausgangslage und Gesetzestext (*Auszüge*)

Artikel 4, Abs. 3 *Personendaten dürfen nur zu einem bestimmten und für die betroffenen Personen klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass die dies mit dem Zweck zu vereinbaren ist*»
Abs. 6 [...] *Für die Bearbeitung von besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.*»

Artikel 12 Daten einer verstorbenen Person
Abs. 3 *Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.*»

Artikel 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.
3 In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

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.

2. Bemerkungen

Der Artikel 4 VE-DSG ist in dieser Form sehr zu begrüssen. Dabei wird aber, unter Berücksichtigung von Artikel 12 und 52 der Revision, die Widersprüchlichkeit für den einzelnen Arzt erkennbar. Gemäss Artikel 4 Abs. 6 VE-DSG ist die Bearbeitung von Gesundheitsdaten, nach Artikel 3 lit c, al 2 VE-DSG, als besonders schützenswerte Personendaten durch den Patienten ausdrücklich zu bewilligen. Dem Patienten steht das Arztgeheimnis (besser das Patientengeheimnis zu). Demzufolge darf nicht einmal die Patientenbeziehung, ohne Einwilligung oder entsprechende gesetzliche Grundlage (Denkbar wäre auch eine kantonale Vorschrift), offen gelegt werden, geschweige denn die Behandlung oder die Diagnose uä. Das Patientengeheimnis gilt über den Tod hinaus. Aktuell gilt in der Praxis, dass

wenn Angehörige eine Kopie der Krankengeschichte einsehen wollen, ein konkrete Güterabwägung vorgenommen werden muss. Warum nun im Entwurf für Daten einer verstorbenen Person, nota bene eines Patienten, dass Berufsgeheimnis nicht mehr gelten soll, ist daher nicht nachvollziehbar. Artikel 12 VE-DSG ist ersatzlos zu streichen. Dies umso mehr, als dass in Art. 52 VE-DSG die Verletzung der beruflichen Schweigepflicht, eine Sanktion nach sich zieht. Diesfalls sind die Bestimmungen 12 und 52 unglücklich abgefasst und sind zwingend abzuändern, ansonsten läuft jeder Leistungserbringer Gefahr, sich einem Strafverfahren und einer Sanktion nach Art 52 VE-DSG auszusetzen, wenn er an den MARS- bzw. MAS Erhebungen oder ähnlich gelagerten Erhebung teilnimmt. Gleichzeitig wird das Patientengeheimnis, mindestens in den wesentlichen Grundzügen, aufgegeben, eine Selbstbestimmung des Patienten ist damit nicht mehr gewährt, was wiederum gegen die geplanten Ziele der Datenschutzgesetzgebung spricht (vgl. Leitlinien nach 1.4.1 im erläuternden Bericht).

Mit dem VE-DSG setzt sowohl das Datenschutzgesetz als auch das Strafgesetzbuch der Weitergabe von Informationen und Daten Schranken, für die Ärzte in der alltäglichen Arbeit ein zentraler Aspekt. Jeder Patient muss sich primär darauf verlassen können, dass seine Informationen beim Arzt verbleiben. Damit wird auch eine sorgfältige und umfassende Anamnese gewahrt. Mit den entsprechenden Bestimmungen, bestehen nun im VE-DSG in strafrechtlicher Hinsicht womöglich sog. Rechtfertigungsgründe, wenn die Datenbearbeitung nach DSG rechtmässig erfolgt ist. Jedoch ist zu berücksichtigen, dass die Datenbekanntgabe datenschutzrechtlich zulässig sein kann, aber dennoch kein Rechtfertigungsgrund vorliegt und damit nach Strafgesetzbuch gerade nicht zulässig und damit strafbar ist. Daher muss die Datenbekanntgabe nach VE-DSG zwingend vom Strafrecht getrennt werden. Die Voraussetzungen des Datenschutzes können aus rechtlicher Warte nicht tel quel auf das Strafrecht übertragen werden. Genau dies wird aber in Art. 12 VE-DSG gemacht, das ist zu korrigieren und der VE-DSG ist auf den Datenschutz zu beschränken.

Daran ändert auch der Passus nichts, dass es sich bei Art. 12 VE-DSG um verstorbene Patienten handelt. Die Einsicht in Patientendokumentationen von Verstorbenen ist in der Praxis ein zunehmendes Handlungsfeld geworden, wobei der Unterzeichnende häufig mit dem kantonalen Gesundheitsamt eine zulässige Lösung erarbeiten muss. Häufig werden dabei die konkreten Umstände abgewogen und die Einsicht wird mit einem Gespräch mit dem zuständigen Arzt in die wesentlichen Unterlagen gewährt. Relativ häufig, wenn nicht ausschliesslich, stehen hinter diesen Einsichtsgesuchen grundsätzlich Verwandte, insbesondere Ehepartner und Kinder. Genau dieser Adressatenkreis, welcher entweder durch den Patienten direkt informiert wurde oder gerade bewusst nicht informiert werden sollte, auch nicht post mortal. Allein daraus, dass jemand mit einer Verstorbenen verwandt oder eng mit ihr verbunden war, kann nicht geschlossen werden, dass die Verstorbene dieser Person ihre Patientendokumentation ohne Einschränkung zugänglich gemacht hätte. Ein Verwandtschaftsverhältnis allein begründet jedenfalls kein genügendes Interesse an einer Offenbarung von Geheimnissen. Dieses Vorgehen hat sich im Kanton Solothurn, vermutlich auch in den anderen Kantonen sehr bewährt. Es erlaubt, die öffentlichen Interessen an der Geheimhaltung zu berücksichtigen. Die Leistungserbringer können sich damit in der Wechselwirkung des DSG und des Strafgesetzbuches rechtskonform verhalten. Eine Geheimniskultur, insbesondere bei haftpflichtfragen, stellt sich überdies in casu nicht, da diese Art von Einsicht anderweitige gesetzliche geregelt ist. Letztlich wird auch nicht klar, wer die Interessenabwägung nach Art. 12 VE-DSG vornehmen soll. Alles in allem ist Artikel 12 VE-DSG sehr unglücklich ausgefallen und dementsprechend ersatzlos zu streichen.

D. Artikeln 13, 14, 15 und 16 sowie 19 VE-DSG

1. Ausgangslage und Gesetzestext

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.
3 Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.
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.
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

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.
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.
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.
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.
2 Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.
3 Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.

Art. 16 Datenschutz-Folgeabklärung
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.

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.

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.

2. Bemerkungen

Wie bereits vorstehend ausgeführt, stellt sich ganz konkret die Frage, was die Revision des DSG für den Arzt und den Patienten bedeutet. Mit der Datenerhebungen MARS bzw. MAS sind unter Berücksichtigung von Artikel 23 und 59a KVG verschiedene Handlungsfelder geöffnet worden, die vor allem Klärungsbedarf ergeben. Damit steht zu Beginn die Frage nach der Funktion des Arztes. Klarheit und unstrittig ist die Qualifikation der Gesundheitsdaten als besonders schützenswerte Personendaten. Nach Artikel 13 ist der Verantwortliche, sprich die Ärztin oder der Arzt in der Pflicht, die betroffene Person über die Beschaffung zu informieren, gleiches dürfte auch für Versicherer gelten (vgl. zweiter Halbsatz von Abs. 1). Nach Massgabe der laufenden Erhebung wäre wohl kein Leistungserbringer in der Lage, dieser Informationspflicht auch nur annährend nach zu kommen, insbesondere ist der Zweck aktuell nicht erkennbar (vgl. Abs. 2). Damit können die Artikel 13 für die Leistungserbringer nicht gelten, was aber weder aus dem Entwurfstext noch aus der Botschaft hervorgeht. Wenn wir davon ausgehen, dass damit Artikel 14 für den Leistungserbringer im Zusammenhang mit MARS bzw. MAS zum Tragen kommt, erscheint die Informationspflicht verhältnismässig formuliert. Gegenwärtig könnte sich der Leistungserbringer wohl auf Art. 14 Abs. 3 lit. a berufen. Damit wäre eine Anpassung nicht nötig. Sollte dies indessen nicht zutreffend sein, so würde Art. 13 für die Leistungserbringer eine aktive Informationspflicht bedeuten, wonach konkret jede Ärztin und jeder Arzt seine Patienten über die Bearbeitung der eigenen Daten informieren muss, auch bezüglich MARS bzw. MAS. Für die Ärztegesellschaften stellt sich damit die Fragen, was aktive Information in casu bedeutet: reicht eine Info auf der Webseite, Wartesaal etc. oder muss die Ärztin bzw. der Arzt jeden Patienten wirklich aktiv mündlich (Sprechstunde) oder schriftlich (mit Schreiben oder auf der Rechnung) informieren. Das wäre ein administrativer Aufwand der kaum zu bewältigen wäre, die Attraktivität der Grundversorger würde nochmals sinken. Überdies stellt sich die Frage, was mit all den Patienten passiert, die mit der Weitergabe der eigenen Daten und der damit verbundenen Aushöhlung des Patientengeheimnisses nicht einverstanden sind. Es ist damit zu rechnen, dass die Patientenorganisation dieses Problem frühzeitig erkennen und dagegen Sturm laufen. Weiter wird in Art. 13 Abs. 2 lit. b in der „oder-Formulierung" von **Kategorien** der bearbeiteten Personendaten gesprochen. Die Formulierung „Kategorie" erinnert an die Schwammigkeit von Art. 59a KVG, doch immerhin ein prominentes Gesetz wenn es um die im Entwurf DSG vielzitierte gesetzliche Grundlage im formellen Sinn geht. Beim Auskunftsrecht in Art. 20 Abs. 2 hingegen, kann die Person unter lit b. die bearbeiteten Personendaten einsehen – hier wird nicht mehr von Kategorien gesprochen. Es bleibt aber eine aktive Plicht der betroffenen Person. Wie ausgeführt, wird es kaum möglich sein, alle Daten genau zu benennen um der Informationspflicht nach Art. 13 gesetzeskonform nachzukommen. Auch aus diesen Gründen verbleibt die Hoffnung, dass für die Leistungserbringer Art. 14 umfassend zum Tragen kommt.

Inwieweit diesbezüglich auch Art. 15 VE-DSG für die Erhebung MARS bzw. MAS mitwirken könnte, kann nicht mit Sicherheit gesagt werden. Es ist davon auszugehen, dass dies für die Erhebungen von Daten bei den Leistungserbringern keine oder nur eine sehr untergeordnete Rolle spielen dürfte. Damit bietet sich hier keine Anpassung an, es sei denn, dieser Bestimmung kommt anstelle von Art. 14 VE-DSG für die Leistungserbringer zur Anwendung.

Indessen sind Art. 16 und 19 VE-DSG von besonderer Tragweite, wenn davon auszugehen ist, dass diese Pflichten, unabhängig vom Ausnahmetatbestand von Artikel 14 VE-DSG, gelten. Während die Ärztin und der Arzt unabhängig eine Dokumentation- und Aufbewahrungspflicht trifft, damit Artikel 19 lit. a VE-DSG ohnehin nachkommen, kann lit b kaum mit realistischen Ressourcen erfüllt werden. Damit bleibt die vage Hoffnung, dass diesbezüglich der letzte Halbsatz zum Tragen kommt wonach eine solche Mitteilung nicht oder nur mit unverhältnismässigem Aufwand möglich ist. Für die Praxis wäre es dienlich, wenn eine solche Überlegung bereits aus den Materialien fliesst. Wie ein Leistungserbringer Artikel 16 gegenwärtig erfüllen könnte, sprich eine Datenschutz-Folgenabschätzung durchführen könnte, ist weder erkennbar noch nachvollziehbar. Hier wird daher der gleiche Ausnahmebestimmung wie in Artikel 19 lit. b VE-DSG – unverhältnismässiger Aufwand – gefordert.

E. Art. 27 VE-DSG Rechtsgrundlagen

1. Ausgangslage und Gesetzestext

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;
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.

2. Bemerkungen

Im Sinne der vorstehenden Erwägungen ist einerseits die Doppelrolle der Leistungserbringer im Gesundheitsrecht konkret in Art. 27 aufzunehmen und andererseits das Arzt- bzw. das Patientengeheimnis konkret weiterhin umfassend zu schützen, während die Strafandrohung und die Sanktion auf dasjenige Mass reduziert werden, wo ein Leistungserbringer trotz ausdrücklicher Einwilligung des Patienten, dessen Daten gestützt auf ein Gesetz im formellen Sin, vorsätzlich nicht weitergibt (echte Unterlassung) bzw. ohne Einwilligung vorsätzlich Dritten, auch Bundesbehörden, zugänglich macht.

F. Art. 52 und 55 VE-DSG

1. Ausgangslage und Gesetzestext (Auszüge)

Art. 52 VE-DSG
Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf Antrag bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er im Rahmen seiner beruflichen Tätigkeit, die die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, oder die er selbst zu kommerziellen Zwecken bearbeitet hat[...]

Art. 55 VE-DSG
Verfolgungsverjährung für Übertretungen
Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.

2. Bemerkungen

Wie unter lic. C, Absatz 2 vorstehend ausgeführt, werden im VE-DSG strafrechtliche Komponenten aufgenommen und unzureichend vermischt. Dies setzt sich in Art. 52 und 55 VE-DSG fort. Art. 52 Abs. 1 VE-DSG übernimmt in leicht geänderter Form den Inhalt von Art. 35 Abs. 1 DSG: Die Strafandrohung verlässt den Rahmen der Busse und wird auf eine Freiheitstrafe erhöht. Aktuell ist der Art. 35 Abs. 1 DSG mit der Bussenandrohung ein Übertretungstatbestand. Indessen würde eine Verletzung von Art. 52 VE-DSG – Strafandrohung einer Freiheitsstrafe bis zu drei Jahren – künftig ein Vergehen darstellen. Gemäss Botschaft sei diese Anpassung im VE-DSG, die an sich im Strafgesetzbuch in Art. 321 StGB zu vollziehen wäre, so gewollt. Durch den Art. 52 VE-DSG soll daher, über die Hintertür, die beruflich Schweigepflicht auf weitere Berufe – ausserhalb von Art. 321 Abs. 1 StGB - ausgedehnt werden. Dieser Systemwechsel muss ausserhalb des VE-DSG diskutiert werden. Dies umso mehr, als dass das prozessuale Pendant des Zeugnisverweigerungsrechts gerade fehlen würde. Wird aber ein Zeugnisverweigerungsrecht wie vorliegend, für nicht angemessen erachtet, so erscheint auch die strafrechtliche Sanktionierung einer Geheimnisverletzung als nicht angemessen. Es ist daher sachlogisch und richtig, auf die Strafbestimmung zu verzichten oder wenn überhaupt, weiterhin in der Ausgestaltung einer Übertretung zu belassen..

Soweit für Art. 55 VE-DSG sachliche Gründen vorliegen, solche sind für uns nicht erkennbar, ist auch auf eine Verlängerung der Verjährungsfrist nach dem allgemeinen Massstab des Strafgesetzbuches, aus Gründen der Rechtssicherheit und auch -klarheit, zu verzichten. Es ist daher von einer dreijährigen Verjährungsfrist auszugehen.

IV. Fazit

Wir erachten den vorliegenden Entwurf für die Gesamtrevision grundsätzlich für zielführend, soweit die vorstehenden Erwägungen berücksichtigt werden und die daraus fliessenden Fragen im Zusammenhang mit der Datenerhebung für und bei Ärztinnen und Ärzten rechtsverbindlich und verständlich, geklärt werden können. Die geforderten Anpassungen sind zu diskutieren und umzusetzen. Daher erscheint es uns unabdingbar, den Dialog zwischen Bund und der Ärzteschaft über die Voraussetzungen zur Sicherstellung des Datenschutzes im Gesundheitswesen auch für den Patientin und den Patienten, weiter zu führen und zu intensivieren, um die verlangte Rechtsunsicherheiten im VE-DSG auszuräumen.

Wir danken für die Berücksichtigung unserer Überlegungen und Argumente, verbunden mit den geforderten Anpassungen.

Mit vorzüglicher Hochachtung

GESELLSCHAFT DER ÄRZTINNEN UND ÄRZTE
DES KANTONS SOLOTHURN (GAeSO)

Der Rechtsberater	Co-Präsident	Co-Präsident
lic. iur. Michel Meier Rechtsanwalt	Dr. med. Florian Leupold	Dr. med. Lukas Meier

Kopie an:
- Vorstand GAeSO
- FMH
- VEDAG

Amstutz Jonas BJ

Von: Kovats Tibor <Tibor.Kovats@grandcasinoluzern.ch>
Gesendet: Sonntag, 26. März 2017 16:40
An: Amstutz Jonas BJ
Betreff: Stellungnahme: Grand Casino Luzern AG
Anlagen: Totalrevision-des-Datenschutzgesetzes_Formular-fuer-Stellungnahme_de_GCL....docx

Sehr geehrter Herr Amstutz

Anbei erhalten Sie eine Stellungsame von uns zur Datenschutzgesetz Totalrevision.

Freundliche Grüsse

Tibor D. Kovats

GRAND CASINO LUZERN AG
Tibor Kovats
Leiter IT / BDSV
Grand Casino Luzern AG
Haldenstrasse 6, Postfach 3264, CH - 6002 Luzern
Tel. +41 41 418 56 56, Fax +41 41 418 56 55

mailto: tibor.kovats@grandcasinoluzern.ch
www.grandcasinoluzern.ch

Ein Unternehmen der Grand Casino Luzern Gruppe

The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

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 : Grand Casino Luzern AG

Abkürzung der Firma / Organisation : GCL

Adresse : Haldenstrasse 6, 6006 Luzern

Kontaktperson : Tibor D. Kovats

Telefon : 041 418 56 56

E-Mail : Datenschutz@GrandCasinoLuzern.ch

Datum : 12.03.2017

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

Allgemeine Bemerkungen ____ 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ 3

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 ____ Fehler! Textmarke nicht definiert.

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ____ Fehler! Textmarke nicht definiert.

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") ____ Fehler! Textmarke nicht definiert.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" ____ Fehler! Textmarke nicht definiert.

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
Grand Casino Luzern AG	Die Totalrevision ist aus unserer Sicht soweit gelungen. Dennoch sind die unten erwähnten Punkte nicht akzeptabel.

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
Grand Casino Luzern AG	DSG	50	1,2,3		Bei Verstoss gegen das Datenschutzgesetz sollte nicht die private Person haften.
Grand Casino Luzern AG	DSG	51	1		Bei Verstoss gegen das Datenschutzgesetz sollte nicht die private Person haften.
Fehler! Verweisquelle konnte nicht gefunden werden.	DSG	52	1		Bei Verstoss gegen das Datenschutzgesetz sollte nicht die private Person haften.
Fehler! Verweisquelle konnte nicht gefunden werden.					
Fehler! Verweisquelle konnte nicht gefunden werden.					

Rii-Seez-Net
Regio Cable Widnau

Gemeindeverwaltung
Gemeinderat
Neugasse 4, Postfach
9443 Widnau

Telefon 071 727 03 24
Telefax 071 727 03 01
gemeinderatskanzlei@widnau.ch
www.widnau.ch

Gemeinde **Widnau**

Eidg. Justiz- und Polizeidepartement
- 3. April 2017
Nr.

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

BA Justiz
E - 4. April 2017
Act

31. März 2017/ck/ss

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 Gemeinde Widnau gerne wahr.
Die Gemeinde Widnau besitzt ein eigenes Kabelnetz und bietet über das Label Rii-Seez-Net Telekommunikationsdienstleistungen an. 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

[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.

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 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

[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.

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.

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 datenschutzrechtlichen 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

---

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.

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	**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
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 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;

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;	dabei ist vom Prinzip auszugehen, dass Fotos grundsätzlich nicht als biometrische 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

VE-DSG	Anträge und Bemerkungen
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; i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des	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 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. **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:

VE-DSG	Anträge und Bemerkungen
Verantwortlichen Personendaten bearbeitet.	„Arbeitnehmer im Sinn von Art. 319 OR sind keine Auftragsbearbeiter").
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.
[6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur	

VE-DSG	Anträge und Bemerkungen
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.	*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). 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.	**Antrag zu Art. 5 Abs. 3 lit. d)**: Streichung der Genehmigungspflicht, Beibehaltung des geltenden Art. 6 Abs. 3 DSG.

VE-DSG	Anträge und Bemerkungen
[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 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. 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. **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,

VE-DSG	Anträge und Bemerkungen
	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 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.	**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.

VE-DSG	Anträge und Bemerkungen
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.
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.

VE-DSG	Anträge und Bemerkungen
[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 gemacht 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.
[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	**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

VE-DSG	Anträge und Bemerkungen
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.	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 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

VE-DSG	Anträge und Bemerkungen
	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), 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.	**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.

VE-DSG	Anträge und Bemerkungen
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 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

VE-DSG	Anträge und Bemerkungen
	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, 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.
[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.	**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

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.	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. **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

VE-DSG	Anträge und Bemerkungen
	"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 [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,

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.	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 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

VE-DSG	Anträge und 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. 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: 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;	**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.

VE-DSG	Anträge und Bemerkungen
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.	
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	**Antrag zu Art. 15 Abs. 2**: Streichen „oder den Erlass einer automatisierten

VE-DSG	Anträge und Bemerkungen
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; 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.	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.
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	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
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. [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	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[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.	
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; 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.	Keine Bemerkungen
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.	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.	
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. [3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.	Keine Bemerkungen
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	**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.

VE-DSG	Anträge und Bemerkungen
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.	
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 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. 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 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. **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.

VE-DSG	Anträge und Bemerkungen
[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 [1] Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern.	**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.
[2] Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.	
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.	**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.

VE-DSG	Anträge und Bemerkungen
[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.	
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. [4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.	**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 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:	**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

VE-DSG	Anträge und Bemerkungen
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; 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.	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.
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.	**Antrag zu Art. 49 lit. d**: Streichen. Wenn der Datenschutzbeauftragte eine Aufsichtsfunktion hat, kann er nicht gleichzeitig auch eine Konsumentenschutzaufgabe erfüllen dürfen.

VE-DSG	Anträge und Bemerkungen
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.	
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 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; b. die es vorsätzlich unterlassen:	**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.

VE-DSG	Anträge und Bemerkungen
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. c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3). [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); 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. 1 lit. b)**: Ändern. Art 13 ist vollständig von der Sanktionierung auszunehmen. **Antrag zu Art. 50 Abs. 1 lit. c)**: Streichen. Ist vollständig von der Sanktionierung auszunehmen. **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. **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;	**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.

VE-DSG	Anträge und Bemerkungen
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. [2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**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 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 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.

VE-DSG	Anträge und Bemerkungen
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 [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.	Keine Bemerkungen
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	**Antrag zu den zivilprozessualen Bestimmungen**: Streichen. Keine Abweichung von den üblichen, prozessualen Regeln im Datenschutzrecht

VE-DSG	Anträge und Bemerkungen
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 …	(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.

Rii-Seez-Net
Regio Cable Widnau

Gemeinde **Widnau**

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse

GEMEINDERAT WIDNAU
Die Gemeindepräsidentin:

Der Gemeinderatsschreiber:

BA Justiz
E -5. April 2017
Act

GGA maur
Genau mit uns.

Eidg. Justiz- und Polizeidepartement
- 4. April 2017
No.

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Binz, 31. März 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 Genossenschaft GGA Maur gerne wahr.

Die GGA Maur 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

Genossenschaft GGA Maur
Binzstrasse 1, CH-8122 Binz, +41 44 982 16 30, Helpline 0800 88 19 11, gga-maur.ch, info@gga-maur.ch

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

---

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.

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 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 ha-

[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.

ben 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.

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

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.

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 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	**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
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 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 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 gesamt*schweizerische 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,

VE-DSG	Anträge und Bemerkungen
	die Bearbeitung 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. [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 ge-

VE-DSG	Anträge und Bemerkungen
	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.
[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

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" Datenbear-

VE-DSG	Anträge und Bemerkungen
	beitern 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), 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.	**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	**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"

VE-DSG	Anträge und Bemerkungen
Auswirkungen auf die betroffene Person hat.	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 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 Persönlich-	**Antrag zu Art. 16**: Streichen. Diese Bestimmung führt in Kombination mit dem drastischen Bestrafungskatalog faktisch zu einer Pflicht, solche Folgeabschät-

VE-DSG	Anträge und Bemerkungen
keit 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. [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.	zungen 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, 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

VE-DSG	Anträge und Bemerkungen
	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.
[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt.	**Antrag zu Art. 17 Abs. 2**: Streichung; In jedem Fall Streichung des Rechts des Beauftragten, die Information des Betroffenen zu verfügen.
[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.	**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,

VE-DSG	Anträge und Bemerkungen
	diese in ihren Persönlichkeiten schützen.
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 Begrün-

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.	dungspflicht 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 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 be-	

VE-DSG	Anträge und Bemerkungen
arbeitet werden; 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: 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;	**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.

VE-DSG	Anträge und Bemerkungen
f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das 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:	**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
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; 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	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem 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 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 For-	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
schung, Planung und Statistik bearbeiten, wenn: 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	Keine Bemerkungen

VE-DSG	Anträge und Bemerkungen
[1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten. [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. [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.	

VE-DSG	Anträge und Bemerkungen
[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 [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	**Antrag zu Art. 41 Abs. 5**: Ergänzung; Die anzeigende Person hat keine Par-

VE-DSG	Anträge und Bemerkungen
Vorgehen und das Ergebnis einer allfälligen Untersuchung.	teistellung und kein Akteneinsichtsrecht. Aufgrund dieser Tatsache könnte 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.	**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
[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; 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

VE-DSG	Anträge und Bemerkungen
	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.
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 unter-	**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
nehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c 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;	**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.

VE-DSG	Anträge und Bemerkungen
f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert. [2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.	**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. **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.

VE-DSG	Anträge und Bemerkungen
10. Abschnitt: Schlussbestimmungen	
Art. 57 Vollzug durch die Kantone [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.	Keine Bemerkungen
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....	**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
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 ...	

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

Beat J. Ambühl
Geschäftsführer

Daniel Bechter
Leiter Finanzen & Controlling

Genossenschaft GGA Maur
Binzstrasse 1, CH-8122 Binz, +41 44 982 16 30, Helpline 0800 88 19 11, gga-maur.ch, info@gga-maur.ch

GOLDBACH
GROUP

Vorab per Email an jonas.amstutz@bj.admin.ch
Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Küsnacht, 05.04.2017

Stellungnahme der Goldbach Group AG zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Die Goldbach Group AG ist die an der SIX Swiss Exchange kotierte Muttergesellschaft der in der Schweiz, Deutschland und Österreich tätigen Goldbach Gruppe. Die Unternehmen der Goldbach vermarkten und vermitteln Werbungen in privaten elektronischen Medien mit dem Fokus auf TV, Radio, Digital out of Home, Online sowie Suchmaschinen- und Mobile-Marketing. Als unabhängiger Aggregator bietet Goldbach ihren Kunden unter anderem auch Werbeplätze an, die aufgrund des Einsatzes von anonymen Nutzerdaten an gewünschte Zielgruppen unabhängig von ihrem Standort individuell ausgespielt werden können. Hierzu setzt Goldbach - wie auch viele andere schweizerische oder europäische Werbevermittler - datengestützte Technologien ein. Dieser Einsatz von datengestützten Technologien soll einerseits den Werbetreibenden ermöglichen, ihr Zielpublikum besser zu erreichen und andererseits den Publishern dabei helfen, seine elektronischen Medien durch den Verkauf von Anzeigen zu fördern und zu monetarisieren. Dies dient vor allem auch dem Überleben von kleineren Medienhäusern und der Medienvielfalt in der Schweiz.

Goldbach ist sich beim Einsatz von datengestützten Technologien den damit verbundenen datenschutzrechtlichen Gefahren bewusst und setzt sich seit vielen Jahren für einen sicheren, geschützten und respektvollen Umgang mit Verbraucherinformationen ein. Goldbach hat sich hierzu auch als erstes Unternehmen der Schweiz strengen selbstregulatorischen Vorschriften zur Einhaltung höchster Datenschutzstandards unterstellt und ist bereits seit dem Jahre 2014 Mitglied der EDAA (European Interactive Digital Advertising Alliance) und bei dieser auch zertifiziert. Daneben ist Goldbach Mitglied des IAB Europe, des IAB Switzerland, der schweizerischen Dachorganisation der kommerziellen Kommunikation, der IGEM sowie weiteren im Umfeld der Werbewirtschaft tätigen Verbänden.

1. Einleitende Gedanken zum Datenschutz und dem vorliegenden Gesetzesentwurf

Für Goldbach wie auch die gesamte schweizerische Werbewirtschaft inklusive der auf Werbefinanzierung angewiesenen Medien ist die Nutzung von Personendaten, wie auch von weiteren zur nutzungsbasierten Auslieferung von Werbungen benötigten anonymen Nutzerdaten, von grösster Wichtigkeit. Eine Einschränkung dieser Marktteilnehmer über unnötig strenge datenschutzrechtliche Regelungen kann für viele Marktteilnehmer existenzbedrohend sein und übertriebene Regelungen können zu einem Verlust der Medienvielfalt in der Schweiz führen.

Der nun vorliegende Entwurf geht in verschiedenen Punkten klar zu weit. Aus Sicht der Goldbach wäre eine Teilrevision des bestehenden Datenschutzgesetzes - welches sich auch im digitalen Zeitalter stets bewährt hat - ausreichend gewesen. Eine Teilrevision wäre letztlich auch für die Beibehaltung eines mit der EU gleichwertigen Datenschutzes ausreichend gewesen, ist ja im internationalen Verhältnis mit der EU auch „nur" das revidierte Übereinkommen des Europarates (SEV 108) zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogerner Daten und nicht die DSGVO verbindlich. Die Anforderungen des SEV 108 wären denn auch mit wesentlich weniger weitreichenden Regelungen als im Vorentwurf, respektive Angleichungen im heutigen DSG, erfüllt worden. Nichts desto trotz ist die Beibehaltung eines gegenüber der EU gleichwertigen Datenschutzes unabdingbar.

In diesem Zusammenhang ist daher festzustellen, dass der vorliegende Gesetzesentwurf in vielen Punkten weit über die vor rund einem Jahr in Kraft gesetzte DSGVO hinaus geht Die Schweiz bürdet sich durch die strengeren Datenschutzregeln einen massiven Standortnachteil auf. So ist insbesondere nicht einzusehen, warum über die DSGVO hinausgehende Informationspflichten eingeführt und Straftatbestände festgehalten werden sollen, die in der DSGVO nicht sanktioniert werden. Vor allem die vollkommen überzogenen Informationspflichten werden zu einem Übermass an administrativem Aufwand für viele schweizerische KMU führen.

Die Tatsache, dass viele Schweizer Unternehmen insbesondere in den direkt angrenzenden Nachbarländern tätig sind, macht es notwendig, dass die schweizerischen Datenschutzregulierungen keinesfalls über die in der DSGVO gesetzten Regelungen hinausgehen. Namentlich für Unternehmen wie Goldbach wären andernfalls zwei derart unterschiedliche datenschutzrechtliche Regelungen im EU Raum und der Schweiz zu beachten. Darüber hinaus hätten die schweizerischen Niederlassungen der Goldbach erhöhte Regulierungen einzuhalten! Diese Sachlage steht diametral zu dem vom Bundesrat verabschiedeten Bericht „Rahmenbedingungen der digitalen Wirtschaft", worin dieser verlauten lässt: **„Der digitale Wandel bietet grosse Chancen für die Schweizer Volkswirtschaft. Der Bundesrat will diese nutzen, um Arbeitsplätze und Wohlstand zu sichern.".** Mit dieser Botschaft des Bundesrates lässt sich der jetzige Vorentwurf nicht vereinbaren.

2. Zu einzelnen Punkten im Vorentwurf in Kürze

Personendaten: Es ist zu begrüssen, dass die Definition der Personendaten nach neuem Recht wie bisher beibehalten werden soll. Insbesondere ist es wichtig, dass keine Ausdehnung auf Sammlungen von anonymen oder pseudonymen Nutzerdaten geschieht, welche heute im Zusammenhang mit der Werbeindustrie von grosser Wichtigkeit sind. Die Beibehaltung der bundesgerichtlichen Rechtsprechung und der Anwendung der sogenannten relativen Methode bei der Ermittlung, ob eine betroffene Person bestimmbar ist oder nicht, ist wichtig und sichert der Schweiz künftig auch die Konkurrenzfähigkeit gegenüber dem EU-Raum.

Profiling: In Bezug auf die Definition des Profiling in Art. 3 Abs. 1 lit. f VE DSG muss sichergestellt werden, dass darunter nicht auch nicht-personenbezogene Daten fallen. Dies würde die Werbeindustrie sowie alle Medienanbieter in der Schweiz gegenüber dem EU Raum massiv benachteiligen. Da für das Profiling eine ausdrückliche Einwilligung des Nutzers vorausgesetzt wird, wäre bei einer Ausdehnung des Begriffs für das Setzen von Cookies oder das Sammeln von ähnlichen Daten zur Nutzungserforschung anonymer Personen eine ausdrückliche Einwilligung erforderlich. Damit würden sämtliche Internetmedien vor praktisch unüberwindbare Probleme gestellt. Es ist in der Definition des Profiling daher zwingend das Wort „Daten" neben Personendaten zu streichen.

Goldbach Group AG I Seestrasse 39 I 8700 Küsnacht-Zürich I Schweiz I T +41 44 914 91 00 I F +41 44 914 93 60 I www.goldbachgroup.com

Informations- und Auskunftspflichten: Die neuen Informations- und Auskunftspflichten im Vorentwurf sind sehr weitreichend und werden in dieser Form grossen teils unnötigen administrativen Aufwand vor allem für kleinere KMU zu Folge haben. Diese Pflichten sind daher auf das Notwendigste zu kürzen und dürfen nicht weiter gehen, als die in der DSGVO festgehaltenen Informations- und Auskunftspflichten. Es kann beispielsweise nicht angehen, dass jeder Wechsel der von einem Datenverarbeiter beigezogenen Datenverarbeitungsbeauftragten eine Informationspflicht an alle Betroffenen nach sich zieht. Auch eine stets kostenlose Auskunft von betroffenen Personen über die von ihr bearbeiteten Daten birgt ein grosses Missbrauchspotential und ist in geeigneter Weise auf Fälle einzuschränken, die in einer Interessenabwägung auch wirklich Kostenlosigkeit rechtfertigen.

Definition der Einwilligung: Die Definition der Einwilligung ist in der vorliegenden Form noch klärungsbedürftig. Die Anforderungen an die Einwilligung sind unbedingt an diejenigen der DSGVO anzugleichen. Dabei sollte eine Einwilligung zwingend auch über die Annahme von Allgemeinen Geschäftsbedingungen möglich sein.

Weitere zu überarbeitende Themen in Kürze: Der Auslandtransfer wurde im Vorentwurf unnötig verkompliziert. Die neuen Notifikations- und Genehmigungspflichten gehen zu weit und sie machen den Transfer langwierig. Zudem drohen empfindliche Sanktionen bei Verstössen, die es in dieser Form in der DSGVO nicht gibt.

Weiter sind die neuen Regelungen über Daten verstorbener Personen aus unserer Sicht überflüssig. Teilweise kommen den Erben aufgrund dieser neuen Regelungen weitergehende Rechte zu, als sie der Verstorbene zu Lebzeiten hatte. Eine diesbezügliche Regelung wäre zudem besser im ZGB aufgehoben.

Die Regelungen zu einer Datenschutzfolgenabschätzung sind grundsätzlich zu begrüssen, jedoch werden nach dem heutigen Wortlaut der diesbezüglichen Bestimmungen allzu viele Fälle davon erfasst. Das Abstützen auf den Begriff „erhöhte Risiken", welche eine Datenschutzfolgeabschätzung erforderlich machen, geht definitiv zu weit und eine Datenschutzfolgeabschätzung sollte nur in Fällen notwendig sein, in denen ein wirklich hohes Risiko vorliegt. Erhöhte Risiken werden in der Praxis rasch vorliegen, zudem sind auch die Anforderungen für eine Datenschutzfolgeabschätzung im Vorentwurf höher als dies in der DSGVO der Fall ist.

Schliesslich gehen die neuen Regelungen in Bezug auf die Aufsicht und die Sanktionen im Vorentwurf eindeutig zu weit. Der primäre Ansatz, welcher auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abzielt ist abzulehnen und wird in hohem Masse die Innovationsfreudigkeit des Schweizer Marktes hemmen. Innovative Persönlichkeiten werden vor Neuentwicklungen zurückschrecken, da sie drastischen strafrechtlichen Risiken ausgesetzt werden. Das Sanktionensystem ist daher nochmals grundlegend zu überarbeiten und es ist dabei darauf zu achten, dass gegenüber der DSGVO nicht weitergehende Strafbestimmungen festgesetzt werden.

Im Übrigen möchten wir auch auf die Stellungnahmen des IAB Switzerland, sowie des KS/CS verweisen, welche wir weitgehend teilen. Dies betrifft insbesondere die Forderung, dass das Datenschutzgesetz **nur insoweit zu revidieren ist, als dies die internationalen Vorgaben zwingend erfordern.** Jeder darüber hinausgehender „Swiss Finish" ist strikte abzulehnen.

Goldbach Group AG I Seestrasse 39 I 8700 Küsnacht-Zürich I Schweiz I T +41 44 914 91 00 I F +41 44 914 93 60 I www.goldbachgroup.com

GOLDBACH
GROUP

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

Freundliche Grüsse

Goldbach Group AG

Michael Frank
CEO

Philipp Stamm
Head of Legal

Anlagen erwähnt

Goldbach Group AG I Seestrasse 39 I 8700 Küsnacht-Zürich I Schweiz I T +41 44 914 91 00 I F +41 44 914 93 60 I www.goldbachgroup.com

Groupe Mutuel
Assurances
Versicherungen
Assicurazioni

Département fédéral de justice et police
DFJP
Palais fédéral ouest
3003 Berne

Par courriel jonas.amstutz@bj.admin.ch

Martigny, le 30 mars 2016

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données – Prise de position du Groupe Mutuel

Madame la Conseillère fédérale, Mesdames, Messieurs,

En date du 21 décembre 2016, le DFJP a ouvert la procédure de consultation susmentionnée. Vous trouverez ci-joint la prise de position du Groupe Mutuel qui sera délivrée également par courriel à l'adresse susmentionnée.

Nous vous remercions de nous avoir donné l'opportunité de faire valoir notre point de vue et vous prions d'agréer, Madame la Conseillère fédérale, Mesdames, Messieurs, nos respectueuses salutations.

Groupe Mutuel

Dr Thomas J. Grichting
Directeur - Secrétaire général

p.o. GAJ
Geneviève Aguirre-Jan
Experte Senior

Annexe mentionnée

Votre contact: Geneviève Aguirre-Jan – Secrétariat général
Tél. 058 758 25 29 - Fax 0848 803 123
gaguirrejan@groupemutuel.ch - www.groupemutuel.ch

Groupe Mutuel
Rue des Cèdres 5 - Case postale - CH-1919 Martigny

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 : Groupe Mutuel Association d'Assureurs

Abréviation de la société / de l'organisation : Groupe Mutuel

Adresse : Rue des Cèdres 5, 1920 Martigny

Personne de référence : Mme Geneviève Aguirre-Jan

Téléphone : 058 758 25 29

Courriel : gaguirrejan@groupemutuel.ch

Date : 30.03.2017

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

Remarques générales _____ **3**

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 _____ **4**

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 :
Groupe Mutuel	La présente révision a le mérite d'adapter la législation aux évolutions technologiques en matière de données, ainsi qu'à l'environnement législatif international. Toutefois, elle présente certaines faiblesses (cf. infra) qu'il convient de relever et de corriger, afin d'en assurer une application optimale, compte tenu du fait que le traitement des données des assurés est au cœur de l'activité d'assurance que ce soit à la conclusion d'un contrat ou lors de la gestion des sinistres, mais aussi dans les activités de marketing. **La proportionnalité** La révision ne se focalise pas sur les menaces principales pouvant peser sur la sphère privée. Certaines mesures n'apportent pas de plus-value significative à ce sujet (la violation d'un devoir d'information ne représente pas une menace pour la sphère privée tout en étant assortie d'une sanction pénale conséquente). Les sanctions pénales sont contre-productives, tant elles sont sévères (cf. commentaires des art. 50 à 55). **La praticabilité et les coûts** Certaines mesures ne tiennent pas compte de la praticabilité (p.ex. droit d'être entendu dans le cadre des décisions automatiques – art. 15 al. 2), ni des coûts de mise-en-œuvre liés à l'augmentation des états-majors. **La cohérence avec l'environnement international** L'environnement juridique suisse est parfois plus sévère que l'international (par ex. l'obligation de donner un consentement exprès en cas de profilage, cf. art. art. 4 al. 6). **L'harmonisation des lois d'assurances sociales avec les nouvelles contraintes de la LPD** Les bases légales de la LAMal, LAA et LPP doivent être aménagées afin de répondre aux nouvelles exigences du projet de loi. Le Groupe Mutuel propose à ce sujet une adaptation des articles 84 et 84a LAMal. En ce qui concerne l'adaptation des articles 85 et 86a LPP et 96 et 97 LAA, il se rallie aux propositions de l'ASA. Dans l'ensemble le Groupe Mutuel est favorable à la révision de la loi, dans la mesure où les imperfections sont corrigées. Les propositions d'amélioration figurent ci-dessous.

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 :
Groupe Mutuel	LPD	3			**Définitions** Certains termes devaient être définis, tels que : conseiller interne à la protection des données, risque accru, décision automatisée.
Groupe Mutuel	LPD	4	6		**Principes** <u>L'obligation d'obtenir des consentements exprès de la personne concernée en cas de profilage</u> L'assurance travaille sur la base de profilages. Si chaque profilage devait nécessiter une demande de consentement de la part de la personne concernée, la charge administrative liée serait énorme. Le profilage doit donc être exclu. Il est à noter que le droit européen ne prévoit pas de consentement exprès à donner en cas de profilage. A notre avis, le consentement devrait pouvoir être obtenu de façon générale (par ex. clause particulière dans les CGA). <u>Proposition</u> 6 Lorsque son consentement est requis pour justifier le traitement de données personnelles, la personne concernée ne consent valablement que si elle exprime sa volonté librement, clairement et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles, ~~ou en cas de profilage,~~ son consentement doit être au surplus exprès.
Groupe Mutuel	LPD	5	5		**Communication de données personnelles à l'étranger** <u>Délai de communication du PFPDT</u> Les modalités de la procédure auprès du PFPDT ne sont pas adaptées quant au délai accordé au PFPDT pour communiquer sa décision sur les garanties fournies pour transférer les données à

					l'étranger. Proposition 5 Dans un délai de ~~six mois~~ 30 jours à compter de la réception du dossier complet des garanties standardisées visées à l'al. 3, let. c, ch. 1 ou des règles d'entreprise contraignantes visées à l'al. 3, let. d, ch. 1, le préposé communique au responsable du traitement ou au sous-traitant si celles-ci sont approuvées ou non.
Groupe Mutuel	LPD	5	6		**Communication de données personnelles à l'étranger** Obligation d'informer le PFPDT Cette obligation n'existe pas dans le cadre du règlement UE 2016/679. Cette obligation occasionne de frais disproportionnés. Proposition ~~6 Le responsable du traitement ou le sous-traitant qui recourt aux garanties standardisées visées à l'al. 3, let. c, ch. 2, en informe le préposé. Il lui communique les règles d'entreprise contraignantes visées à l'al. 3, let. d, ch. 2.~~
Groupe Mutuel	LPD	6	2		**Communication exceptionnelle de données personnelles à l'étranger** Obligation d'informer le PFPDT Le coût de cette disposition est disproportionné. Par ailleurs, une telle obligation n'existe pas dans le droit européen. Proposition ~~2 Le responsable du traitement ou le sous-traitant informe le préposé des communications de données personnelles effectuées en vertu de l'al. 1, let. b, c et d.~~
Groupe Mutuel	LPD	7	3		**Sous-traitance**

					Sous-traitance, 2e niveau – accord obligatoire La procédure prévue est trop lourde à exécuter. Une simple information au responsable du traitement suffit. Proposition 3 Le sous-traitant ne peut lui-même sous-traiter un traitement à un tiers ~~qu'avec l'accord écrit préalable~~ qu'après avoir informé le responsable du traitement.
Groupe Mutuel	LPD	8 / 9			**Recommandations de bonnes pratiques et respect** Le Groupe Mutuel salue le fait que la loi pose le principe de la collaboration du PFPDT avec les milieux intéressés pour l'élaboration des recommandations de bonnes pratiques. Toutefois il ne se justifie pas que le PFPDT acquiert le statut d'un « quasi-législateur ». Le caractère non contraignant des recommandations doit être clairement indiqué. Dans cette optique, Le PFPDT n'a pas non plus de pouvoir d'approbation des recommandations émises par les milieux intéressés ou les responsables du traitement. Proposition (art. 8) 1 Le préposé édicte des recommandations de bonnes pratiques non contraignantes qui précisent les dispositions de protection des données. Il associe les milieux intéressés et tient compte des particularités des différents domaines concernés ~~ainsi que du besoin de protection des personnes vulnérables~~. 2 Les responsables du traitement ainsi que les milieux intéressés peuvent ~~compléter les recommandations du préposé ou~~ élaborer leurs propres recommandations. Ils peuvent consulter le préposé lors de leurs préparations ~~les faire approuver par le préposé~~. ~~Ce dernier donne son approbation lorsque les recommandations sont conformes aux dispositions de protection des données.~~ ~~3 Le préposé publie les recommandations de bonnes pratiques qu'il a édictées ou approuvées.~~

					Proposition (art. 9) Suppression
Groupe Mutuel	LPD	11	1		**Sécurité des données personnelles** L'avant-projet ne précise pas l'étendue des mesures techniques et organisationnelles. Le terme « approprié » laisse sous-entendre qu'il y a lieu de faire une pesée d'intérêt entre les coûts et le niveau de sécurité. En accord avec le Règlement UE 2016/679, il convient de tenir compte d'un degré de risque, surtout que les mesures de sécurité en matière technique peuvent être très onéreuses. Il serait par ailleurs disproportionné de prévoir les mêmes mesures de protection technique pour toutes les données personnelles traitées. Proposition 1 Les responsables du traitement et les sous-traitants doivent assurer la sécurité des données personnelles. Celles-ci doivent être protégées en fonction du risque encouru contre tout traitement non autorisé et toute perte, par des mesures organisationnelles et techniques appropriées.
Groupe Mutuel	LPD	13	4		**Devoir d'informer lors de la collecte de données personnelles** Il est globalement souhaité que l'information et les communications puissent se faire de façon générale et standard par le biais des CGA, les propositions d'assurance, etc., faute de quoi la mise en œuvre de des obligations prévues aux alinées 1, 3 s'avérera coûteuse. Cette possibilité d'ailleurs est évoquée dans le rapport. L'alinéa 4 prévoit pour sa part une obligation non seulement coûteuse, mais aussi susceptible d'entraîner des violations du secret d'affaire. Il doit donc être supprimé. Proposition ~~4 Lorsqu'un traitement est confié à un sous-traitant, le responsable du traitement communique à la personne concernée son identité et ses coordonnées, ainsi que les données personnelles ou les catégories de données personnelles concernées.~~
Groupe Mutuel	LPD	13	5		**Devoir d'informer lors de la collecte de données personnelles**

					Cette obligation est impraticable et occasionne des frais administratifs conséquents. Sa suppression est demandée. Ex : En cas d'achat par une compagnie d'assurance d'une liste d'adresses de personnes physiques (prospects), celles-ci devrait informer ces personnes lors de l'enregistrement des données. Proposition ~~5 Si les données personnelles ne sont pas collectées auprès de la personne concernée, celle-ci doit être informée au plus tard lors de leur enregistrement ou, en l'absence d'un enregistrement, lors de la première communication à un tiers.~~
Groupe Mutuel	LPD	14	3		**Exceptions au devoir d'informer et restrictions** Dans certains cas de figure le responsable du traitement peut être obligé de prendre des informations de la part de tiers, sans avoir l'autorisation de les transmettre à la personne concernée. Les assureurs sont contractuellement tenus au secret. Par ex. dans le droit de la responsabilité, le traitement d'un sinistre nécessite pour l'assureur de travailler tant sur les données du preneur d'assurance que celles de la partie lésée. Ces données ne sont pas toujours strictement séparables. Si l'assureur devait toujours informer la personne concernée, il violerait, dans certains cas de figure, le contrat d'assurance conclu avec le preneur d'assurance. Proposition 3 Le responsable du traitement peut restreindre ou différer la communication des informations, ou y renoncer, si l'une des conditions suivantes est remplie: a. une loi au sens formel ou un contrat le prévoit ; b. les intérêts prépondérants d'un tiers l'exigent.
Groupe Mutuel	LPD	14	4	a	**Exceptions au devoir d'informer et restrictions** La personne privée qui communique des données personnelles à des tiers ne peut pas restreindre ou différer la communication d'informations (cf. art. 14 al. 4). Or, dans le cadre d'un groupe, la

					communication de données est par définition une communication à des tiers. Dès lors, les sociétés membres d'un groupe ne bénéficient plus des restrictions légales à l'obligation d'informer. L'art. 14 al. 4 let. a doit être modifié. <u>Proposition</u> 4 Il est au surplus possible de restreindre, de différer la communication des informations ou d'y renoncer dans les cas suivants : a. si le responsable du traitement est une personne privée, lorsque ses intérêts prépondérants l'exigent ~~et à condition qu'il ne communique pas les données personnelles à des tiers~~ ; b. si le responsable du traitement est un organe fédéral : 1. si un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieurs de la Confédération l'exige, ou 2. si la communication des informations risque de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative.
Groupe Mutuel	LPD	15	2		**Devoir d'informer et d'entendre la personne concernée en cas de décision individuelle automatisée** Cette obligation est lourde et coûteuse à mettre en place (alourdissement des états-majors). Toutefois, elle prévue dans le droit européen (STE no 108). Elle doit donc être restreinte le plus possible dans son application. La LPD a notamment pour objectif de protéger la sphère privée et d'empêcher l'emploi abusif de données. Une décision individuelle automatisée représente-t-elle vraiment une menace pour la sphère privée ? Tous les contrats déploient des effets juridiques. En l'espèce, la conclusion de contrat en ligne seraient soumis à l'obligation d'entendre la personne concernée, ce qui n'est pas praticable. Il est proposé que le droit d'être entendu n'aille pas au-delà de ce qui est prévu dans la convention STE no 108, art. 8, al. 1, let. a « Toute personne a le droit : a. de ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte. (pas de proposition de texte).

Groupe Mutuel	LPD	16	1		**Analyse d'impact relative à la protection des données** L'analyse d'impact est requise lorsque le traitement envisagé est susceptible d'entraîner un risque accru pour la personnalité et les droits fondamentaux de la personne concernée. La loi ne définit pas la notion de « risque accru ». Faute de définition, il est proposé de la remplacer par la notion de « risque élevé » (« hohes Risiko »). Proposition 1 Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité et les droits fondamentaux de la personne concernée, le responsable du traitement ou le sous-traitant procède au préalable à une analyse d'impact.
Groupe Mutuel	LPD	16	3		**Analyse d'impact relative à la protection des données** La procédure de communication au PFPDT des résultats de l'analyse d'impact doit être supprimée (cf. al. 3). Il s'agit d'une procédure qui n'est pas prévue par la convention STE no 108 (cf. art. 8bis al. 2). Dans l'hypothèse où cette procédure serait maintenue, le délai de 3 mois est trop long et doit être raccourci (proposition : 30 jours). Proposition ~~3 Le responsable du traitement ou le sous-traitant communique les résultats de l'analyse d'impact au préposé, ainsi que les mesures envisagées.~~
Groupe Mutuel	LPD	16	4		**Analyse d'impact relative à la protection des données** La suppression de l'al. 3 entraîne celle de l'al. 4. Proposition ~~4 Si le préposé a des objections concernant les mesures envisagées, il en informe le responsable du traitement ou le sous-traitant dans un délai de trois mois dès la réception de toutes les informations nécessaires.~~

Groupe Mutuel	LPD	17	1		**Notification des violations de la protection des données** Seules les violations présentant des risques élevés pour la personne concernée doivent être annoncées. <u>Proposition</u> 1 Le responsable du traitement notifie sans délai au préposé tout traitement non autorisé ou toute perte de données personnelles, à moins que la violation ne présente vraisemblablement pas de risques élevés pour la personnalité et les droits fondamentaux de la personne concernée.
Groupe Mutuel	LPD	19	1	b	**Autres obligations** L'obligation d'annoncer aux destinataires auxquels des données ont été communiquées de toute rectification, effacement, ou destruction des données personnelles, de toute violation de la protection des données ainsi que de toute limitation du traitement, est impraticable et onéreuse. Par ailleurs, cette obligation n'est pas prévue par la convention STE no 108. Elle doit donc être supprimée. <u>Proposition</u> ~~b. d'informer les destinataires auxquels des données ont été communiquées de toute rectification, effacement, ou destruction des données personnelles, de toute violation de la protection des données ainsi que de toute limitation du traitement selon l'art. 25, al. 2 ou 34 al. 2, à moins qu'une telle information s'avère impossible ou exige des efforts disproportionnés.~~
Groupe Mutuel	LPD	20	3		**Droit d'accès** <u>Droit d'accès en cas de décision individuelle automatisée</u> L'information de l'assuré concernant l'existence de décision individuelle est prévue aux articles 20 al. 2 let. e et 15 al. 1. L'alinéa 3 doit être biffé dans la mesure où il constitue une régulation excessive, représente une restriction à la liberté commerciale et pourrait occasionner des violations du secret des affaires. Ainsi, dans le domaine de l'assurance, le calcul des primes d'un effectif relève du secret des affaires. Cette obligation imposerait à l'assureur de dévoiler les critères de calcul des primes.

					Proposition ~~3 Lorsque le traitement de données personnelles conduit à une décision, en particulier à une décision individuelle automatisée, la personne concernée reçoit des informations sur le résultat de la décision, la manière dont elle a été obtenue ainsi que sur ses conséquences.~~
Groupe Mutuel	LPD	23	2	c	**Atteintes à la personnalité** L'obtention d'un consentement „exprès" pour du profilage n'est pas réalisable pour un portefeuille de clientèle. Les contrats d'assurance sont en vigueur sur une longue période. En cas de refus d'un client, celui-ci doit être exclu des autres profilages, ce qui n'est pas réalisable. Par ailleurs, cet alinéa va plus loin que la réglementation européenne. Il est dommageable à l'activité des assureurs, qui sont des acteurs majeurs de l'économie suisse. Il est proposé de remplacer le consentement par une information. Proposition 2 Constitue notamment une atteinte à la personnalité le fait de : a. traiter des données personnelles en violation des principes définis aux art. 4 à 6 et 11 ; b. traiter des données personnelles contre la manifestation expresse de la volonté de la personne concernée ; c. communiquer à des tiers des données sensibles ; d. faire du profilage sans ~~le consentement exprès de~~ en informer la personne concernée.

Groupe Mutuel	LPD	44	3		**Procédure** Dans la procédure administrative, les recours contre les mesures provisoires ont un effet suspensif qui peut dans des cas particuliers être retiré (art. 55 PA). Il n'y a pas de motif de s'écarter de cette règle. Le rapport n'explique d'ailleurs pas une exclusion générale de l'effet suspensif. Le refus d'accorder l'effet suspensif peut avoir des effets conséquents dans la pratique, par exemple en cas d'empêchement d'utiliser le système. Ainsi, les concurrents qui auraient une pratique similaire pourraient poursuivre celle-ci, alors que l'entreprise incriminée ne le pourrait déjà plus. Proposition 3 Les recours formés contre les mesures provisoires visées à l'art. 42 ~~n'ont pas~~ ont un effet suspensif.
Groupe Mutuel	1	45			**Obligation de dénoncer** Le droit européen ne prévoit pas une telle obligation d'annonce (STE no 108). La convention STE no 108 ainsi que la directive UE 2016/680 prévoient la possibilité d'annoncer aux autorités judiciaires les violations des dispositions de la protection des données. Il n'y a donc pas lieu d'aller au-delà du droit européen. Proposition Art. 45 Dénonciation des violations des dispositions de la protection des données Le préposé ~~est tenu de dénoncer aux autorités de poursuite pénale les infractions poursuivies d'office dont il a connaissance dans l'exercice de ses fonctions.~~ Peut dénoncer les violations des dispositions de la protection des données aux autorités de poursuite pénale.

Groupe Mutuel	LPD	50 à 55			**Les dispositions pénales** Les dispositions sont de natures pénales, alors que le droit européen prévoit d'abord des sanctions administratives. Si le niveau des sanctions est cohérent avec le niveau des peines pécuniaires prévues par le droit européen, elle concerne d'abord les personnes et non pas les entreprises. Dès lors, recruter des employés qualifiés exposés à de telles sanctions pourrait s'avérer à l'avenir difficile, compte tenu du nombre important de dispositions de la LPD assorties de sanctions pénales. Par ailleurs, les peines sont disproportionnées. La LPD a pour but de protéger la sphère privée et l'emploi abusif des données. Les sanctions pénales devraient se focaliser sur les menaces essentielles sur la sphère privée. Le système de sanction doit être revu dans son ensemble et de la façon suivante : - Les sanctions pénales doivent être prévues pour les personnes morales et non physiques (sous réserve des actes criminels intentionnels de collaborateurs, tels que le vol de données). - Seul le comportement intentionnel devrait être sanctionné. - Le catalogue des obligations assorties de sanctions devrait être réduit.
Groupe Mutuel	LPD	52			**Violation du devoir de discrétion** Cet article est trop large et trop vague. Par ailleurs, il devrait figurer dans le code pénale et non dans la LPD. Il apporte une grande insécurité notamment aux collaborateurs des assurances maladie sociales puisque l'art. 54 al. 1 lit. D LSAMal sanctionne déjà la violation de cette obligation par une amende pouvant aller jusqu'à CHF 500 000.-.
Groupe Mutuel	LPD	59			**Disposition transitoire** Le délai transitoire ne concerne que l'introduction des études d'impact (art. 16), la protection des données dès la conception et par défaut (art. 18) et la documentation du traitement des données personnelles (art. 19a). D'autres éléments nécessiteraient l'application d'un délai transitoire, par ex, les nouvelles obligations en matière d'information, d'accès aux données, de décision individuelle

					automatique. Compte tenu du nombre de nouvelles obligations (mise à jour de la documentation contractuelle, adaptation des processus, etc.), les dispositions transitoires devraient s'appliquer de façon générale. Par ailleurs, la loi ne doit pas avoir d'effet rétroactif.
Groupe Mutuel	LAMal	84	1		**Traitement de données personnelles** La sécurité du droit nécessite l'unification de la terminologie avec celle de la LPD. Par ailleurs, dans le cadre du traitement des données personnelles par les organes fédéraux, l'art. 27 al. 2 impose la création d'une base légale formelle en matière de profilage et de décision automatisée. Il sied de noter que les assureurs maladie procèdent déjà à l'heure actuelle à des contrôles et donc à des décisions automatisées pour traiter l'énorme nombre de factures. Sans base légale, ce système ne pourrait plus être maintenu ce qui engendrerait des coûts démesurés. De plus, nous estimons que les bases légales par rapport aux mesures de Managed Care, notamment le Case Management ainsi que dans le cadre des modèles alternatifs d'assurance sont insuffisant au vue des dispositions de l'avant-projet LPD. Pour cette raison, nous proposons de les créer. <u>Proposition</u> 1 Les organes chargés d'appliquer la présente loi ou la LSAMal, d'en contrôler ou surveiller l'exécution sont habilités à traiter et à faire traiter les données personnelles, y compris les données personnelles sensibles au sens de l'art. 3 let. a et c LPD, d'effectuer des profilages au sens de l'art. 3 let. f LPD et de prendre des décisions individuelles automatisées au sens de l'art. 15 al. 1 LPD qui leur sont nécessaires pour accomplir les tâches que la présente loi ou la LSAMal leur assignent, notamment pour: a. veiller au respect de l'obligation de s'assurer; b. calculer et percevoir les primes; c. établir le droit aux prestations, les calculer, les allouer et les coordonner avec celles d'autres assurances sociales; c. bis. procéder à des mesures de Managed Care c. ter. gérer des modèles alternatifs d'assurance en collaboration avec les fournisseurs de prestations et leurs représentants ;

					d. établir le droit à des réductions de primes au sens de l'art. 654, les calculer et les verser; e. faire valoir une prétention récursoire contre le tiers responsable; f. surveiller l'exécution de la présente loi; g. établir des statistiques; h. attribuer ou vérifier le numéro d'assuré AVS; i. calculer la compensation des risques.
Groupe Mutuel	LAMal	84	2		**Traitement de données personnelles** L'art. 27 al. 3 permet aux organes fédéraux de traiter des données personnelles sans bases légales, sous des conditions strictes. Afin d'éviter que le « case management » ne puisse plus être autorisé en raison des nouvelles dispositions de la LPD (le case management ne fait pas partie des tâches déléguées aux assureurs par la loi, mais d'efforts de réinsertions organisés par les assureurs LAMal), un alinéa 2 est ajouté, afin de créer une base légale ad hoc. Proposition 2 Les organes chargés d'appliquer la présente loi sont habilités à traiter et à faire traiter les données personnelles, y compris les données sensibles au sens de l'art. 3 let. a et c LPD, d'effectuer des profilages au sens de l'art. 3 let. f LPD, afin de prendre les mesures de Case management, avec le consentement de l'assuré. Le consentement de l'assuré peut être donné par écrit ou par tout autre moyen permettant d'en établir la preuve par un texte.
Groupe Mutuel	LAMal	84a	1		**Communication de données** Il y a lieu de prévoir que la LPD n'entrave pas l'exécution des tâches des assureurs, notamment en ce qui concerne les outils mis en place, tel que le managed-care, les modèles alternatifs d'assurances et la coordination avec les acteurs de l'assurance privée. Dans ce but, les compléments doivent être apportés. Art. 84a al. 1 a bis / Art. 84a al. 1 b ter / Art. 84a al. 1 b quater Proposition 1 Dans la mesure où aucun intérêt privé prépondérant ne s'y oppose, les organes chargés d'appliquer

					la présente loi ou la LSAMal ou d'en contrôler ou surveiller l'application peuvent communiquer des données, en dérogation à l'art. 33 LPGA: a. à d'autres organes chargés d'appliquer la présente loi ou la LSAMal ou d'en contrôler ou surveiller l'exécution, lorsque ces données sont nécessaires à l'accomplissement des tâches que la présente loi ou la LSAMal leur assignent; a bis à des fournisseurs de soins dans le cadre de la gestion des modèles alternatifs d'assurance b. aux organes d'une autre assurance sociale, lorsque, en dérogation à l'art. 32, al. 2, LPGA, l'obligation de les communiquer résulte d'une loi fédérale; bbis.6 aux organes d'une autre assurance sociale, en vue d'attribuer ou de vérifier le numéro d'assuré AVS; b ter. à des fournisseurs de soins et leur représentants dans le cadre de la gestion des modèles alternatifs d'assurance b quater. aux assureurs privés, lorsque les données sont nécessaires à coordonner l'évaluation et le calcul des prestations ; c. aux autorités compétentes en matière d'impôt à la source, conformément aux art. 88 et 100 de la loi fédérale du 14 décembre 1990 sur l'impôt fédéral direct et aux dispositions cantonales correspondantes; d. aux organes de la statistique fédérale, conformément à la loi du 9 octobre 1992 sur la statistique fédérale8; e. aux organismes chargés d'établir des statistiques servant à l'exécution de la présente loi, lorsque les données sont nécessaires à l'accomplissement de cette tâche et que l'anonymat des assurés est garanti; f. aux autorités cantonales compétentes, s'agissant des données visées à l'art. 22a qui sont nécessaires à la planification des hôpitaux et des établissements médico-sociaux ainsi qu'à l'examen des tarifs; g. aux autorités d'instruction pénale, lorsqu'il s'agit de dénoncer ou de prévenir un crime; gbis. au SRC ou aux organes de sûreté cantonaux à l'intention du SRC lorsque les conditions visées à l'art. 13a de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI) sont remplies;

					h. dans des cas d'espèce et sur demande écrite et motivée: 1. aux autorités compétentes en matière d'aide sociale, lorsqu'elles leur sont nécessaires pour fixer ou modifier des prestations, en exiger la restitution ou prévenir des versements indus, 2. aux tribunaux civils, lorsqu'elles leur sont nécessaires pour régler un litige relevant du droit de la famille ou des successions, 3. aux tribunaux pénaux et aux organes d'instruction pénale, lorsqu'elles leur sont nécessaires pour établir les faits en cas de crime ou de délit, 4. aux offices des poursuites, conformément aux art. 91, 163 et 222 de la loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite11, 5. aux autorités de protection de l'enfant et de l'adulte visées à l'art. 448, al. 4, CC, 6. au SRC ou aux organes de sûreté cantonaux à l'intention du SRC lorsque les conditions visées à l'art. 13a de la LMSI sont remplies.
Groupe Mutuel		LAMal	84a	5	**Communication des données** Il est nécessaire d'assouplir la forme dans laquelle le consentement doit être donné, compte tenu des moyens de communication électronique actuels. <u>Proposition</u> 5 Dans les autres cas, des données peuvent être communiquées à des tiers, en dérogation à l'art. 33 LPGA : a. s'agissant de données non personnelles, lorsqu'un intérêt prépondérant le justifie; b. s'agissant de données personnelles, lorsque la personne concernée y a, en l'espèce, consenti par écrit par tout autre moyen permettant d'en établir la preuve par un texte ou, s'il n'est pas possible d'obtenir son consentement, lorsque les circonstances permettent de présumer qu'il en va de l'intérêt de l'assuré.

Amstutz Jonas BJ

Von: Grundrechte Schweiz <grundrechte@bluewin.ch>
Gesendet: Dienstag, 4. April 2017 17:35
An: Amstutz Jonas BJ
Betreff: DSG Revision
Anlagen: DSG REV GRUNDRECHTE.docx

Sehr geehrter Herr Amstutz
Beiliegend finden Sie unsere Stellungnahme im Rahmen der Vernehmlassung zur Revision des DSG.
Mit freundlichen Grüssen

Catherine Weber, Geschäftsführerin

grundrechte.ch
Postfach
3001 Bern
Tel. 031 312 40 30
info@grundrechte.ch
grundrechte@bluewin.ch
www.grundrechte.ch

grundrechte.ch
Postfach, 3001 Bern
info@grundrechte.ch // grundrechte@bluewin.ch
Telefon 031 312 40 30

Bern, den 4. April 2017

EJPD
Frau Bundesrätin Simonetta Sommaruga
Vernehmlassung DSG
Per Email zu senden an (als word Datei)
jonas.amstutz@bj.admin.ch

Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse zum Datenschutz (SR 235.1)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Gerne beteiligen wir uns an der Vernehmlassung zur Totalrevision des DSG. grundrechte.ch begrüsst die Stossrichtung der Vorlage. Das Ziel der Revision ist, den Datenschutz zu stärken, die Transparenz zu erhöhen, das Verantwortungsbewusstsein der Datenbearbeiter zu erhöhen und die Aufsicht zu stärken. Die technische Entwicklung und die immer stärkere Vernetzung haben zu einer immensen Erhöhung der Datenmengen geführt und ermöglichen eine überaus komplexe, mächtige Nutzung von Daten. Die mit dem Datenschutz verknüpften Rechte der Betroffenen geraten dadurch immer mehr unter Druck. Eine Stärkung des Datenschutzes tut not vor dem Hintergrund dieser Entwicklung.

Mit dem revidierten DSG folgt die Schweiz der Entwicklung im europäischen Raum. Die entsprechende EU-Datenschutzgesetzgebung ist aus unserer Sicht als Mindeststandart zu betrachten. Würde dieser unterschritten, wäre die für das Schutzniveau, aber auch aus wirtschaftlicher Sicht erforderliche Gleichwertigkeit mit der EU-Regelung nicht gewährleistet. Punktuell erscheine aus unserer Sicht zusätzliche Schutznormen als erforderlich, insbesondere, weil die EU-Datenschutzgesetzgebung neuen Qualitäten der Datenbearbeitung, welche sich aus dem Big-Data-Ansatz und der vernetzten Nutzung von Daten ergeben, noch nicht ausreichend gerecht wird.

Nachstehend nehmen wir zu den aus unserer Sicht wichtigsten Bestimmungen im Detail Stellung und legen dar, welcher Änderungen es aus unserer Sicht bedarf, um den Zielen der Revision gerecht zu werden.

Wir bedanken uns für die Gelegenheit, eine Vernehmlassung einzureichen und hoffen, dass unsere Überlegungen und Anträge in den Gesetzgebungsprozess einfliessen können.

RA Viktor Györffy, Präsident von grundrechte.ch

Unsere Stellungnahme im Einzelnen:

Art. 2 – Räumlicher Geltungsbereich
Im Gegensatz zur neuen Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) enthält der vorliegende Entwurf zum revidierten Datenschutzgesetz (DSG) keine besondere Bestimmung zum räumlichen Geltungsbereich. 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 Inhaber von Datensammlungen – nach heutiger Terminologie – vergleichbar, die komplett aus dem Ausland operieren, sich aber an Personen in der Schweiz richten. Zu erwähnen sind etwa Amazon (unter anderen mit Amazon Web Services), Facebook (auch mit Instagram und WhatsApp), Google (unter anderem mit Gmail, Google Analytics und YouTube), LinkedIn, Microsoft (unter anderem mit Office 365), Twitter, Salesforce und XING.

In all diesen Fällen kann – im Unterschied zur neuen EU-DSGVO – 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 internationa-lem Charakter anzuwenden, lässt sich denn auch in der gängigen Praxis nicht nachvollziehen. Ein der neuen EU-DSGVO entsprechendes *Marktortprinzip* muss daher vorgesehen werden. Damit würde dann auch ein in der Schweiz nötiges, vergleichbares Datenschutzrecht gelten.

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.

Art. 3 lit. a – Personendaten

Der erläuternde Bericht hält in der Definition zum Begriff «bestimmbare Person» folgendes fest:

«Wie auch nach dem aktuellen Recht reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei bestimmbar. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Die zur Verfügung stehenden technischen Möglichkeiten werden in Bezug darauf geprüft, wie hoch der zeitliche und finanzielle Aufwand für ihre Anwendung ist. Mit Blick auf die immer gezielteren Technologien zur Datenauswertung und deren konstante Weiterentwicklung verschwimmt die Grenze zwischen Personendaten und anderen Daten indes zusehends. Daten, bei denen heute noch eine rein theoretische Möglichkeit der Identifizierung anzunehmen ist, können morgen vielleicht bereits einer bestimmbaren Person zugeordnet werden.»

Es genügt nicht, wenn besonders schützenswerte Personendaten bearbeitet, Dritten bekannt gegeben und veröffentlicht werden dürfen, sofern die Möglichkeit besteht, dass sich diese Personendaten allenfalls zukünftig de-anonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann.

Insbesondere in der Forschung, Planung und Statistik sind Konzepte, wie Differential Privacy seit langem bekannt. Mithilfe von *Noise Injection* lassen sich beispielsweise Daten so verfremden, dass sie zwar statistisch weiterhin auswertbar sind, sie aber keine verlässlichen Rückschlüsse auf Personen mehr zulassen.

Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist daher in der Botschaft und den Ausführungsbestimmungen festzuhalten.

Art. 3 lit. c Ziff. 4 – Biometrische Daten
Biometrische Merkmale lassen 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. Wenn folglich biometrische Merkmale zur Identifizierung geeignet sind oder zur Identifikation 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). **Der Absatz ist zu ergänzen mit: *«Die Bearbeitung personenbezogener Daten sowie die Auswahl und Gestaltung der Datenbearbeitungssysteme sind dahin gehend 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.

Übermittelt die betroffene Person (wie beispielhaft im erläuternden Bericht festgehalten) ihre Adresse im Hinblick auf den Erhalt einer Kundenkarte, so mag die Weiterbenutzung dieser Adresse durch das betreffende Unternehmen zu Werbezwecken im Rahmen einer anfänglich erkennbaren Zweckbestimmung liegen. Findet die Übermittlung im Rahmen einer Bestellung (online oder nicht) statt, sollte jedoch nicht davon ausgegangen werden können.
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», der nicht abgelehnt werden kann, ist für die betroffene Person wenig hilfreich. Es muss auch jederzeit die Möglichkeit des Widerrufs einer Einwilligung gegeben sein. Zudem müssen Personen in einem Abhängigkeitsverhältnis vor unwillentlich abgegebenen und unverhältnismässigen Zustimmungen geschützt werden (zum Beispiel Arbeitnehmer vor Pauschalvollmachten 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 ein entsprechendes 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. **Wir erwarten vom Bundesrat, dass die erwähnten technischen und organisatorischen Schutzmassnahmen mindestens auf Verordnungsstufe konkretisiert werden.**

Art. 12 – Daten einer verstorbenen Person
Die neue Bestimmung über «Daten einer verstorbenen Person» wird begrüsst.

Art. 13 Abs. 3 und 4 – Informationspflicht bei der Beschaffung von Personendaten
Die Bestimmungen gilt auch für die Auskunftspflicht nach Art. 20 Abs. 2 lit. g. Zur Erfüllung der *Informationspflicht* ist die Bekanntgabe der Kategorien der bearbeiteten Daten, der Kategorien der zur Auftragsbearbeitung übergebenen Daten und der Kategorien der Datenempfänger ausreichend. Die *Auskunftspflicht* hingegen muss aber neben den Daten auch die Empfänger der Daten – und nicht nur deren Kategorien umfassen. **Eine Unterscheidung der Auskunftspflicht und der Informationspflicht ist daher (in Art. 20) sinnvoll.**

Art. 14 Abs. 3 und 4 – Ausnahmen von der Informationspflicht und Einschränkungen
Die Einschränkungen und Bestimmungen gelten speziell für die Auskunftspflicht nach Art. 21. Sind von der *Auskunftspflicht* jedoch «überwiegende Interessen Dritter» betroffen, sollten diese Angaben geschwärzt werden, damit keine Rückschlüsse auf die betroffenen Personen gemacht werden können. Um beispielsweise in Telekommunikationsmetadaten die Rechte der anderen an der Kommunikation beteiligten Personen zu schützen, sind diese zu anonymisieren. Die Auskunftspflicht ist dadurch aber nicht weiter einzuschränken (oder aufzuschieben oder darauf zu verzichten).

Daher ist Abs. 3 wie folgt abzuändern:

Abs. 3: *«Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn ein Gesetz im formellen Sinn dies vorsieht. Er anonymisiert die Auskunft in Teilen, falls dies aufgrund überwiegender Interessen Dritter erforderlich ist.»*

Weitere Ausnahmen vom Auskunftsrecht für Bundesorgane sind formell in den betreffenden Gesetzen, wie beispielsweise dem Nachrichtendienstgesetz, zu regeln.

Abs. 4 lit. b: *«[…] wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls die Übermittlung der Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage stellt.»*
Die Abs. 3 und 4 wären unseres Erachtens in Art. 21 besser aufgehoben.

Art. 15 Abs. 1 – Informationspflicht bei einer automatisierten Einzelentscheidung
Es 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.
Alternativen: Es könnte auch der Beauftragte zur Prüfung herangezogen werden, ob es sich beim angewandten Entscheidungsprozess um eine automatisierte Einzelentscheidung im Sinne von Art. 15 handelt. Und/oder das angewandte Verfahren müsste im Rahmen einer Datenschutz-Folgenabschätzung nach Art. 16 regelmässig auf seine Wirksamkeit geprüft werden.

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. Zudem müssen Datenschutz-Folgenabschätzungen auch rückwirkend, wie in Art. 59 lit. a vorgesehen, für bereits bestehende Datenbearbeitungen durchgeführt werden:
«Die Datenschutz-Folgeabschätzung muss vom Verantwortlichen oder vom Auftragsbearbeiter bei einer Änderung des Risikos oder spätestens alle fünf Jahre wiederholt werden. Eine Benachrichtigung des Beauftragten durch den Verantwortlichen und eine Beurteilung durch den Beauftragten erfolgt bei einem abweichenden Ergebnis der Datenschutz-Folgenabschätzung oder einer Anpassung der Massnahmen.»

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

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. 17 Abs. 4 – Meldung von Verletzungen des Datenschutzes

Der Auftragsbearbeiter muss den Verantwortlichen nicht nur über eine unbefugte Datenbearbeitung, sondern auch – wie in Abs. 1 für den Verantwortlichen festgehalten – über einen Verlust von Daten informieren. **Der Absatz muss daher lauten: *«Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung oder den Verlust von Daten.»***

Art. 17 Abs. 5 (neu) – Meldung von Verletzungen des Datenschutzes durch Internetkriminalität
Beim Verlust von Daten durch Internetkriminalität sollte neben dem Beauftragten und den betroffenen Personen auch die Melde- und Analysestelle Informationssicherung MELANI informiert werden. Durch das Wissen aus konkreten Fällen ist es ihr möglich, Gefahren für Schweizer Unternehmen zu erkennen, ein Gefahrenbild zu erstellen und Massnahmen zu empfehlen. Entsprechend ist der Beauftragte zu ermächtigen, MELANI zu informieren: ***«Bei Verlust von Daten informiert der Beauftragte die für die Sicherheit von Computersystemen und des Internets zuständige Melde- und Analysestelle Informationssicherung MELANI.»***

Art. 18 – Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen sind wichtige Prinzipien und sorgen erst dafür, dass die Einwilligung der betroffenen Person nach Art. 4 Abs. 6 auch tatsächlich eingeholt wird. **Ein Verstoss muss sanktioniert sein/bleiben.** Zudem müssen Massnahmen für Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen **auch rückwirkend, wie in Art. 59 lit. b vorgesehen, für bereits bestehende Datenbearbeitungen umgesetzt 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 entspricht nicht den Anforderungen aus dem Übereinkommen SEV 108 und der EU-DSGVO. **Vielmehr muss auch nachgewiesen werden können, dass die Datenschutzbestimmungen eingehalten werden. Dies geht über ein Register der Datenbearbeitungen hinaus. Dies ist zu verdeutlichen.**

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
Die Auskunft ist - wie im Vorentwurf vorgesehen - kostenlos vom Verantwortlichen zu leisten.

Art. 20 Abs. 2 lit. c – Auskunftsrecht zur Rechtsgrundlage
Gegenüber der Bestimmung im geltenden DSG wurde hinsichtlich dem Auskunftsrecht 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 aber 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 statt. Beispiele sind Social Media-Plattformen, personalisierte Werbung und Beeinflussung durch Microtargeting.

In Zukunft werde noch viel mehr persönliche Daten aus dem «Internet of Things», vom Strom-Smart-Meter über Mobilitäts- und Gesundheitsdaten bis zu Sensordaten aus «intelligenten» Fernsehern 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 Mechanismus Transparenz 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.»

Neue Formulierung für Art. 20 Abs. 2 lit. e: ***«[…] das Vorliegen einer automatisierten Bearbeitung;»***

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, da Schweizer Firmen, falls sie sich an Personen in der EU richten, dies nach EU-Recht einführen müssen. Ein Verzicht nützt den Unternehmen nichts, schwächt aber die Konsumentenrechte in der Schweiz. **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. 21 – Einschränkung des Auskunftsrechts
Die Ausnahmen zur *Informationspflicht* und Einschränkungen aus Art. 14 sollten von der Auskunftspflicht getrennt werden. Sind von der *Auskunftspflicht* «überwiegende Interessen Dritter»

betroffen (bei denen die betroffene Person durch die Information über die Datenbearbeitung auch Informationen über Drittpersonen erhält und dadurch die Interessen dieser Drittpersonen beeinträchtigt werden können), müssen diese Angaben so «geschwärzt» werden, dass keine Rückschlüsse auf die betroffenen Personen gemacht werden können. Um beispielsweise in Telekommunikationsmetadaten die Rechte der anderen an der Kommunikation beteiligten Personen zu schützen, sind diese zu anonymi-sieren. **Die Auskunftspflicht ist dadurch aber nicht weiter einzuschränken (oder aufzuschieben oder darauf zu verzichten).**

Übernahme von Art. 14 Abs. 3:

Abs. 1: ***«Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn ein Gesetz im formellen Sinn dies vorsieht. Er anonymisieren die Auskunft in Teilen, falls dies aufgrund überwiegender Interessen Dritter erforderlich ist.»***

Weitere Ausnahmen vom Auskunftsrecht für Bundesorgane sind formell in den betreffenden Gesetzen, wie zum Beispiel dem Nachrichtendienstgesetz, zu regeln.

Übernahme von Art. 14 Abs. 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 die Übermittlung der Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage stellt.»

Der zweite Satz in Art. 21 Abs. 2 ist damit überflüssig. Der Absatz lautet neu verkürzt:

«Der Verantwortliche muss begründen, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt.»

Art. 22 und Art. 24 Abs. 2 lit. d – Medien
Die Medienlandschaft hat sich in den letzten Jahren dramatisch gewandelt. Traditionelle Zeitungen verschwinden, Online-Angebote nehmen deren Platz ein und Betreiber von Blogs tragen immer mehr zur journalistischen Arbeit bei. Die Einschränkung des Auskunftsrechts für Medienschaffende sollte sich daher stärker am Zweck der Datenbearbeitung als an einem «periodischen Medium» oder dem Beruf des «Medienschaffenden» orientieren.
Auf die Anforderungen bezüglich «beruflich» und «periodisch» ist deshalb zu verzichten.

Art. 24 Abs. 2 lit. e – Anonymisierung usw.
Gemäss den Erläuterungen zum Vorentwurf, wie auch nach dem aktuellen Recht, reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei *bestimmbar*. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Der Begriff wird hiermit zu eng gefasst, da unnötig in Kauf genommen wird, dass besonders schützenswerte Personendaten sich (zukünftig) deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann.
Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten (siehe Art. 3 lit. a).

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 ist weniger relevant. **Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen (s.a. Ausführungen zu Art. 50 ff.).**

Art. 25 Abs. 1 lit. c – Recht auf Vergessenwerden
Im Entscheid zum «Recht auf Vergessenwerden», wie ihn der Europäische Gerichtshof gegenüber Google gefällt hat, geht es nicht primär um das Löschen oder Vernichten von Daten. Vielmehr musste der Suchalgorithmus von Google dahingehend angepasst werden, dass Suchergebnisse zu einem bestimmten Ereignis bei der Suche nach einer Person nicht mehr angezeigt werden. **Der Begriff des «Löschens» sollte entsprechend mit diesem Bezug erläutert werden.**

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 einzelner Kunde oder 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).

Gemäss dem erläuternden Bericht sollen die Instrumente der kollektiven Rechtsdurchsetzung im Rahmen der Umsetzung der Motion 13.3931 Birrer-Heimo in einem grösseren, möglichst Sektor übergreifenden Kontext geprüft werden. In der Stellungnahme des Bundesrates zur Motion ist zu entnehmen:

«Neben der Verbesserung im Rahmen der bereits bestehenden Instrumente erachtete er dabei die Einführung neuer, eigenständiger Instrumente der kollektiven Rechtsdurchsetzung für denkbar, namentlich die Schaffung eines Muster- oder Testverfahrens sowie eines Gruppenklage- oder Gruppenvergleichsverfahrens. Vor diesem Hintergrund ist der Bundesrat bereit, entsprechende punktuelle Gesetzesänderungen vorzuschlagen oder im Rahmen laufender Gesetzgebungsarbeiten zu berücksichtigen. In diesem Zusammenhang sei beispielsweise auf die laufende Aktienrechtsrevision sowie die Arbeiten an einem Finanzdienstleistungsgesetz (Fidleg) hingewiesen. Dagegen erachtet es der Bundesrat nicht als opportun, einen eigenständigen Erlass zum kollektiven Rechtsschutz (‹Sammelklagengesetz›) zu erarbeiten.»

Folgerichtig muss im neuen DSG eine Regelung zur kollektiven Rechtsdurchsetzung (Verbandsklagerecht und Sammelklage), analog beispielsweise zum UWG, vorgesehen sein:
Art. 25 Abs. 4 (neu): *«Klageberechtigt sind auch Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die sich statutengemäss unter anderem dem Datenschutz widmen.»*

Art. 25 Abs. 5 (neu) – Beweislastumkehr
Eine unrechtmässige Bearbeitung von Daten ist nur schwierig und/oder in einem langwierigen Verfahren nachzuweisen, wenn die Klärung des Sachverhalts auf die Mitarbeit und Informationen der beschuldigten Partei angewiesen ist. In schwerwiegenden Fällen muss die Beweislast daher umgedreht werden.

Beispiel: Ein Online-Dienstleister bearbeitet Daten «im Auftrag» der Personen, die den Dienst nutzen. Dies können zum Beispiel deren Fotos, das Adressbuch und die Kontakte innerhalb der Plattform sein. Als Dienstanbieter verwendet er diese Daten aber ebenfalls für sich selbst oder für Dritte, zum Beispiel für Werbung. Und wiederum verwendet er diese Daten «im Auftrag» für andere Personen, die den Dienst nutzen, um Kontakte zu verknüpfen oder Personen in deren Fotos zu erkennen. Betroffen von dieser vielfältigen Datenbearbeitung sind aber nicht nur die beauftragenden Personen, sondern auch unbeteiligte Dritte, zum Beispiel auf den Fotos oder in den Adressbüchern.

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. 27 Art. 2 – Rechtsgrundlagen
Das Profiling birgt immer besondere Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen. Daher muss für ein Profiling immer eine Grundlage in einem formellen Gesetz gegeben sein; **eine Regelung in einem Gesetz im materiellen Sinn ist nicht ausreichend.**

Art. 29 Abs. 4 – Bekanntgabe von Personendaten
Wir lehnen die Ausnahme gemäss Art. 29 Abs. 4 ab. Die Annahme, solche Grundangaben zur Identifizierung einer Person könnten ohnehin auf einfachem Weg in Erfahrung gebracht werden, ist nicht zulässig. Gerade in einem digitalen Kontext stellt beispielsweise das Geburtsdatum ein wichtiges Identitäts- und Sicherheitsmerkmal dar.

Art. 29 Abs. 5 – Bekanntgabe von Personendaten
Die Adressangaben beispielsweise aus der Switch-WHOIS-Datenbank werden regelmässig automatisiert ausgelesen und unrechtmässig weiterbearbeitet. Bei der Zugänglichmachung von Personendaten mittels automatisierter Informations- und Kommunikationsdienste muss entsprechender Missbrauch wirkungsvoll verhindert werden.
Abs. 5 sollte daher ergänzt werden: *«Ein missbräuchliches, insbesondere automatisiertes Beschaffen der Daten durch Dritte ist wirkungsvoll zu verhindern.»*

Art. 30 Abs. 2 – Widerspruch gegen die Bekanntgabe von Personendaten
Die historische Rechtsabwägung nach lit. b ist nicht mehr nötig und zu streichen.
Abs. 2: ergänzen: *«Das Bundesorgan weist das Begehren ab, wenn eine Rechtspflicht zur Bekanntgabe*

besteht.»

Art. 32 Abs. 1 – Datenbearbeitung für Forschung, Planung und Statistik
Gemäss den Erläuterungen zum Vorentwurf, wie auch nach dem aktuellen Recht, reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei *bestimmbar*. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren.

Der Begriff wird hiermit zu eng gefasst, da unnötig in Kauf genommen wird, dass besonders schützenswerte Personendaten sich (zukünftig) deanonymisieren lassen und dadurch den betroffenen Personen erheblichen Schaden zugeführt werden kann.

Eine entsprechende Präzisierung zu den Begriffen «Personendaten» und «bestimmbare Person» ist in der Botschaft und den Ausführungsbestimmungen festzuhalten (siehe Art. 3 lit. a).

Art. 34 Abs. 3bis (neu) – Verbands- und Sammelverfahren
Analog zu Art. 25 Abs. 4 (neu) sind auch die Voraussetzungen für Verbands- und Sammelverfahren zu schaffen: ***«Ansprüche und Verfahren stehen ebenso Organisationen von gesamtschweizerischer oder regionaler Bedeutung zu, die sich statutengemäss unter anderem dem Datenschutz widmen.»***

Art. 37 Abs. 1 – Ernennung und Stellung
Der Beauftragte kontrolliert unter anderem auch die Verwaltung. Er sollte daher unabhängig vom Bundesrat und der übrigen Exekutive beziehungsweise Verwaltung gewählt werden:
«Die oder der Beauftragte wird von der Bundesversammlung für eine Amtsdauer von vier Jahren gewählt.»

Art. 41 – Untersuchung
Die erweiterten Untersuchungsbefugnisse werden begrüsst. Diese entsprechen auch den Vorgaben von Europarat und EU. Allerdings geben diese eine Behandlungspflicht (und nicht nur eine Möglichkeit) durch den Beauftragten vor. 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 eröffnen, 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 in der Regel ein Organisationsverschulden anzunehmen. Die Feststellung des schuldhaften Verhaltens einzelner Personen ist weniger relevant. Anstatt Strafrecht anzuwenden, wären auch Verwaltungssanktionen durch den Beauftragten vorzusehen (s.a. Ausführungen zu Art. 50 ff.).

Art. 50 und 51 – Verwaltungssanktionen
Die aktuell bereits bestehenden Strafbestimmungen im DSG haben sich nicht bewährt: Entsprechende Urteile sind fast gänzlich unbekannt.

Der Entwurf sieht vor, auf die in der EU-DSGVO verankerten Verwaltungssanktionen zu verzichten. Stattdessen sollen die Strafbarkeitsbestimmungen ausgebaut und insbesondere der Strafrahmen stark ausgedehnt werden. Die Wirksamkeit strafrechtlicher Sanktionen vermag jedoch offenkundig nicht an jene von Verwaltungssanktionen heranzureichen. Strafrechtliche Sanktionen können nur greifen, soweit der Rechtsverstoss einer Person individuell zugeordnet werden kann. Die Höhe der Busse orientiert sich wesentlich am individuellen Verschulden dieser Person und ist auch durch ihre persönlichen finanziellen Verhältnisse limitiert.

Im Rahmen von Verwaltungssanktionen kann ein Verstoss viel umfassender gewürdigt und sanktioniert werden. Anders als bei einer strafrechtlichen Verfolgung fällt dabei jede in einer Organisation feststellbare Pflichtverletzung ins Gewicht. Ihre Auswirkungen können umfassend berücksichtigt werden, ebenso die wirtschaftliche Potenz der betroffenen Organisation und die von ihr - allenfalls unter Inkaufnahme von datenschutzrechtlichen Pflichten - erzielten Gewinne.

Nach Art. 30 Abs. 1 StGB kann auch nur die Person, die durch eine Tat verletzt worden ist, die Bestrafung des Täters beantragen. Bei der Pflicht zur Dokumentation von Datenbearbeitungen oder der Durchführung einer Datenschutz-Folgenabschätzung dürfte jedoch oft unklar sein, wer durch eine Unterlassung konkret betroffen ist.

Insbesondere bei gravierenden Verstössen gegen das Datenschutzrecht ist zudem in der Regel von einem Organisationsverschulden auszugehen, bei dem unterschiedliche Akteure in vielfältigen Funktionen und verteilt über verschiedene Gremien und Hierarchien beteiligt sind. Untersuchungen, die darauf ausgerichtet sind, den Grad des schuldhaften Verhaltens von einzelnen Akteuren festzustellen, scheinen wenig sinnvoll. Dabei droht die Sicht auf das Ganze verloren zu gehen.

Insbesondere bei Verstössen von grosser Tragweite wird der Beauftrage mit grosser Wahrscheinlichkeit zugezogen. Das Argument des Bundesrats ist daher falsch, dass die Organisation des Beauftragten verändert werden müsste, um Verwaltungssanktionen durch den Beauftragten aussprechen zu können, worauf insbesondere mit Blick auf die Kosten verzichtet wurde. Es ist auch ökonomisch sinnvoll, die Kompetenz für solche komplexen Untersuchungen zentral zu halten. Im Strafrecht droht zudem die Gefahr von Bauernopfern.

Die EU sowie der Europarat verlangen ausdrücklich auch Verwaltungssanktionen, die der Beauftragte verhängen kann. Die Sanktionen müssen wirksam, verhältnismässig und abschreckend sein. Strafrechtliche Massnahmen vermögen a priori nicht die Wirksamkeit und Abschreckung zu gewährleisten, welche denjenigen von Verwaltungsmassnahmen entsprechen.

Um nicht zuletzt die Angemessenheit hinsichtlich der EU-DSGVO zu gewährleisten, erscheint es daher (allenfalls zusätzlich zu den vorgeschlagenen Strafbestimmungen) als erforderlich, Verwaltungs-sanktionen durch den Beauftragten vorzusehen. Die Konzepte sind nicht neu. Die Schweiz kennt sie zum Beispiel aus der Wettbewerbskommission und der ComCom.

Art. 50 und 51 – Strafmass
Auch gegenüber grossen Unternehmen, die unter Umständen mehrere Milliarden Dollar Gewinn pro Quartal erzielen, müssen Sanktionen genügend abschreckend sein. Die in der EU drohenden Strafen von

20 Mio. Euro oder 4 % des Umsatzes (was entsprechend höher ist) scheinen angemessen. Mit den im Entwurf vorgesehenen Bussen ist eine vergleichbare Wirksamkeit und Abschreckung gegenüber grossen Unternehmen nicht zu erzielen.

Art. 52 – Verletzung der beruflichen Schweigepflicht
Mit der Bestimmung würde (im Bereich der Personendaten) ein Tatbestand für Mitarbeiter von Privatfirmen geschaffen, welcher der Amtsgeheimnisverletzung bei staatlichen Angestellten entspricht. **Dies könnte negative Auswirkungen für Informanten (Whistleblower) haben, welche berechtigterweise auf Missstände in ihren Unternehmen aufmerksam machen wollen. Wir lehnen die neue Bestimmung deshalb ab.**

Art. 57 Abs. 1 – Vollzug durch die Kantone
Die Unterstellung der Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unter das Bundesgesetz über den Datenschutz wird begrüsst.

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

Ermächtigungen zur Datenbearbeitung in anderen Gesetzen
Das totalrevidierte Datenschutzgesetz beruht über weite Strecken auf denselben Grundprinzipien wie das bisherige Recht. Die Tragweite neu geschaffener Vorschriften ist grösstenteils aus sich selbst genügend klar. Unmittelbarer Änderungsbedarf in Einzelgesetzen besteht somit nur beschränkt. Jedenfalls ist die Totalrevision des Datenschutzgesetzes nicht der richtige Ort, um spezifische Bestimmungen zur Bearbeitung von Personendaten in einzelnen Bundesgesetzen zu schaffen oder abzuändern. Sofern der Bundesrat hier Änderungen anstrebt, sind diese im Rahmen einer Revision des jeweiligen Bundesgesetzes zu diskutieren und allenfalls zu beschliessen. Nur so erscheint als gewährleistet, dass die im Rahmen der konkreten Materie vorzunehmenden Abwägungen im Gesetzgebungsprozess mit der erforderlichen Sorgfalt getroffen werden.

Abgesehen von redaktionellen Änderungen, welche sich aus der neuen Terminologie ergeben, ist daher im Rahmen dieser Revision von der Änderung spezifischer datenschutzrechtlicher Bestimmungen in Einzelgesetzen abzusehen. Namentlich sind sämtliche Bestimmungen, mit denen Ermächtigungen zur Datenbearbeitung in anderen Gesetzen geschaffen oder ausgedehnt werden, zu streichen. Dies betrifft insbesondere die Ermächtigungen zum Profiling. In den Bundesgesetzen müssen individuelle, klare und strenge Rahmenbedingungen für das Profiling vorgesehen werden.

DIE SPITÄLER DER SCHWEIZ
LES HÔPITAUX DE SUISSE
GLI OSPEDALI SVIZZERI

Departement für Justiz und Polizei
3003 Bern

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

Ort, Datum	Bern, 20. März 2017	Direktwahl	031 335 11 13
Ansprechpartner	Martin Bienlein	E-Mail	martin.bienlein@hplus.ch

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

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

H+ Die Spitäler der Schweiz ist der nationale Verband der öffentlichen und privaten schweizerischen Spitäler, Kliniken und Pflegeinstitutionen. Uns sind 236 Spitäler, Kliniken und Pflegeinstitutionen als Aktivmitglieder an 369 Standorten sowie über 170 Verbände, Behörden, Institutionen, Firmen und Einzelpersonen als Partnerschaftsmitglieder angeschlossen. Unsere Antwort beruht auf einer Mitgliederumfrage.

1 Allgemeine Bemerkungen

Der Datenschutz ist ein bedeutendes Thema für die Spitäler, Kliniken und Pflegeinstitutionen.

Dem Spitalalltag Rechnung tragen
Wir bitten Sie, dem Alltag unserer Mitglieder Rechnung zu tragen, da im Gesundheitswesen laufend besonders schützenswerte Personendaten verarbeitet werden müssen und die Anwendung des Datenschutzes in den Spitäler, Kliniken und Pflegeinstitutionen täglich erfolgt. Die Kerntätigkeit der Spitäler, Kliniken und Pflegeinstitutionen umfasst unter anderem die Datenweitergabe an Angehörige auch im Todesfall, die Datenweitergabe von ausländischen Patientinnen und Patienten zu Behandlungszwecken ins Ausland, die systematische medizinische Datenbearbeitung (Profiling), die Datenbearbeitung zur Forschung, die Berücksichtigung von kantonalen Gesetzen und eidgenössischen Spezialgesetzen.

Nur Notwendiges legiferieren, um EU-Recht einzuhalten
Mit der Revision soll sich die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Diese Annäherung und die Ratifizierung des revidierten Übereinkommens SEV 108 sind zentral, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig möglich bleibt. Eine schweizerische Gesetzgebung über das EU-Recht hinaus erscheint H+ nicht opportun. Deshalb sollte so viel wie nötig und so wenig wie möglich legiferiert werden, um mit der EU-Regelung in Einklang zu kommen, aber nicht um die Arbeit im medizinischen Alltag unnötig zu behindern und zur weiteren Aufblähung des Administ-

rativapparates und damit der Kosten zu führen. Es sind auch bundesrechtliche Vorgaben, die in den letzten Jahren zur Prämiensteigerung der sozialen Krankenkasse beigetragen haben.

Weitere Bürokratisierung verhindern
H+ ist es ein Anliegen, dass das Gesetz nicht eine grosse administrative Arbeit auslöst.

2 Detailkommentare

Art. 3, Bst. f Begriffe
Der Begriff "Profiling" ist genauer zu definieren. Betrifft es auch die systematische medizinische Analyse auf Grund der Lebensdaten und medizinischer Befunde?

Art. 4 Grundsätze
Abs. 3 und 4
Es sollte noch der Vorbehalt einer gesetzlichen Grundlage erwähnt werden. Ansonsten ist nicht klar, ob der Betroffene auf gesetzlich erlaubte Datenbearbeitung hingewiesen werden muss, sofern diese nicht „erkennbar“ ist.

Die in Abs. 3 und 4 formulierten Einschränkungen berücksichtigen nicht, dass zahlreiche kantonale Gesetze Vorschriften zur Aufbewahrung von Personendaten machen. Im medizinischen Bereich gilt bezüglich Krankengeschichte verbreitet eine Aufbewahrungspflicht von zehn Jahren seit der letzten Behandlung.

Abs. 6
Letzten Satz streichen oder für das Gesundheitswesen einschränken.

Gemäss Abs. 6 bedarf es für die Bearbeitung von besonders schützenswerten Personendaten und für das Profiling einer ausdrücklichen Einwilligung. Datenverarbeitung im Rahmen einer medizinischen Behandlung (insbesondere Diagnostik) würde aufgrund der Profiling-Definition von Art. 3 bst. f fraglos darunter fallen. Es ist jedoch davon auszugehen, dass diese Datenverarbeitung ein Teil des vom Patienten häufig formlos erteilen Auftrags an die Medizinalpersonen ist. Hier noch eine ausdrückliche Einwilligung zu verlangen, ist nicht zielführend. Dies ganz abgesehen von den zahlreichen Behandlungsverhältnissen, in denen der Patient mangels Urteilsfähigkeit nicht einwilligen kann. Im Rahmen der Patientenbehandlung ist deshalb auf das Erfordernis einer ausdrücklichen Einwilligung zu verzichten.

Die Regulierung im Bereich der Datenportabilität muss zurzeit zurückgestellt werden, um die präzise Ausgestaltung und Anwendung der entsprechenden EU-Regulierung abzuwarten. Eine Überprüfung im Rahmen der Strategie „Digitale Schweiz“ erscheint zweckmässig.

Es ist nicht klar, was im letzten Satz mit „ausdrücklich“ gemeint ist.

Art. 5 Bekanntgabe ins Ausland und Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen
Für die Spitäler und Kliniken ist der Datenversand ins Ausland bei entsprechenden internationalen Patienten, aber auch bei Mitarbeitenden in länderübergreifenden Unternehmungen von grossem Interesse. Die Voraussetzungen für den Datenversand dürfen nicht verschärft, sondern müssen im Gegenteil erleichtert werden. H+ lehnt die neue, bürokratisch aufwändige Genehmigungspflicht von „verbindlichen unternehmensinternen Datenschutzvorschriften“ klar ab. Die Sperrfrist von 6 Monaten muss deutlich verkürzt werden, falls die strengen Voraussetzungen an den Datenversand aufrechterhalten werden.

Artikel 7, Absatz 3 Auftragsdatenbearbeitung
Abs. 3 streichen oder für das Gesundheitswesen einschränken.

Die vorgängige schriftliche Zustimmung führt zu zeitlicher Verzögerung, welche die Patientensicherheit tangieren kann. Dies beispielsweise, wenn bei einem Systemstillstand der Lieferant externe Spezialisten hinzuziehen muss.

Art. 8 Empfehlungen der guten Praxis
Zwar sind die Empfehlungen des EDOEB nicht bindend; praktisch wird ihnen aber als entscheidende Auslegungsquelle der guten Praxis diese Wirkung zukommen. Das ist rechtsstaatlich bedenklich.

Art. 12 Daten einer verstorbenen Person
Abs. 2 streichen oder für das Gesundheitswesen einschränken.

Die Ausführungen betreffend die Daten einer verstorbenen Person und die „Richtlinien für den digitalen Tod“ und deren Harmonisierung mit dem Erbrecht sind von besonderer Relevanz für die Spitäler, Kliniken und Pflegeinstitutionen. Wenn nahestehende Drittpersonen Auskunftsrechte verlangen, sind heikle Situationen im Spital vorhersehbar. Diese Problematik muss weiterhin über schriftliche Vollmachten und/oder Entbindungserklärungen der Gesundheitsdirektionen/Spitalämter geregelt werden können, was in der Praxis für die konkrete Umsetzung der Informationspflichten gegenüber den Betroffenen (Art. 13 VE-DSG) von zentraler Bedeutung ist.

Diese Bestimmung widerspricht dem ärztlichen Berufsgeheimnis und hebt es gegenüber Erben und Angehörigen von Verstorbenen auf. Gemäss Entwurf könnte ein allfälliges Amts- oder Berufsgeheimnis gegenüber solchen Auskunftsbegehren nicht geltend gemacht werden. Mangels anderer Zuständigkeit hiesse dies, dass Medizinalpersonen die Interessenabwägung auch noch selber vorzunehmen hätten. Abs. 3 ist deshalb ersatzlos zu streichen, womit aufgrund des Vorbehaltes in Abs. 5 das mit Art. 321 StGB geschützte Berufsgeheimnis weiter gelten würde, und der Weg über einer Bewilligung durch die Aufsichtsbehörde offen bliebe. Gemäss Abs. 4 könnte jeder Erbe verlangen, dass die Daten des Erblassers kostenlos gelöscht oder vernichtet werden. Vorbehalten werden gemäss Abs. 5 einzig spezielle Bestimmungen anderer Bundesgesetze. Diese Bestimmung würde im medizinischen Bereich bestehenden und im kantonalen Recht geregelten Pflichten von Medizinalpersonen widersprechen. In der Regel besteht bezüglich Krankengeschichte eine Aufbewahrungspflicht von zehn Jahren seit der letzten Behandlung. Diese gesetzlichen Aufbewahrungspflichten müssten ebenfalls Vorrang haben.

Die neue Bestimmung wäre zudem kaum mit vernünftigem Aufwand umsetzbar. Gemäss Erläuterungen soll jeder Erbe allein die Löschung verlangen können. Unklar bleibt, wie der Verantwortliche erkennen kann, ob Interessen Dritter entgegenstehen. Insbesondere innerhalb einer Erbengemeinschaft, aber auch im weiteren Kreis wären Konflikte vorprogrammiert. Es darf nicht sein, dass für solche Gesuche ein beliebiger Aufwand zu leisten ist, der überdies noch kostenlos erbracht werden soll und zu nichts weiter führt, als dass Daten einer verstorbenen Person gelöscht werden. Schliesslich kann ausgerechnet ein Gesuchsteller wenig ehrenwerte Gründe haben für die verlangte Löschung, und dies nicht nur im medizinischen Bereich. In diesem Zusammenhang wird auch auf den weiteren potentiellen Aufwand gemäss Art. 17 Bst. b hingewiesen.

In den Spitälern, Kliniken und Pflegeinstitutionen kommt es recht häufig vor, dass Ehegatten / Ehefrauen oder Kinder einer verstorbenen Person die Herausgabe der Krankenakten verlangen. Bis anhin haben Spitäler gemäss Art. 1 Abs. 7 VDSG nach dem Interessen der Herausgabe gefragt und dann entschieden. Nach dem neuen Datenschutzgesetz sollen Personen, die mit der verstorbenen Person in gerader Linie verwandt oder mit ihr im Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten, per se ein schutzwürdiges Interesse an der Einsicht haben. Das Berufsgeheimnis wird wegbedungen. Bis anhin mussten die Hinterbliebenen ein Interesse nachweisen. Nach dem neuen Recht müssten die Spitäler, Kliniken und Pflegeinstitutionen herausfinden, ob

schutzwürdige Interessen gegen eine Herausgabe der Krankengeschichte sprechen und müssen dann begründen, weshalb sie die Daten nicht herausgeben. Vom Prinzip her sind die betreffenden Personen ja berechtigt, die Daten zu erhalten. Die Spitäler, Kliniken und Pflegeinstitutionen können aber nicht immer abschätzen, ob die Herausgabe den Interessen des Verstorbenen widerspricht. Das geht zu weit: erstens weil damit die Daten der Verstorbenen zu wenig geschützt werden und zweitens weil damit ein beträchtlicher Aufwand auf die Spitäler, Kliniken und Pflegeinstitutionen zukommt. Das Berufsgeheimnis muss deshalb weiterhin auch für verstorbene Personen gelten und die Nachkommen müssen nachweisen, dass sie ein schutzwürdiges Interesse an den Krankengeschichten haben.

Artikel 13, Abs. 3 und 4 Informationspflicht
Absätze 3 und 4 streichen oder für das Gesundheitswesen einschränken.

Die Informationspflicht führt zu sehr grossem administrativen Aufwand und würde bedeuten, dass die Spitäler, Kliniken und Pflegeinstitutionen alle Patientinnen und Patienten informieren müssten, wenn z.B. im Rahmen eines Supportfalles durch den Lieferanten auf ihre Daten zugegriffen wurde. Das können sehr schnell viele verschiedene Fälle sein, wenn zur Fehlereingrenzung Vergleiche nötig sind.

Art. 13 Informationspflicht und 19 Weitere Pflichten
Die vorgesehenen - aktiven - Informationspflichten gehen über die EU-Grundverordnung hinaus. Dies wird zu einem erheblichen Mehraufwand für die Spitäler, Kliniken und Pflegeinstitutionen führen, welcher in keinem Verhältnis zum Informations- und Schutzbedürfnis der Patientinnen und Patienten steht.

Art. 16 Datenschutzfolgeabschätzung
Der Begriff „voraussichtliche [...] erhöhtes Risiko“ ist nicht klar. Die Spitäler haben in den meisten Bereichen eine gesetzliche Grundlage zur Bearbeitung von Patientendaten; es sollte klar sein, dass dafür nicht zusätzlich eine Folgenabschätzung vorgenommen werden muss.

Die Maximaldauer von 3 Monaten für die Genehmigung der Datenschutz-Folgeabschätzungen durch den Beauftragten kann zu grösseren Projektverzögerungen führen. Dies v.a. wenn in deren Verlauf kurzfristig Aufträge an weitere Beteiligte (Berater/Experten) nötig sind.

Angesichts der für die Medizin geltenden gesetzlichen Datenbearbeitungs- und Dokumentationspflichten im Gesundheits- und Sozialversicherungsrecht ist für diesen Bereich auf die vorgesehene Datenschutz-Folgenabschätzung zu verzichten.

Art. 17 Meldung von Verletzungen des Datenschutzes
Die in Abs. 1 statuierte Pflicht, dem Beauftragten unverzüglich jede unbefugte Datenbearbeitung oder den Verlust von Daten zu melden, geht zu weit. Im Bereich der medizinischen Daten ist die Persönlichkeit der betroffenen Person regelmässig tangiert, was aber noch nicht rechtfertigt, jedes Versehen unabhängig vom konkreten Schadens- oder Gefährdungspotenzial melden zu müssen. Die Mitteilung einer Verletzung des Datenschutzes an Patientinnen und Patienten bildet die Ausnahme: Eine solche Meldung hat nur dann zu erfolgen, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Eidgenössische Datenschutz- und Informationsbeauftragte es verlangt. Eine sich bei einer Ärztin oder einem Arzt befindliche Information führt nicht zu einem Abbau dieses Schutzes. Dies gilt auch dann, wenn die Information einem Spital, einer Klinik oder Pflegeinstitution mitgeteilt wird, die als öffentlich-rechtliche Einrichtung konstituiert ist. Denn in diesem Fall unterstehen die Mitarbeitenden dem Amtsgeheimnis, unabhängig davon ob sie Ärztin resp. Arzt sind. Eine Information an Patientinnen und Patienten dürfte somit die absolute Ausnahme bleiben.

Die Meldepflicht führt zu einem grossen Aufwand, der nicht zu automatisieren ist. Wer griff warum auf welche Daten zu? Der konsequenten Auswertung der Logs (z.B. im Klinikinformationssystem) auf suspekte Zugriffe müssten Abklärungen über deren Gründe folgen, auch bei allen externen Dienstleistern. Dies mit verschiedensten Deutungsmöglichkeiten („habe mich vertippt“

etc.), die unter die Meldepflicht fallen. Temporär oder endgültig nicht mehr gefundene Papierakten bzw. Teile davon sind Alltag. Dies müsste neu sowohl dem Beauftragten wie auch den betroffenen Patienten gemeldet werden, was zu dauerhaftem administrativem Aufwand führt.

Gemäss Bst. b wären Empfänger von Personendaten insbesondere über jede Berichtigung, Löschung oder Vernichtung von Daten und über Verletzungen das Datenschutzes zu informieren, es sei denn, dies sei nicht oder nur mit unverhältnismässigem Aufwand möglich. Der Sinn einer solchen Pflicht ist in der Medizin nicht ersichtlich. Jeder Aufwand wäre als unverhältnismässig. Für die Umsetzung einer solchen Vorgabe müssten z.B. Medizinalpersonen, welche nach Ablauf der 10-jährigen Aufbewahrungsfrist die Krankengeschichte vernichten, hierüber unter Umständen eine Vielzahl von Adressaten früherer Korrespondenz informieren, auch jene, die selber keine Daten mehr über die betroffene Person gespeichert haben (z.B. eine Krankengeschichte, welche ein 40-jähriges Behandlungsverhältnis dokumentiert und zehn Jahre nach dem Tod der Patientin vernichtet wird).

Artikel 19 Weitere Pflichten
Bei gewissen Mutationen oder auch bei Löschanträgen ganzer Dossiers durch Patientinnen oder Patienten müssten alle externen Empfänger von Informationen informiert werden. Das ist nicht praktikabel.

Art. 20 Auskunftsrecht
Im geltenden Recht kann der Bundesrat noch Ausnahmen von der Kostenlosigkeit des Auskunftsrechts vorsehen, was gemäss dem Entwurf nicht mehr möglich wäre. Das Erteilen von Auskünften kann jedoch sehr aufwändig sein, etwa das Kopieren umfangreicher Krankengeschichten mit Medienbrüchen und unterschiedlichen Formaten. Dass dies in jedem Fall kostenlos sein soll, ungeachtet der Gründe für ein Auskunftsersuchen, ist stossend. Der Bundesrat sollte deshalb auch in Zukunft Ausnahmen von der Kostenlosigkeit vorsehen können.

Insbesondere der Löschungsanspruch ist nicht vereinbar mit der gesetzlichen Pflicht zur Führung einer Krankengeschichte, mit den in den meisten kantonalen Gesundheitsgesetzen vorgesehenen Aufbewahrungsfristen und schliesslich im Spital mit der Pflicht zum Angebot eines Elektronischen Patientendossiers. Die gesetzlichen Aufbewahrungspflichten sind ausdrücklich vorzubehalten.

Bei ausserordentlichem Aufwand müsste wie in anderen Rechtsbereichen auch eine Entschädigung verlangt werden können.

Art. 24 Abs. 2 Rechtfertigungsgründe
Der Begriff „möglicherweise“ ist sehr unbestimmt. Es besteht die Gefahr, dass durch ihn mehr Verwirrung denn Klarheit geschaffen wird. Angesichts des Umstandes, dass Art. 24 VE DSG eine wichtige Thematik aufgreift (Rechtfertigungsgründe einer Verletzung der Persönlichkeit), ist eine präzisere Formulierung notwendig.

Abschnitt 8, Art. 50 bis 55 Strafbestimmungen
Vorgesehen ist eine massive Erhöhung der möglichen Bussen und die strafrechtliche Sanktion richtet sich gegen die verantwortliche natürliche Person. Dies ist unverhältnismässig, zumal die Kriminalisierung auch bei fahrlässiger Begehung und selbst beim Unterlassen von hier als völlig sinnlos einzustufenden Tätigkeiten droht. Für Fahrlässigkeit ist die mögliche Bussenhöhe von bis zu 250‘000 Franken, also der Hälfte des Maximums für Vorsatz, viel zu hoch angesetzt.

Die Strafbestimmungen sind angesichts der erheblichen Strafandrohung zu wenig konkret gehalten. Zudem sind sie nicht mit den Strafbestimmungen des Arztgeheimnisses (Art. 321 StGB) abgestimmt (Fahrlässigkeit nach Art. 321 StGB ist nicht strafbar).

3 Andere Gesetze

Der vorliegende Entwurf des DSG äussert sich nicht zum Verhältnis zum Bundesgesetz über die Forschung am Menschen (Humanforschungsgesetz, HFG). Eine Klarstellung im Gesetz oder mindestens in der Botschaft ist notwendig, wonach das HFG als Lex specialis vorgeht, was die Bearbeitung von Personendaten im Forschungskontext betrifft. Dies muss auch nach Inkrafttreten des totalrevidierten DSG so sein. D.h. der Grundsatz des Vorrangs des jüngeren Erlasses [„Lex posterior derogat legi priori“] soll nicht gelten.

In diesem Zusammenhang ein Hinweis redaktioneller Natur: Das HFG verweist in Art. 42 Abs. 2 auf Art. 6 des bestehenden DSG. Der VE DSG beabsichtigt keine entsprechende Anpassung des Art. 42 Abs. 2 HFG. Neu werden die Voraussetzungen der Bekanntgabe ins Ausland jedoch in Art. 5 und 6 VE DSG geregelt.

Bezüglich der Datenbearbeitung im Forschungskontext erachten wir eine Abstimmung mit der Rechtsabteilung des BAG (RB 3) bzgl. einer etwaigen Neuregelung von Art. 42 Abs. 2 HFG als notwendig. Eventuell ist ein pauschaler Verweis auf die Bekanntgabe-Norm des DSG angesichts der Totalrevision und der damit verbundenen gänzlich neuen Struktur des Gesetzes nicht mehr adäquat. Ferner besteht aus unserer Sicht Klärungsbedarf, was das Verhältnis des HFG zu Art. 24 Abs. 2 lit. e VE DSG (Privileg bzgl. Datenbearbeitung in der Forschung [sog. „Forschungsprivileg“]) anbelangt.

Wir danken für die Aufnahme unserer Anliegen und stehen Ihnen bei Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Dr. Bernhard Wegmüller
Direktor

handelskammer beider basel

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrain 20
3003 Bern

Parallel per E-Mail an jonas.amstutz@bj.admin.ch

Basel, 3. April 2017 hk

Stellungnahme zur Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Sehr geehrte Damen und Herren,

In der Beilage lassen wir Ihnen unsere Stellungnahme zur obgenannten Revision zukommen.

Wir danken Ihnen für die Berücksichtigung unseres Anliegens und stehen Ihnen bei Fragen in Zusammenhang mit unserer Darstellung selbstverständlich jederzeit gerne zur Verfügung.

Freundliche Grüsse

Handelskammer beider Basel

Dr. Franz A. Saladin
Direktor

Martin Dätwyler
Stv. Direktor

Beilage: Stellungnahme

Martin Dätwyler
Stv. Direktor

T +41 61 270 60 81
F +41 61 270 60 65

m.daetwyler@hkbb.ch

Handelskammer beider Basel
St. Jakobs-Strasse 25
Postfach
CH-4010 Basel

T +41 61 270 60 60
F +41 61 270 60 05

www.hkbb.ch

beider basel handelskammer

Stellungnahme

Basel, 3. April 2017 hk

Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Die Handelskammer beider Basel fordert den unbedingten Vorrang des Humanforschungsgesetzes und all seiner Verordnungen als lex specialis vor dem Datenschutzgesetz. Sie schliesst sich ausserdem den Stellungnahmen von Interpharma, economiesuisse und dem Schweizerischen Verband Creditreform an.

Das neue Datenschutzgesetz muss der Wirtschaft genügend Raum für Entwicklung lassen und darf sich in keinem Fall hemmend auf das wirtschaftliche Potenzial und die Wettbewerbsfähigkeit von Unternehmen auswirken, so der Anspruch der Handelskammer beider Basel.
Kritische Bemerkungen und Anträge betreffen folgende Aspekte und Artikel:

Vorrang des Humanforschungsgesetzes (HFG) als lex specialis

Im erläuternden Bericht zur Revision des Datenschutzgesetzes wird auf Seite 39 verdeutlicht, dass durch die lex specialis Regel bereichsspezifische Datenschutznormen als dem Datenschutzgesetz übergeordnet behandelt werden. Dies betrifft auch das Humanforschungsgesetz und seine Verordnungen, welche v.a. für die in der Humanforschung tätigen Unternehmen des Life Sciences-Standortes Basel von grosser Bedeutung sind. Die Handelskammer erwartet daher die konsequente Berücksichtigung der lex specialis Regel. Entsprechend fordert die Kammer das Humanforschungsgesetz mit all seinen Verordnungen in der Botschaft explizit als vorrangige Spezialgesetzgebung aufzuführen.

Auf den Art. 24 Abs. 2 lit. E. Ziff. 1 (Rechtfertigungsgrund der Forschung, Planung und Statistik) soll im Kontext mit Art. 4 Abs. 4 (Datenaufbewahrung) verzichtet werden. Aufgrund der lex specialis-Regelung geht auch hier das HFG vor.

Spezifische Regelungen für Verstorbene

Die Handelskammer fordert, die Bestimmungen auf Personendaten lebender Personen zu beschränken und die ersatzlose Streichung von Art. 12.

Deborah Strub
Bereichsleiterin Life Sciences

T +41 61 270 60 76
F +41 61 270 60 65

d.strub@hkbb.ch

Handelskammer beider Basel
St. Jakobs-Strasse 25
Postfach
CH-4010 Basel

T +41 61 270 60 60
F +41 61 270 60 05

www.hkbb.ch

Überhöhte Informations- und Meldepflichten
Die Handelskammer wehrt sich kategorisch gegen die neuen Bestimmungen zu Informations- und Meldepflichten.
Diese Pflichten bringen ausser erheblichem Mehraufwand nicht die mit dem Gesetz angestrebte Transparenz für die betroffenen Personen. Komplexe Geschäftsvorgänge z.B. in grossen Konzernen werden damit zusätzlich und unnötig verkompliziert und behindern die Wirtschaft. Die Kammer fordert daher eine klare Reduktion der Informations- und Meldepflichten.
Insbesondere fordert die Kammer, dass Art. 16 „Datenschutz-Folgenabschätzung" nur für Betriebe ab 50 Mitarbeitern vorzusehen ist.

Keine übertriebenen Regelungen über EU-Grundsätze hinaus
Auf die Einführung neuer Schutzkategorien, die über die europäische Datenschutz-Grundverordnung und die Konvention 108 des Europarates hinausgehen, ist zu verzichten. Die Handelskammer fordert deshalb, dass das Sanktionssystem, v.a. dessen Strafbestimmungen, revidiert wird.
Im Besonderen soll ein sogenanntes Profiling erst schutzrelevant werden, wenn das Profil verwendet wird und nicht bereits bei der Erstellung.

Einführung eines betrieblichen Datenschutzbeauftragten
Muss aufgrund europäischer Vorgaben oder Ausrichtung nach der DSGVO ein betrieblicher Datenschutzbeauftragter eingeführt werden, so erwartet die Handelskammer dies auf freiwilliger Basis und unter gelockerten Informations- und Meldepflichten vorzusehen. Weiter fordert sie, dies erst ab einer Betriebsgrösse von 250 Mitarbeitern und nur für Unternehmen, die nach Europa exportieren, einzuführen. Der Datenschutzbeauftragte soll zu Selbstregulierung und Verantwortung in den Unternehmen beitragen. Es muss vermieden werden, dass dessen Einführung zu weiteren unnötigen Kosten in den Unternehmen insb. KMU führt.

Begrifflichkeiten der genetischen und biometrischen Daten
Bei der Definition von genetischen und biometrischen Daten muss deutlich herausgestellt werden, ob diese zum Zweck der Identifizierung erhoben werden. Es muss sichergestellt sein, dass die Untersuchung von genetischen Daten zur Erforschung von Mechanismen möglich ist. Die Identität der einzelnen Datenspender steht nicht im Vordergrund der Forschung und wird dafür auch nicht benötigt.

Fazit
Die Handelskammer beider Basel stellt folgende Forderungen an das revidierte Datenschutzgesetz:

1. Die explizite Nennung des Humanforschungsgesetzes, dessen Verordnungen und deren Vorrang als lex specialis vor dem Datenschutzgesetz.
2. Den Verzicht auf Art. 12.
3. Klare Reduktion der überhöhten Informations- und Meldepflichten und der Art. 16 darf ausschliesslich für Betriebe ab 50 Mitarbeiter gelten.
4. Den Verzicht auf Regelungen, die über europäisches Recht hinausgehen.
5. Einführung eines betrieblichen Datenschutzbeauftragten auf freiwilliger Basis und nur für nach Europa exportierende Betriebe ab 250 Mitarbeitern.
6. Eindeutigkeit in der Definition der Begrifflichkeiten von genetischen und biometrischen Daten.

Im Weiteren unterstützt die Handelskammer die Stellungnahmen von Interpharma, economiesuisse und dem Schweizerischen Verband Creditreform.

HEV Schweiz

Hauseigentümerverband Schweiz
Seefeldstrasse 60
Postfach 8032 Zürich
Tel. 044 254 90 20
Fax. 044 254 90 21
info@hev-schweiz.ch
www.hev-schweiz.ch

Eidg. Justizdepartement
Frau
Bundesrätin Simonetta Sommaruga
Bundeshaus
3000 Bern

HE/Gm/Ob

22. März 2017

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

---

Sehr geehrte Frau Bundesrätin
sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit, zum Vorentwurf betreffend die Totalrevision des Datenschutzgesetzes (DSG) Stellung nehmen zu können. Nebst der Anpassung an Datenschutznormen der Europäischen Union, die teilweise strenger sind als die bisherigen schweizerischen, wird insbesondere eine Stärkung der Stellung des Datenschutzbeauftragten bezweckt. Folgende Punkte der Revision sind besonders bemerkenswert:

- ✓ Die Rechte der betroffenen Personen werden klarer definiert. So weist der VE-DSG ausdrücklich auf das Recht hin, dass Betroffene Anspruch auf Löschung der Daten haben. Ausserdem wird der gerichtliche Zugang erleichtert, indem Verfahren gegenüber privaten Verantwortlichen von den Gerichtskosten befreit werden.
- ✓ Die Stellung und die Unabhängigkeit des Beauftragten werden gestärkt. Nach Abschluss einer Untersuchung, die von Amtes wegen oder auf Anzeige hin eingeleitet wurde, kann der Beauftragte Verfügungen erlassen, die für die Verantwortlichen und die Auftragsbearbeiter verbindlich sind.

- ✓ Der strafrechtliche Teil des DSG wird ausgebaut. Damit wird insbesondere der Tatsache Rechnung getragen, dass der Beauftragte nach wie vor nicht befugt ist, Verwaltungssanktionen zu erlassen. So wird z.B. der Höchstbetrag der Bussen auf CHF 500'000.00 erhöht.

Der Hauseigentümerverband Schweiz ist der Auffassung, dass ein möglichst griffiges Datenschutzgesetz auch im Interesse der Haus- und Grundeigentümer liegt. Wir leben in einer Zeit, in der die Persönlichkeitsrechte sowie die Daten jedes Einzelnen durch die sozialen Medien und die Möglichkeiten des Internets in einem immer stärker werdenden Ausmass bedroht werden. Zur Abwehr dieser negativen Auswirkungen bedarf es einer stringenten Datenschutzgesetzgebung. Wir begrüssen daher die Stossrichtung der Gesetzesrevision ausdrücklich. Insbesondere positiv zu bewerten ist die vorgesehene Stärkung der Stellung des Datenschutzbeauftragten sowie die Verschärfung der Strafbestimmungen. Nur so lässt sich sicherstellen, dass der Datenschutz auch inskünftig den Herausforderungen durch die digitale Welt gewachsen ist. Wir beschränken uns in unserer Stellungnahme auf die Problematik der Bewertungsplattformen im Internet und entsprechenden Applikationen auf „samrtphones".

Bewertungsplattformen im Internet

Der HEV Schweiz sah sich in jüngster Zeit mit der Problematik einer von der Fa. Comparis im Internet aufgeschalteten Bewertungsplattform im Internet konfrontiert. So bietet Comparis seit einiger Zeit eine Immobiliensuchmaschine (Wohnungen und Häuser zum mieten oder kaufen) an. Gemäss Angaben auf der Homepage bewertet die Comparis-Note die Attraktivität des Mietpreises im Vergleich zum Richtpreis. Der Richtpreis entspricht dem durchschnittlichen Mietpreis im Vergleich zu ähnlichen, im Internet ausgeschriebenen Objekten in der betreffenden Wohngegend. Mit der Comparis-Note wird das mögliche Sparpotenzial ermittelt, das angibt, um wie viel tiefer der Kauf- oder Mietpreis der angebotenen Immobilie im Vergleich zum Richtpreis ist. Die Methodik der Bewertung beruht auf einem statistischen Modell eines ETH Forschers. Berücksichtigt werden unter anderem die Kriterien Postleitzahl, Wohnfläche und sofern im Originalinserat erwähnt, Balkon, Lift, Sitzplatz und Cheminée. Andere Merkmale, wie Ausbaustandard und Standort, können laut Comparis nicht berücksichtigt werden. Der HEV Schweiz lehnt das Vorgehen und insbesondere das Benotungssystem von Comparis ab. Die Aufschaltung der Inserate erfolgt ohne das Einverständnis der Inserenten. Trotz Reklamationen von Betroffenen weigerte sich Comparis vorerst, die Noten zu löschen. Danach stellte Comparis gegenüber dem HEV Schweiz in Aussicht, die Noten zu löschen, sofern vom Gesuchsteller ein Eigentümernachweis, eine Kopie des Identitätsausweises und des Makler-/Verwaltungsvertrags beigebracht werde. Der HEV Schweiz ist der Auffassung, dass Comparis mit der Benotung von Immobilien gegen das geltende Datenschutzgesetz verstösst und verpflichtet wäre, den betroffenen Immobilieneigentümern ein rasches und unbürokratisches Löschverfahren bezüglich ihrer Daten zur Verfügung zu stellen. Es ist kein überwiegendes privates oder öffentliches Interesse an der Vergleichbarkeit von Immobilieninseraten ersichtlich, welches der Löschung entgegengehalten werden könnte. So werden denn nicht alle Inserate bewertet, die von Comparis aufgeschaltet werden und die „geklauten" Inserate stammen von verschiedensten Immobilienplattformen.

Eine objektive Vergleichbarkeit erscheint unter diesen Umständen mehr als fraglich. Auf der anderen Seite kann die unseriöse Bewertung für den Immobilieneigentümer negative finanzielle Konsequenzen nach sich ziehen.

Bewertungsapplikationen auf „smartphones"
Im vergangenen Jahr entwickelte die Firma Comparis eine Immobilien Application Software, welche alle Inserate der grössten Immbilien-Portale der Schweiz umfasst. Gemäss Informationen auf der Website der Fa. Comparis enthält die Software Zusatzinformationen wie Standortfaktoren oder frühere Immobilien- und Mietpreise an der gewählten Adresse.

Die Sammlung der früheren Immobilien- und Mietpreise an der gewählten Adresse, aus welcher auf den Eigentümer bzw. Vermieter der betreffenden Immobilien und Wohnungen geschlossen werden kann, geschieht ebenfalls ohne Einverständnis der Betroffenen. Stossend ist bei dieser Applikation vor allem, dass nicht ersichtlich ist, weshalb die momentan angebotene Wohnung zu einem höheren Mietzins angeboten wird als in einem früheren Vermietungszeitpunkt. Somit kann sich der Mietinteressent kein Bild machen, wieso der aktuell verlangte Mietzins höher ist als in früheren Inseraten. Durch die Auflistung früherer Inserate wird zudem die Anfechtung von Anfangsmietzinsen gefördert, was dem Mieterfrieden abträglich ist. Unserer Auffassung nach müsste ein Vermieter von Comparis den Verzicht auf die Auflistung dieser Inserate verlangen können. Die Fa. Comparis hat in erster Linie ein finanzielles Interesse an der Software. Das ist unseres Erachtens kein ausreichender Rechtfertigungsgrund, um Daten von Vermietern bearbeiten zu können, sofern diese sich im nach hinein nicht damit einverstanden erklären. Den Betroffenen müsste auch diesfalls ein rasches und unbürokratisches Verfahren zur Löschung dieser Daten zu verlangen. Es kann davon ausgegangen werden, dass sich die Firma Comparis auch diesfalls einer solchen Möglichkeit widersetzen dürfte.

Datenschutzrechtliche Konsequenzen
Von Bewertungsplattformen im Internet oder auf sogenannten „Smartphones" sind nicht nur Haus- und Grundeigentümer betroffen. Es gibt heute unzählige Bewertungsplattformen, in welchen die unterschiedlichsten Personen und Sachen bewertet werden. Als Beispiele sei auf die Bewertung von Ärzten und Zahnärzten, auf die Bewertung von Lehrern und Professoren sowie auf die Bewertung von Hotels und Restaurants hingewiesen. Auf der Homepage des Eidgenössischen Datenschutzbeauftragten wird zur Zielsetzung des Datenschutzes folgendes ausgeführt:

„Personendaten sind also nicht nur in materieller, sondern auch in ideeller Hinsicht ein wertvolles Gut, weil es in einer demokratischen und rechtsstaatlichen Gesellschaft nicht angeht, dass der Mensch nicht einmal mehr über eine minimale Kontrolle über die Verwendung von Daten, die ihn betreffen, verfügt. Das so genannte informationelle Selbstbestimmungsrecht bildet einen wichtige Grundsatz unserer gesellschaftlichen Ordnung. D.h. jeder Mensch soll so weit wie nur möglich selber darüber bestimmen können, welche Informationen über ihn wann, wo und wem bekannt gegeben werden."

Wir gehen davon aus, dass diese Aussagen auch auf Daten zutreffen, die in Bewertungsplattformen im Internet verwertet werden. Nach vorherrschender Auffassung ist der Begriff der Personendaten weit zu verstehen. Das DSG erfasst somit

auch Daten mit geringem Personenbezug und geringer Gefährdung der Persönlichkeit der betroffenen Person (vgl. Rosenthal/Jöhri, Handkommentar zum DSG, Zürich, 2008, Art. 3 Note 2). Somit sind auch Daten, welche sich z.B. auf Immobilien- und Mietpreise, auf Haus- und Wohnungsmerkmale beziehen, geschützt. Weil – wie bereits erwähnt – für den Betrieb von derartigen Plattformen kein Rechtfertigungsgrund ersichtlich ist, bedarf es grundsätzlich der Bewilligung der Betroffenen. Zumindest müssen diese die Möglichkeit haben, in einem raschen und einfachen Verfahren die Löschung publizierter Daten zu verlangen. Bei Bewertungsplattformen und entsprechenden Applikationen auf „Smartphones" besteht das Risiko von Falschbewertungen, die für die Betroffenen persönlichkeitsverletzend beziehungsweise mit finanziellen Nachteilen verbunden sein können.

Ausdrückliche Regelung im Gesetz
Der HEV Schweiz verlangt eine ausdrückliche Regelung dieser Problematik im Gesetz, damit dem wachsenden Datenmissbrauch entgegengewirkt werden kann. Nur so können Betreiber von Bewertungsplattformen dazu gebracht werden, dem Datenschutz die notwendige Beachtung zu schenken. Wenn finanzielle Interessen im Spiel stehen, dürfte manch ein Betreiber einer Bewertungsplattform den Datenschutz als „quantité négligeable" betrachten. Dies zeigt der Fall Comparis deutlich. Anstatt den Betroffenen die rasche und einfache Löschung ihrer Daten zu ermöglichen, werden diesen bei der Durchsetzung von Löschungsanträgen bürokratische Hürden in den Weg gestellt. Dies offensichtlich mit dem Ziel, die Löschung letzten Endes nicht vornehmen zu müssen, weil die Betroffenen aufgrund des Aufwandes resignieren.

Die Expertenkommission soll entscheiden, wo im Gesetzesentwurf die ausdrückliche Regelung einzufügen ist. **Eine Möglichkeit wäre beispielsweise, diese Regelung bei den in Art. 4 VE-DSG aufgezählten Grundsätzen anzufügen. Es ist ausdrücklich darauf hinzuweisen, dass die auf Bewertungsplattformen im Internet bzw. auf Applikationen auf „smartphones" aufgeschalteten Daten dem Datenschutz unterstehen. Es ist ferner ausdrücklich festzuhalten, dass die Betreiber verpflichtet sind, den Betroffenen ein rasches und einfaches Löschungsverfahren für ihre Daten zur Verfügung zu stellen, auf welches auf den entsprechenden Webseiten bzw. „Smartphone"-Applikationen hinzuweisen ist.**

Für die Berücksichtigung unserer Stellungnahme danken wir Ihnen bestens.

Mit freundlichen Grüssen
HAUSEIGENTÜMERVERBAND SCHWEIZ
Der Präsident: Der Direktor:

NR H. Egloff A. Gmür

Amstutz Jonas BJ

Von: Chvojka Michaela <michaela.chvojka@hotelleriesuisse.ch>
Gesendet: Dienstag, 4. April 2017 09:22
An: Amstutz Jonas BJ
Cc: Meier Claude; Hans Christophe
Betreff: Totalrevision Datenschutzgesetz Stellungnahme
Anlagen: Totalrevision-des-Datenschutzgesetzes_Stellungnahme hotelleriesuisse_04042017.doc; Totalrevision-des-Datenschutzgesetzes_Stellungnahme hotelleriesuisse_04042017.pdf; Totalrevision-des-Datenschutzgesetzes_Stellungnahme hotelleriesuisse_04042017.doc; Totalrevision-des-Datenschutzgesetzes_Stellungnahme hotelleriesuisse_04042017.pdf

Kategorien: Rote Kategorie

Sehr geehrter Herr Amstutz

In der Beilage senden wir Ihnen fristgerecht unsere Stellungnahme zur Totalrevision des Datenschutzgesetzes, einmal wie gewünscht im Word-Format und einmal unterzeichnet in pdf-Version.

Wir bedanken uns für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
Michaela Chvojka

hotelleriesuisse – Kompetent. Dynamisch. Herzlich.
Michaela Chvojka
lic.iur., Fürsprecherin
Projektleiterin Rechtsdienst
Monbijoustrasse 130, Postfach, 3001 Bern
Telefon +41 31 370 43 46, Fax +41 31 370 44 44
www.hotelleriesuisse.ch

hotelbildung.ch – Karriere beginnt mit einem Klick!
Die umfassende Bildungsplattform von hotelleriesuisse.

Please consider the environment before printing this email.

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 : hotelleriesuisse

Abkürzung der Firma / Organisation :

Adresse : Monbijoustrasse 130, 3007 Bern

Kontaktperson : Michaela Chvojka

Telefon : 031 370 43 46

E-Mail : michaela.chvojka@hotelleriesuisse.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 ____ 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) ____ 5

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 ____ 15

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ____ 16

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") ____ 17

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" ____ Fehler! Textmarke nicht definiert.

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
hotelleriesuisse	Sehr geehrte Frau Bundesrätin Sehr geehrte Damen und Herren hotelleriesuisse ist das Kompetenzzentrum für die Schweizer Hotellerie und vertritt als Unternehmerverband die Interessen der national und international ausgerichteten Hotelbetriebe. Die von hotelleriesuisse klassierten Betriebe repräsentieren rund zwei Drittel der Schweizer Hotelbetten und generieren knapp 75 Prozent der Logiernächte. Gemäss Satellitenkonto 2015 erzielt der Tourismus mit einer Nachfrage von 45 Mrd. Franken eine direkte Bruttowertschöpfung von 16 Mrd. Franken – was einem Anteil von 2,6 Prozent an der gesamtwirtschaftlichen direkten Bruttowertschöpfung der Schweiz entspricht. Der Tourismus gehört zudem zu den vier wichtigsten Exportbranchen der Schweiz. Die Hotellerie als Rückgrat des Tourismus erwirtschaftet allein einen jährlichen Umsatz von über 7,6 Mrd. Franken und beschäftigt zirka 63'000 Vollzeitangestellte. hotelleriesuisse setzt sich deshalb mit Nachdruck für die Verbesserung der Erfolgs- und Wachstumschancen wettbewerbswilliger und wettbewerbsfähiger Hoteliers und Hotels in der Schweiz ein. Als Vertreter von hotelleriesuisse und seinen Mitgliedern danken wir für die Möglichkeit der Stellungnahme zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz. Die mit der Revision verfolgten Ziele (Anpassung an veränderte technologische und gesellschaftliche Verhältnisse, Verbesserung der Transparenz von Datenbearbeitungen, die Stärkung der Selbstbestimmung der betroffenen Personen über ihre Daten und die Annäherung und die Ratifizierung des revidierten Übereinkommens SEV 108, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig möglich bleibt) können wir mehrheitlich nachvollziehen, die Umsetzung gemäss Vorentwurf jedoch nur bedingt befürworten. Generell sind wir der Meinung, dass mit den vorgeschlagenen neuen Bestimmungen eine unnötige Überregulierung (inkl. «Swiss Finish») geschaffen wird, die im Weiteren einen enormen administrativen und finanziellen Aufwand mit sich bringt, der zum möglichen Nutzen in keinem Verhältnis steht. So sind wir der Ansicht, dass beispielsweise die vorgesehene Ausweitung der Informationspflicht sogar betreffend banale, d.h. nicht sensible Personendaten übers Ziel hinausschiesst. Im Weiteren ist bei der Informationspflicht auch ein «Swiss Finish» zu erkennen, in dem die im Vorentwurf vorgesehene Angabe von der Identität und Kontaktdaten der Auftragsbearbeiter in dieser Weise nicht einmal in der DSGVO verlangt wird. Auch ist die Schweizer Regelung bezüglich des Zeitpunkts der Information strenger als die EU-Regelung, die eine längere Zeitspanne vorsieht. In diesem Zusammenhang ist auch auf die Regulierungsfolgenabschätzung hinzuweisen, in welcher die Meinung gewisser

Fachpersonen wiedergegeben wird, die auch die Gefahr einer „Informationsüberflutung“ sehen.

Auch bei anderen Pflichten, wie der Auskunftspflicht oder der «Breach Notification», können im Vergleich zu den europäischen Vorgaben Überregulierungen festgestellt werden. Angesichts dessen, dass die «Angemessenheit» des Schutzes gemäss DSGVO wie gesagt lediglich einen «angemessenen» Schutz durch Rechtsstaatlichkeit, gelebte Schutzmechanismen, Betroffenenrechte und unabhängige Aufsicht verlangt (Art. 45 Abs. 2 DSGVO), ist auf jegliche weitergehende Verschärfung in der schweizerischen Gesetzgebung zu verzichten, um die ohnehin schon entstehenden zusätzlichen Kosten und neuen administrativen Aufwände auf das Nötigste begrenzt zu halten.

Generell abgelehnt werden muss die erhebliche potentielle Kriminalisierung von Datenbearbeitern und somit in den meisten Fällen von Mitarbeitenden. Von einer Strafbarkeit von natürlichen Personen ist grundsätzlich abzusehen. Auch sind die Strafmasse markant zu reduzieren.

Unsere Branche sieht sich unter den vorherrschenden Marktverhältnissen und der steigenden Flut von neuen Bestimmungen zunehmend in der Existenz bedroht. Das neue Datenschutzrecht möge hier nicht noch für weitere unnötige Erschwernisse sorgen. Weiter sind unverhältnismässige Massnahmen auf ein vernünftiges und nachvollziehbares Niveau zu senken.

Wir geben der Hoffnung Ausdruck, dass unsere Argumente verstanden werden und danken Ihnen für die Kenntnisnahme unserer Position. Bei weiteren Fragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

hotelleriesuisse

Claude Meier
Direktor

Christophe Hans
Leiter Wirtschaftspolitik

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
hotelleriesuisse	DSG-VE	3		c / Ziff. 4	Die Definition betreffend biometrische Daten ist so zu präzisieren, dass bspw. nicht jedes Gesichtsfoto als besonders schützenswertes Personendatum gilt, sondern nur dasjenige bzw. diejenigen biometrischen Daten, die zum Zweck bearbeitet werden, die natürliche Person eindeutig zu identifizieren. Empfehlung: Präzisierung im Sinne der Ausführungen.
hotelleriesuisse	DSG-VE	3		f	Die Definition des «Profiling» ist zu weit gefasst. Sie geht zudem über die Regelung in der DSGVO hinaus («Swiss Finish»). Empfehlung: Das Profiling soll nur die automatisierte Auswertung von Personendaten umfassen.
hotelleriesuisse	DSG-VE	3		h	Die Definition des „Verantwortlichen“ ist zu wenig klar definiert. Auch die Erwägungen sind diesbezüglich nicht ausreichend. Da der Verantwortliche mehrheitlich die ausschliessliche Verantwortung für die Pflichterfüllung zu tragen hat und auch persönlich haften soll (was hier abgelehnt wird, vgl. dazu Art. 53), ist eine Präzisierung zwingend, um bereits im Vorfeld allfällige Unsicherheiten zu vermeiden. Empfehlung: Präzisierung der Definition.
hotelleriesuisse	DSG-VE	4	3		Es ist zu präzisieren, dass sofern eine bestimmte Datenbearbeitung vom Schweizer Recht vorgeschrieben ist, dies per se für die Zweckbindung genügt und keinen speziellen Hinweis erfordert. Empfehlung: Ergänzung im oben erwähnten Sinn. Das Erfordernis der «klaren» Erkennbarkeit ist zu streichen, da verwirrend.

hotelleriesuisse	DSG-VE	4	6		Das Wort «eindeutig» ist zu streichen oder – gemäss dem Erläuternden Bericht zu diesem Artikel - zu ergänzen, dass die Einwilligung auch durch konkludentes Verhalten gegeben sein kann. Begründung: Das Wort «eindeutig» schliesst das konkludente Handeln je nach Auslegung nicht mit ein. Daher bedarf es einer Präzisierung bereits im Gesetz selber. Empfehlung: Streichung des Worts «eindeutig» oder Ergänzung durch «konkludentes Verhalten».
hotelleriesuisse	DSG-VE	5	5		Die Frist von sechs Monaten ist zu lange bemessen. Eine solche würde Unternehmen bei grenzüberschreitenden Tätigkeiten übermässig lange blockieren. Empfehlung: Die Frist ist auf 30 Tage zu verkürzen.
hotelleriesuisse	DSG-VE	6	1	b	Mit dieser Regelung geht die Schweiz über diejenige der DSGVO (Art. 49 Abs. 1 Bst. c) hinaus, welche die Bekanntgabe auch dann erlaubt, wenn der Vertrag lediglich im Interesse der betroffenen Person abgeschlossen worden ist. Diese Ergänzung wäre auch für das Schweizer Recht sinnvoll. Empfehlung: Ergänzung von Bst. b mit «(…) Abschluss oder der Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags (…)»
hotelleriesuisse	DSG-VE	6	2		Diese Bestimmung verlangt, dass grenzüberschreitende Datenexporte wie bspw. in Fällen, welche durch Vertragsabschluss oder Vertragserfüllung gerechtfertigt sind, dem Beauftragten gemeldet werden müssen. Dies kann – neben einer Flut von Meldungen und erheblichem administrativen Aufwand - dazu führen, dass Unternehmen auch unnötig Geschäftsgeheimnisse offenlegen müssen. Die Ausdehnung dieser Meldepflicht auf Auftragsbearbeiter geht zudem zu weit, da diese oft nicht über die nötigen Angaben verfügen. Empfehlung: Ganzer Absatz 2 ist zu ersatzlos zu streichen.
hotelleriesuisse	DSG-VE	7	2		Die Verpflichtung des Verantwortlichen, sich zu vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Personen zu gewährleisten geht zum einen zu weit und ist zum anderen zu unklar. Was heisst «sich vergewissern» und was heisst «in der Lage sein». Beide Aussagen wurden in keiner Weise im Erläuternden Bericht präzisiert. Es muss

					ausreichend sein, dass der Verantwortliche den Auftragsbearbeiter schriftlich zur Einhaltung der Datensicherheit und der Rechte der Betroffenen verpflichtet. Weiter ist die Delegationsnorm an den Bundesrat in dem Sinne zu korrigieren, dass dieser nicht *weitere* (d.h. zusätzliche) Pflichten festlegen darf, sondern höchstens die bereits in Art. 7 DSG-VE vorgesehenen Pflichten. Empfehlung 1: Abs. 2 ist zu ersetzen durch «Der Verantwortliche verpflichtet den Auftragsbearbeiter schriftlich zur Einhaltung der Datensicherheit und der Rechte der Betroffenen» Empfehlung 2: Das Wort «weiteren» ist zu streichen.
hotelleriesuisse	DSG-VE	7	3		Unklar ist, was unter «schriftlicher Zustimmung» zu verstehen ist. Von dieser zusätzlichen Hürde ist abzusehen. Massgeblich ist, dass eine Zustimmung belegt werden kann. Eine Schriftlichkeit ist hierfür nicht massgebend. Empfehlung: Das Wort «schriftlicher» ist zu streichen.
hotelleriesuisse	DSG-VE	8			Die Einführung der «Empfehlungen der guten Praxis» ist grundsätzlich zu begrüssen. Insbesondere, dass «interessierten Kreisen» die Möglichkeit gewährt werden soll, eigene Empfehlungen der guten Praxis auszuarbeiten und genehmigen zu lassen, ist unterstützungswert. Da der Beauftragte für den Schutz der betroffenen Personen zu Sorgen hat, ist jedoch fraglich, ob die von seiner Seite erarbeiteten Empfehlung nicht zu streng und einseitig ausfallen werden. Da diese Empfehlungen keiner Überprüfung einer höheren Instanz unterliegen, sind dem Beauftragten auch keine Grenzen gesetzt. Aus diesem Grund ist vorzusehen, dass Empfehlungen nur von Seiten der interessierten Kreise erstellt werden können und diese dann vom Beauftragten zu genehmigen sind. Alternativ ist für den Erlass der Empfehlungen eine neutrale Stelle vorzusehen. Empfehlung 1: Streichung von Abs. 1. Empfehlung 2: Anpassung von Abs. 2 und 3 in dem Sinne, dass nur der Verantwortliche bzw. interessierte Kreise Empfehlungen ausarbeiten können und diese dem Beauftragten zur Genehmigung vorlegen können.

hotelleriesuisse	DSG-VE	12	1	b	Fraglich ist, wie der Verantwortliche in Erfahrung bringen kann, dass keine überwiegenden Interessen der verstorbenen Person oder von Dritten einer Einsicht in die Daten durch Dritte entgegenstehen. Es ist praktisch unmöglich und darf auch nicht sein, dass der Verantwortliche aktiv danach zu forschen hat, ob solche überwiegenden Interessen bestehen. Empfehlung: Bst. b ist zu streichen. Gleichzeitig ist das schutzwürdige Interesse von Drittpersonen näher zu definieren, um Missbräuche zu verhindern.
hotelleriesuisse	DSG-VE	12	4		Indem jeder Erbe einzeln verlangen kann, dass Daten des Erblassers gelöscht oder vernichtet werden, sind diverse Konflikte schon vorprogrammiert. Hier muss mindestens verlangt werden, dass sich die Erben untereinander diesbezüglich einig sind. Sind die Daten erst einmal gelöscht oder vernichtet, sind sie in den meisten Fällen nicht rekonstruierbar. Bezüglich Bst. b von Ziffer 4 ist das Gleiche anzumerken wie bei Ziffer 1: Fraglich ist, wie der Verantwortliche in Erfahrung bringen kann, dass keine überwiegenden Interessen der verstorbenen Person oder von Dritten einer Einsicht in die Daten durch Dritte entgegenstehen. Es ist praktisch unmöglich und darf auch nicht sein, dass der Verantwortliche aktiv danach zu forschen hat, ob solche überwiegenden Interessen bestehen. Empfehlung 1: «jeder Erbe» ist zu ersetzen durch «die Erbengemeinschaft oder deren bevollmächtigte Vertretung». Empfehlung 2: Bst. b ist zu streichen. Gleichzeitig ist das schutzwürdige Interesse von Drittpersonen näher zu definieren, um Missbräuche zu verhindern.
hotelleriesuisse	DSG-VE	13	1		Die neuen Informationspflichten gelten – im Gegensatz zur bisherigen Regelung im DGS – für die Beschaffung jeglicher, d.h. auch banaler, nicht-sensibler Personendaten. Dies geht eindeutig zu weit. Aufwand und Nutzen stehen hier absolut nicht im Gleichgewicht. Im Gegenteil, es kann sogar bezweifelt werden, ob mit dieser Informationsflut der betroffenen Person überhaupt gedient wird, oder ob es nur nutzlosen Aufwand für die Datenbeschaffer bedeutet. Empfehlung: Auf eine Informationspflicht auch bei banalen, nicht-sensiblen Daten ist zu verzichten. Die heute geltende Regelung mit der Beschränkung auf besonders schützenswerte Daten und

					Persönlichkeitsprofilen (neu: Profiling) soll beibehalten werden.
hotelleriesuisse	DSG-VE	13	2		Dieser Absatz ist zu offen formuliert. Trotz Beispielen in Bst. a bis c bleibt es für die Verantwortlichen unklar, welche Informationen genau mitgeteilt werden müssen. Angesichts der massiven Strafen, die bei einer Verletzung dieser Informationspflicht drohen, sind die in Bst. a bis c aufgezählten Angaben als abschliessende Liste zu führen. Weitergehende Informationen sind über das Auskunftsrecht abgedeckt. Empfehlung: Umformulierung des Abs. 2, in dem Sinne, dass die aufgezählten zwingenden Angaben die Informationspflicht abschliessend umschreiben.
hotelleriesuisse	DSG-VE	13	4		Die Pflicht, auch die Identität und die Kontaktdaten der Auftragsbearbeiter aktiv offenzulegen, geht zu weit und tangiert allenfalls sogar das Geschäftsgeheimnis. Zudem ist zu befürchten, dass diese Mitteilungspflicht auch zu einer Informationsüberflutung führt. Im Weiteren könnte dieses Anliegen über das Auskunftsrecht abgedeckt werden. Empfehlung: Abs. 4 ist zu streichen.
hotelleriesuisse	DSG-VE	13	5		Diese Regelung ist wiederum ein «Swiss Finish». Die DSGVO gewährt eine Frist von bis zu einem Monat, gemäss DSG-VE soll die betroffene Person bei indirekter Datenbeschaffung spätestens mit Speicherung erfolgen. Empfehlung: Die Frist ist zu verlängern. Die Schweizer Regelung darf zudem nicht strenger sein als die Europäische.
hotelleriesuisse	DSG-VE	14	2	a	Die Ausnahme nach Art. 14 Abs. 2 Bst. a darf nicht nur gelten, wenn die Daten über Dritte beschafft werden. Aus Sicht der Hotellerie würde dies bedeuten, dass jeweils ausländische Gäste aktiv darüber informiert werden müssten, dass nach AuG eine Meldepflicht besteht und ihre Daten bei der Ortspolizei gemeldet werden müssen. Für inländische Gäste bestehen unterschiedliche kantonale Vorschriften bezüglich Gästekontrollen. Auch diesbezüglich müsste jeweils vorab informiert werden. Empfehlung: Abs. 1 ist zu ergänzen mit «(…) wenn sich die Datenbearbeitung aus dem Gesetz ergibt, in den betroffenen Kreisen als bekannt gilt oder sich aus den Umständen ergibt.»

hotelleriesuisse	DSG-VE	14	4	a	Die Beschränkung der Ausnahme des «überwiegenden Interesses des Verantwortlichen» auf Personendaten, die nicht an Dritte weitergegeben werden, ist zu eng. Die Ausnahmeregelung des «überwiegenden Interesses des Verantwortlichen» soll auch bei Weitergabe der Daten an Dritte gelten. Empfehlung: Steichen des Satzteils «und er die Personendaten nicht Dritten bekannt gibt»
hotelleriesuisse	DSG-VE	15	2		Die explizite Anhörungspflicht ist ein weiterer unverhältnismässiger, administrativer Aufwand der Unternehmen anfällt und der in keinem Verhältnis zum Nutzen der betroffenen Personen steht. Mit der Informationspflicht bleibt es der betroffenen Person unbenommen, sich zum Entscheid zu äussern. Im Weiteren handelt es sich wiederum um einen «Swiss Finish». Empfehlung: Abs. 2 ist zu streichen.
hotelleriesuisse	DSG-VE	16	1		Diese Regelung ist wiederum unnötig strenger als diejenige der EU, indem im DSG-VE von einem «erhöhten» Risiko ausgegangen wird und in der DSGVO von einem «hohen» Risiko. Ein erhöhtes Risiko ist schneller anzunehmen und führt daher teilweise zu unnötigen Aufwänden und auch zu erheblichen zeitlichen Verzögerungen. Auf die Erwähnung der Grundrechte ist zu verzichten, da diese im privaten Bereich nur zu Verwirrung führt. Weiter sollte explizit mindestens je eine Ausnahme für gesetzlich vorgesehene Bearbeitung und für von der betroffenen Person genehmigte Datenbearbeitungen aufgenommen werden. Eine weitere, nicht praktikable und problematische Erweiterung («Swiss Finish») gegenüber den EU-Regelungen bildet die Ausweitung der Pflicht zur Abklärung auf den Auftragsbearbeiter. Empfehlung 1: Den Begriff «erhöhtes» Risiko ersetzen durch «hohes» Risiko. Sowie Ergänzung: «und ist die Datenbearbeitung nicht gesetzlich vorgeschrieben oder durch die betroffene Person genehmigt worden», so muss (…). Empfehlung 2: die Einschübe «oder die Grundrechte» sowie «oder der Auftragsbearbeiter» sind zu streichen.

hotelleriesuisse	DSG-VE	16	3		Die Meldepflicht gegenüber dem Beauftragten soll nicht in jedem Fall gelten, sondern höchstens - wie in der EU vorgesehen – wenn trotz Ergreifen von Schutzmassnahmen ein hohes Risiko für eine Persönlichkeitsverletzung bestehen bleiben sollte. Empfehlung 1: Ergänzung mit (…), «wenn trotz Ergreifen von Schutzmassnahmen ein hohes Risiko für eine Persönlichkeitsverletzung bestehen bleibt». Empfehlung 2: «oder der Auftragsbearbeiter» ist zu streichen.
hotelleriesuisse	DSG-VE	16	4		Auch hier geht die Schweizer Regelung über diejenige der EU hinaus («Swiss Finish»). Die Frist von 3 Monaten ist viel zu lang bemessen und verzögert bzw. behindert so Projekte bzw. Geschäftstätigkeiten von Unternehmen. Empfehlung 1: «innerhalb von drei Monaten» ist zu ersetzen mit «innerhalb eines Monats». Empfehlung 2: «oder der Auftragsbearbeiter» ist zu streichen.
hotelleriesuisse	DSG-VE	17	1		Diese Bestimmung beinhaltet wiederum einen «Swiss Finish». Sie geht ohne Grund über die Regelungen in der DSGVO hinaus und ist daher mindestens auf das Mass der EU-Regelung zu reduzieren. Eine Meldepflicht soll höchstens gelten für Verletzungen der getroffenen Schutzmassnahmen und wenn diese Verletzung zu einem Bruch oder Verlust des Gewahrsams an den Daten führt. Nicht jedoch darf eine strafrechtlich relevante Meldepflicht für jegliche Datenbearbeitung, die gegen das DSG verstösst, eingeführt werden. Dies würde eindeutig zu weit gehen. Auch ist der Zeitpunkt der Meldung praxistauglicher festzulegen. «Unverzüglich» sollte durch «ohne unnötigen Verzug» ersetzt werden. Empfehlung 1: Anpassung der Regelung, indem nur Meldepflichten an den Beauftragten bestehen, wenn eine Vielzahl von Personen betroffen ist. Weiter muss es sich um Verletzungen von getroffenen Sicherheitsmassnahmen handeln, welche zu einem Bruch oder Verlust des Gewahrsams an den Daten geführt haben. Empfehlung 2: «Unverzüglich» ist durch «ohne unnötigen Verzug» zu ersetzen.

hotelleriesuisse	DSG-VE	19		a	Die Dokumentationspflicht soll gemäss den Erläuterungen zur DSG-VE durch die Verordnung konkretisiert werden. Damit diese nicht zu weitläufig bzw. uferlos wird, sind wie in der DSGVO (Art. 30) die zwingend zu dokumentierenden Angaben direkt im Gesetz festzuhalten. Dabei ist darauf zu achten, dass den Unternehmen kein übermässiger und nutzloser Aufwand entsteht, indem beispielsweise keine eigenständige Dokumentation verlangt wird, sondern auf bestehende Dokumentationen zurückgegriffen werden darf. Auch ist von der in den Erläuterungen erwähnten Dokumentationspflicht von Datenschutzverletzungen abzusehen. Unbedingt bedarf es analog Art. 30 Abs. 2 DSGVO auch der Ausnahmeregelung, dass kleinere und mittlere Betriebe von der Dokumentationspflicht ausgenommen sind, sofern keine regelmässigen Datenbearbeitungen mit erheblichem Risiko vorkommen. Empfehlung: Präzisierung der Bestimmung im vorerwähnten Sinn. Zwingend bedarf es einer Ausnahmeregelung für KMU.
hotelleriesuisse	DSG-VE	19		b	Die Regelung, dass auch Empfänger/innen der Daten jeweils über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung informiert werden müssen, ist uferlos und absolut nicht praxistauglich. Die Informationspflicht gegenüber Empfängerinnen ist zu beschränken auf Fälle, in welchen die betroffene Person dies verlangt und ein schützenswertes Interesse an dieser Weitergabe der Informationen darlegen kann. Empfehlung: Präzisierung der Bestimmung im vorerwähnten Sinn.
hotelleriesuisse	DSG-VE	20	3		Diese Bestimmung geht absolut zu weit, ist unpraktikabel und greift übermässig in die Freiheiten der Unternehmen und Personen ein. Das Auskunftsrecht betreffend Ergebnis, Zustandekommen und Auswirkungen der Entscheidung ist – wenn überhaupt – auf automatisierte Einzelentscheide zu beschränken, die eine erhebliche Auswirkung haben. Im Weiteren ist zu präzisieren, dass die Informationen nur auf konkreten Anfrage/Rückfrage hin mitgeteilt werden müssen. Empfehlung: Streichen oder wenn dann Präzisierung im Sinne des Vorerwähnten.

hotelleriesuisse	DSG-VE	23	2	d	Dass ein Profiling ohne ausdrückliche Einwilligung der betroffenen Person neu automatisch eine Persönlichkeitsverletzung darstellen soll, geht zu weit, und sogar über die Regelung in der DSGVO hinaus («Swiss Finish»). Wie im bisherigen Recht sollte nur die Weitergabe des Profilings ohne Rechtsfertigungsgrund eine Persönlichkeitsverletzung darstellen. Empfehlung: Ergänzung von Bst. d mit «durch Weitergabe eines Profilings ohne ausdrückliche Einwilligung der betroffenen Person.»
hotelleriesuisse	DSG-VE	24	2		Das Wort «möglicherweise» führt zu Auslegungsschwierigkeiten. Empfehlung: Im Sinne der Rechtssicherheit ist das Wort «möglicherweise» zu streichen.
hotelleriesuisse	DSG-VE	41	3		Insbesondere das neu vorgesehene Recht des Beauftragten, ohne Vorankündigung Räumlichkeiten zu inspizieren, führt zu einer unverhältnismässigen Machterweiterung ohne Schranken und sorgt zudem für eine unklare Kompetenzverteilung. So ist in der jetzigen Fassung eine – mit der vorliegenden Stellungnahme in Frage gestellte - Strafverfolgung durch die kantonalen Strafbehörden vorgesehen. Empfehlung: Art. 41 Abs. 3 ist zu streichen.
hotelleriesuisse	DSG-VE	44	3		Gemäss Verwaltungsverfahrensgesetz haben Beschwerden grundsätzlich aufschiebende Wirkung. Dass gemäss DSG-VE Beschwerden gegen vorsorgliche Massnahmen des Beauftragten in jedem Fall keine aufschiebende Wirkung zukommen soll, ist abzulehnen. So kann es sein, dass die – evt. auch nicht gerechtfertigten - vorsorglich verfügten Massnahmen massive Kosten oder Schäden für das betroffene Unternehmen mit sich bringen. Solange diese Kosten nicht vom Beauftragten bzw. vom Staat übernommen werden, muss dem Unternehmen die Möglichkeit gegeben werden, sich gegen die sofortige Umsetzung vor der nächsthöheren Instanz wehren zu können. Das ist bereits im heutigen Recht so vorgesehen und ist entsprechend beizubehalten. Empfehlung: Art. 44 Abs. 3 ist zu streichen.

hotelleriesuisse	DSG-VE	45			Von einer Anzeigepflicht ist abzusehen. Empfehlung: Art. 45 ist zu streichen.
hotelleriesuisse	DSG-VE	50ff.			Dass für Datenschutzverletzungen neu private Personen strafrechtlich verfolgt und sanktioniert werden sollen, ist klar abzulehnen. Diese Regelungen gehen wiederum über die DSGVO und die Konvention 108 hinaus. Sie sind zudem unverhältnismässig und führen sogar bei Fahrlässigkeit zu einer Kriminalisierung von Mitarbeitern, obwohl teilweise gar kein Schaden entstanden ist. Um sich vor einer persönlichen Strafverfolgung zu schützen, werden sich die datenverantwortlichen Mitarbeitende jeweils durch externe Gutachten/Beratung absichern wollen, was zu enormen zusätzlichen Kosten führen wird. Die Bestimmung des Verantwortlichen wird zudem erschwert, da sich jeder vor den möglichen Konsequenzen fürchtet. Als Maximum sollen Verwaltungssanktionen vorgesehen werden, die jedoch nur in schweren Fällen Bussen beinhalten. Empfehlung: Von einer strafrechtlichen Verfolgung der privaten Person durch kantonale Strafgerichte ist grundsätzlich abzusehen. Verwaltungssanktionen sollen nicht nur Bussen vorsehen. Diese sollen zudem nur bei schweren Verstössen zur Anwendung gelangen.
hotelleriesuisse	DSG-VE	52			Die Regelung, die Verletzung der beruflichen Schweigepflicht betreffend aller geheimen Personendaten mit Freiheitstrafe von bis zu drei Jahren zu bestrafen, ist absolut unverhältnismässig. Für die Gleichstellung bezüglich Sanktionierung von Datenbearbeitern mit Rechtsanwälten, Geistlichen, Ärzten ist nicht nachvollziehbar und ungerechtfertigt. Die heute geltende Regelung in Art. 35 DSG sanktioniert bis anhin nur die vorsätzliche unbefugte Bekanntgabe von geheimen, besonders schützenswerten Personendaten oder Persönlichkeitsprofilen und sieht im Weiteren als Sanktion lediglich eine Busse vor. Die neue Regelung ist eine massive und unnötige Verschärfung, die zu uferloser und ungerechtfertigter Kriminalisierung von Mitarbeitern führt. Empfehlung: Die Bestimmung des heute gültigen DSG (Art. 35) ist beizubehalten bzw. Art. 52 DSG-VE ist entsprechend anzupassen.

hotelleriesuisse	DSG-VE	53			Im Sinne des oben unter DSG-VE 50ff. Ausgeführten, ist von der Strafbarkeit von natürlichen Personen grundsätzlich abzusehen und eine allfällige Busse vom Geschäftsbetrieb zahlen zu lassen. Empfehlung: Anpassung im erwähnten Sinn, d.h. generell die Haftung/Strafbarkeit auf den Geschäftsbetrieb beschränken.
hotelleriesuisse	DSG-VE	55			Für eine Verlängerung der Verfolgungsverjährung für Übertretungen von üblicherweise 3 Jahren auf 5 Jahre besteht kein Anlass. Empfehlung: Art. 55 ist zu streichen.
hotelleriesuisse	STGB-VE	179novies			Von der vorgesehenen Ausweitung dieses Strafartikels ist abzusehen. Die bisherige Regelung, dass nur wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Datensammlung beschafft, auf Antrag bestraft wird, ist beizubehalten. Eine Ausweitung auf jegliche Personendaten ist unverhältnismässig und uferlos. Empfehlung: Beibehaltung der bisherigen Regelung. Verzicht auf die vorgesehene Erweiterung der Strafbarkeit auf alle Personendaten.

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
hotelleriesuisse	generell	Die Erläuterungen sind im Sinne der Bemerkungen/Empfehlungen zu den einzelnen Artikeln des DSG-VE anzupassen und zu präzisieren.