Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik

Referenz/Aktenzeichen: COO.2180.109.7.138327 / 212.9/2012/00754

Datum: 29. Oktober 2014

Normkonzept zur Revision des Datenschutzgesetzes

Bericht der Begleitgruppe Revision DSG

Inhaltsverzeichnis

1. Ausgangslage ... 3
2. Internationales Umfeld ... 4
3. Standpunkte der Mitglieder der Begleitgruppe zum gesetzgeberischen Handlungsbedarf ... 6
4. Wesentlicher Inhalt der Revision ... 7
4.1 Konzept und Umsetzung ... 8
4.1.1 Konzept ... 8
4.1.2 Umsetzung ... 9
4.2 Geltungsbereich und Begriffe ... 12
4.2.1 Geltungsbereich ... 12
4.2.2 Begriffe ... 16
4.3 Allgemeine Grundsätze des Datenschutzes ... 18
4.3.1 Transparenz der Datenbearbeitung ... 18
4.3.2 Sorgfaltspflichten ... 18
4.3.3 Einwilligung ... 22
4.3.4 Weitere Grundsätze ... 22
4.4 Rechte der betroffenen Personen ... 22
4.4.1 Einleitung ... 22
4.4.2 Katalog der Rechtsansprüche ... 23
4.4.3 Auskunftsrecht ... 24
4.4.4 Recht auf Berichtigung ... 25
4.4.5 Recht auf Löschung ... 25
4.4.6 Automatisierte Einzelentscheidungen ... 26
4.4.7 Recht auf Datenübertragbarkeit ... 27
4.5 Grenzüberschreitende Datenbekanntgabe ... 27
4.6 Zertifizierungsverfahren ... 28

4.7 Register der Datensammlungen 29
4.8 Besondere Bestimmungen betreffend das Bearbeiten von Personendaten durch private Personen 29
4.8.1 Regelungskonzeption 29
4.8.2 Persönlichkeitsverletzungen und Rechtfertigungsgründe 30
4.8.3 Rechtsansprüche und Verfahren 31
4.9 Besondere Bestimmungen betreffend das Bearbeiten von Personendaten durch Bundesorgane 37
4.9.1 Regelungskonzeption 37
4.9.2 Zulässigkeit der Datenbearbeitung (insbesondere genügende Rechtsgrundlage) 37
4.9.3 Besondere Bestimmungen für bestimmte Datenbearbeitungsformen 38
4.9.4 Organisatorische Massnahmen 39
4.9.5 Rechtsansprüche und Verfahren 39
4.9.6 Verhältnis zwischen den Vorschriften des DSG und des BGÖ 40
4.10 Aufsichtsbehörden 41
4.10.1 Einleitung 41
4.10.2 Aufgaben und Kompetenzen der Aufsichtsbehörde 41
4.10.3 Organisation der Aufsichtsbehörde 47
4.10.4 Wiederwahl und Amtsdauer 50
4.10.5 Zusammenarbeit zwischen Aufsichtsbehörden auf nationaler und internationaler Ebene 50
4.10.6 Finanzierung 51
4.11 Strafbestimmungen 53
4.12 Schlussbestimmungen 53
5. Erlassform und normatives Umfeld 53
6. Grobstruktur der Regelung 54
7. Normative Dichte (Detaillierungsgrad) 55
8. Zeitplan 55

Anhang: Stellungnahmen einzelner Mitglieder der Begleitgruppe

1. Ausgangslage

Das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) ist am 1. Juli 1993 in Kraft getreten. Es dient dem Persönlichkeitsschutz von Personen, über die Daten bearbeitet werden (Art. 1 DSG), und damit der Gewährleistung des Grundrechts auf Privatsphäre (Art. 13 Abs. 2 der Bundesverfassung, BV; SR 101). Als Einheitsgesetz ist es grundsätzlich auf die Bearbeitung von Personendaten durch Private wie auch durch Bundesorgane anwendbar (Art. 2 Abs. 1 DSG).

Knapp 20 Jahre nach seinem Inkrafttreten ist das DSG einer weitreichenden Evaluation unterzogen worden. Gemäss dem Evaluationsbericht des Bundesrates vom 9. Dezember 2011[1] erzielt das DSG im Bereich der Herausforderungen, die bereits zum Zeitpunkt seines Inkrafttretens bestanden haben, eine spürbare Schutzwirkung. Allerdings hat die Evaluation gezeigt, dass sich die Bedrohungen für den Datenschutz angesichts der rasant fortschreitenden technologischen und gesellschaftlichen Entwicklungen seit einigen Jahren akzentuieren.

Aufgrund dieser Evaluationsergebnisse hat der Bundesrat das Eidgenössische Justiz- und Polizeidepartement (EJPD) damit beauftragt, gesetzgeberische Massnahmen zur Stärkung des Datenschutzes zu prüfen, um den neuen Gefahren für die Privatsphäre Rechnung tragen zu können. Konkret möchte der Bundesrat untersuchen lassen, mit welchen Massnahmen insbesondere die folgenden Zielsetzungen erreicht werden können:

- früheres Greifen des Datenschutzes;
- verstärkte Sensibilisierung der betroffenen Personen für die mit den technologischen Entwicklungen einhergehenden Risiken für den Persönlichkeitsschutz;
- Erhöhung der Transparenz über Datenbearbeitungen;
- Verbesserung der Kontrolle und der Herrschaft über einmal bekannt gegebene Daten;
- Schutz von Minderjährigen.

Weitere Handlungsmöglichkeiten, die der Bundesrat als prüfungswürdig erachtet, sind die Verstärkung der Unabhängigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), der Ausbau des Instruments der Selbstregulierung sowie die Kompetenz- und Aufgabenverteilung zwischen Bund und Kantonen.

Das EJPD soll dem Bundesrat bis spätestens Ende 2014 Vorschläge zum weiteren Vorgehen unterbreiten. Dabei soll es namentlich die Ergebnisse der Evaluation sowie die im Bereich Datenschutz gegenwärtig laufenden Entwicklungen in der Europäischen Union und beim Europarat berücksichtigen. Die Federführung innerhalb des EJPD liegt beim Bundesamt für Justiz (BJ).

Um das nötige Fachwissen einzubeziehen sowie die Interessen der verschiedenen, von einer allfälligen Revision des Datenschutzgesetzes betroffenen Kreise zu berücksichtigen, hat das BJ zur Begleitung der Reformüberlegungen eine breit abgestützte Arbeitsgruppe eingesetzt, welcher Vertreter der Bundesverwaltung, der Kantone, der Wissenschaft sowie der Wirtschafts- und Konsumentenorganisationen angehören (nachfolgend «Begleitgruppe»).[2] Gemeinsam mit der Begleitgruppe hat das BJ im Rahmen mehrerer Sitzungen

---

[1] Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011 (BBl 2012 335).

[2] Die Begleitgruppe setzt sich aus folgenden Mitgliedern zusammen: Rolf Reinhard (Datenschutz-,

von September 2012 bis Oktober 2014 den gesetzgeberischen Handlungsbedarf zum DSG erörtert und die Diskussionsergebnisse – gestützt auf die Vorarbeiten einer Redaktionsgruppe[3] – im vorliegenden Normkonzept zusammengefasst. Das Normkonzept könnte als Grundlage für einen Vorentwurf zur Revision des Datenschutzgesetzes dienen, wenn der Bundesrat dem EJPD einen entsprechenden Auftrag erteilt (vgl. Ziff. 8). Angesichts der Vielfalt der Interessenlagen innerhalb der Begleitgruppe sind für die im Normkonzept vorgeschlagenen Gesetzgebungsmassnahmen häufig verschiedene Lösungsvarianten ausgearbeitet worden. Einzelne Mitglieder der Begleitgruppe haben ferner eine separate Stellungnahme zum Normkonzept eingereicht, in der sie ihre Position in eigenen Worten darlegen (vgl. Anhang).

Schliesslich sind verschiedene parlamentarische Vorstösse mit datenschutzrechtlichen Anliegen in den Räten hängig oder bereits an den Bundesrat überwiesen worden, welche einen Bezug zu den laufenden Revisionsarbeiten haben. Auf diese Vorstösse wird im Normkonzept jeweils themenspezifisch eingegangen.

2. Internationales Umfeld

Reformen des Datenschutzes sind sowohl in der Europäischen Union (EU) als auch im Rahmen des Europarates im Gange. Nach der Auffassung des Bundesrates müssen diese Entwicklungen in die Revisionsüberlegungen auf nationaler Ebene einbezogen werden (vgl. Ziff. 1):

– Modernisierung der Datenschutzkonvention SEV 108 des Europarates[4]: Die von der Schweiz ratifizierte Datenschutzkonvention SEV 108 wird grundlegend überarbeitet. Dieses Übereinkommen könnte zu einem universellen Mindeststandard werden, da es auch Nichtmitgliedstaaten des Europarates zum Beitritt offen steht und derzeit – zusammen mit seinem Zusatzprotokoll[5] – die einzige verbindliche völkerrechtliche Regelung im Bereich des Datenschutzes ist. Anfang 2011 hat der Europarat einen Prozess zur Modernisierung der Konvention eingeleitet. Mit dieser Revision werden zwei Hauptziele verfolgt: Einerseits sollen die Herausforderungen für die Privatsphäre, die sich aufgrund der Nutzung neuer

---

Öffentlichkeits- und Informatikschutzbeauftragter EJPD), Jean-Philippe Walter (Stv. EDÖB), Stephan Brunner (Bundeskanzlei), Thomas Pletscher/Marlis Henze (economiesuisse), Bruno Baeriswyl (Datenschutzbeauftragter des Kantons Zürich, Präsident von «Privatim»), Bertil Cottier (Università della Svizzera italiana), Florence Bettschart (Fédération romande des consommateurs), Marc Langheinrich (Università della Svizzera italiana), Dieter Kläy (Schweizerischer Gewerbeverband), David Rosenthal (Verein Unternehmens-Datenschutz), Jacques Vifian (Eidgenössisches Büro für Konsumentenfragen), Franz Zeller (Bundesamt für Kommunikation), Philippe Künzler (Bundesarchiv, ab Juli 2014) sowie Monique Cossali Sauvain (Bundesamt für Justiz, Leitung der Begleitgruppe).

[3] Von Januar 2014 bis Juni 2014 hat ein Ausschuss der Begleitgruppe (Redaktionsgruppe) einen Vorentwurf zum Normkonzept erarbeitet. Der Redaktionsgruppe haben folgende Mitglieder angehört: Jean-Philippe Walter (Stv. EDÖB), Stephan Brunner (Bundeskanzlei), Bertil Cottier (Università della Svizzera italiana), David Rosenthal, (Verein Unternehmens-Datenschutz) sowie Monique Cossali Sauvain (Bundesamt für Justiz, Leitung der Redaktionsgruppe). Dieser Vorentwurf ist anschliessend von Juli 2014 bis Oktober 2014 durch die Begleitgruppe besprochen und überarbeitet worden.

[4] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SR 0.235.1).

[5] Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung (SR 0.235.11).

Informations- und Kommunikationstechnologien ergeben, angegangen werden. Andererseits sollen die Mechanismen zur Umsetzung und Kontrolle der Datenschutzkonvention SEV 108 gestärkt werden. Es ist möglich, dass der Modernisierungsentwurf im Laufe des Jahres 2015 verabschiedet und den Vertragsparteien zur Unterzeichnung unterbreitet wird.[6] Dabei scheint es eher unrealistisch, dass die Schweiz die modernisierte Datenschutzkonvention SEV 108 nicht ratifizieren wird. Ein solcher Entscheid hätte insbesondere auf den grenzüberschreitenden Datenverkehr erhebliche negative Auswirkungen, was mit nachteiligen Konsequenzen für die schweizerische Wirtschaft verbunden wäre.

– Reformpaket der EU: Gegenwärtig werden in der EU Revisionsvorlagen für eine *Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* (nachfolgend «Entwurf zur EU-Datenschutz-Grundverordnung»)[7] sowie für eine *Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr* (nachfolgend «Entwurf zur EU-Datenschutz-Richtlinie»)[8] erarbeitet. Der Entwurf zur EU-Datenschutz-Grundverordnung soll die Richtlinie 95/46/EG[9] ersetzen, während der Entwurf zur EU-Datenschutz-Richtlinie dem Rahmenbeschluss 2008/977/JI[10] nachfolgen soll. Ziele dieser Reformarbeiten bilden die Modernisierung des Rechtssystems im Bereich des Datenschutzes, die Stärkung der Individualrechte, ein Abbau der administrativen Formalitäten zur Gewährleistung des freien Datenverkehrs in der EU und über den EU-Raum hinaus, eine Verbesserung der Klarheit und Kohärenz der EU-Vorschriften zum Schutz personenbezogener Daten sowie die Gewährleistung einer konsistenten und wirksamen Anwendung und Durchsetzung der datenschutzrechtlichen Vorschriften in allen Tätigkeitsbereichen der EU.

  Die Schweiz ist nur insofern an die neuen EU-Datenschutzerlasse gebunden, als diese eine Weiterentwicklung des Schengen/Dublin-Besitzstandes darstellen. Beim *Entwurf zur EU-Datenschutz-Richtlinie zur polizeilichen und justiziellen Zusammenarbeit* trifft dies eindeutig zu. Noch unklar sind die Verhältnisse in Bezug auf den *Entwurf zur EU-Datenschutz-Grundverordnung*. In den Bereichen, die von den Schengen/Dublin-Assoziierungsabkommen nicht erfasst werden, gilt die Schweiz der EU gegenüber als Drittstaat. Der Datenverkehr steht diesbezüglich grundsätzlich unter der Voraussetzung, dass die EU das Datenschutzniveau der Schweiz als angemessen anerkennt (Angemessenheitsentscheidung), was gegenwärtig der Fall ist. Will die Schweiz diesen Status beibehalten, hat sie somit alles Interesse daran, ihre Datenschutzvorschriften zu stärken und der europäischen Gesetzgebung anzugleichen, auch wenn nicht eine wörtliche Anpassung an den

---

[6] Die letzte Sitzung des Ad-hoc-Komitees, das mit der Prüfung des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 beauftragt ist (Ad Hoc Committee On Data Protection [CAHDATA]), findet Anfang Dezember 2014 statt.

[7] Vgl. <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52012PC0011&qid=1410779268743> (Vorschlag der Kommission vom 25. Januar 2012).

[8] Vgl. <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52012PC0010&qid=1410777949926> (Vorschlag der Kommission vom 25. Januar 2012).

[9] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281, S. 31–50).

[10] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (Abl. L 350, S. 60–71).

Entwurf zur EU-Datenschutz-Grundverordnung erforderlich ist.

Der Zeitplan für die Revisionsarbeiten der EU ist noch ungewiss. Die Trilog-Verhandlungen (informelles Dreiertreffen, an dem Vertreter des Europäischen Parlaments, des Rates und der Kommission teilnehmen) haben noch nicht begonnen. Die EU-Datenschutzreform wird voraussichtlich nicht vor Ende 2015 abgeschlossen sein.

Die laufenden Reformbestrebungen auf europäischer Ebene haben für das Revisionsprojekt zum DSG folgende Konsequenzen:

– Die durch die Evaluation von 2011 ausgelösten Revisionsarbeiten zum DSG sollten – soweit als möglich – die Voraussetzungen für eine Ratifizierung der *modernisierten Datenschutzkonvention SEV 108* schaffen (sofern die Revision der Konvention innerhalb einer angemessenen Frist abgeschlossen wird): Das vorliegende Normkonzept berücksichtigt daher die Anforderungen des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 in seiner derzeitigen, noch nicht definitiven Fassung[11].
– An den *Entwurf zur EU-Datenschutz-Grundverordnung* ist die Schweiz nur soweit gebunden, als dieser eine Schengen/Dublin-Weiterentwicklung darstellt. Trotzdem berücksichtigt das vorliegende Normkonzept dessen Zielsetzungen in allgemeiner Weise. Eine Revision der schweizerischen Datenschutzgesetzgebung sollte auf keinen Fall hinter den geltenden Schutzstandard zurückfallen, da andernfalls die Angemessenheitsentscheidung der EU für die Schweiz als Drittstaat ausserhalb der Schengen/Dublin-Zusammenarbeit beeinträchtigt werden könnte.
– Der *Entwurf zur EU-Datenschutz-Richtlinie im Bereich Justiz und Polizei* wäre wahrscheinlich gesondert von einer allgemeinen Revision des DSG ins schweizerische Recht umzusetzen, sowohl aus terminlichen Gründen als auch wegen der Referendumsklausel (Art. 141*a* Abs. 2 BV), obwohl eine Verbindung der beiden Vorlagen nicht ausgeschlossen wird. Dabei wären die Kohärenz und Koordination der verschiedenen Revisionsarbeiten zu gewährleisten. Für die Umsetzung des Entwurfs zur EU-Datenschutz-Richtlinie wird ein separates Normkonzept ausgearbeitet.

Unabhängig von den Reformentwicklungen in Europa muss die Schweiz den Empfehlungen aus der zweiten Schengen-Evaluation von 2014 (korrekte Anwendung der Schengen-Bestimmungen zum Datenschutz) Rechnung tragen.

Die Reformen auf europäischer Ebene haben Auswirkungen auf den Zeitplan der nationalen Gesetzgebungsarbeiten (vgl. dazu Ziff. 8).

3. Standpunkte der Mitglieder der Begleitgruppe zum gesetzgeberischen Handlungsbedarf

Über die Notwendigkeit von gesetzgeberischen Massnahmen zur Stärkung des Datenschutzrechts werden in der Begleitgruppe im Grundsatz zwei gegensätzliche Auffassungen vertreten.

Eine *Minderheit der Begleitgruppe*, die sich aus Vertretern der Wirtschaftsorganisationen zusammensetzt, ist der Meinung, eine Revision des DSG sei nicht gerechtfertigt, sondern das geltende Recht gewährleiste die Rechte und Pflichten der betroffenen Personen ausreichend. Dieser Teil der Begleitgruppe plädiert dafür, dass der Bundesrat den Abschluss der

[11] Version vom 18. Dezember 2012 (mit den von der 29. Plenarsitzung verabschiedeten Modernisierungsvorschlägen); vgl. <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)04Rev4_F_Convention%20108%20modernisée%20version%20F.pdf>.

Reformen im Bereich des Datenschutzes innerhalb der EU und des Europarates abwarten und nur die Änderungen vorschlagen soll, die für den Marktzugang (bzw. den freien Datenverkehr) erforderlich sind.

Die *Mehrheit der Begleitgruppe* vertritt dagegen die Auffassung, dass das derzeit geltende Gesetz revidiert werden müsse. Es seien entsprechende Massnahmen zu treffen, ohne das Inkrafttreten der Revisionen auf europäischer Ebene abzuwarten. Ausserdem befürwortet dieser Teil der Begleitgruppe eine weitergehende Gesetzesrevision, die sich nicht auf die für den Marktzugang notwendigen Voraussetzungen beschränkt. Nach ihrer Ansicht soll die Datenschutzgesetzgebung nicht nur dazu dienen, den Datenverkehr zwischen privaten Personen in geschäftlicher Hinsicht zu regeln. Sie habe einen viel weitergehenden Bestimmungszweck und müsse insbesondere das verfassungsmässige Recht jedes Einzelnen umsetzen, frei über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Der Staat solle wirksame Massnahmen zur Durchsetzung dieses Rechts vorschlagen und nicht zuwarten, bis er dazu verpflichtet werde.

Für den Fall, dass sich der Bundesrat für eine Fortsetzung der Gesetzgebungsarbeiten entscheidet, haben sich auch die Mitglieder der Begleitgruppe, welche einer Revision des Datenschutzgesetzes ablehnend gegenüberstehen, zum vorliegenden Normkonzept geäussert. Ihre Meinung wird daher in den nachfolgenden Ausführungen berücksichtigt.

Mehrere Mitglieder der Begleitgruppe haben ihre Position ferner in einer separaten Stellungnahme zum Normkonzept festgehalten (vgl. Anhang).

4. Wesentlicher Inhalt der Revision

Die nachfolgenden Vorschläge für eine Anpassung des DSG an die technologischen und gesellschaftlichen Entwicklungen (bzw. die damit einhergehenden Bedrohungen für die Privatsphäre)[12] orientieren sich am geltenden Aufbau des DSG. Neben einem allgemeinen Teil, der Datenbearbeitungsgrundsätze enthält, die sowohl für die Organe des Bundes als auch für private Datenbearbeitende gelten (vgl. nachfolgend Ziff. 4.1 bis 4.7), sind je spezifische Bestimmungen für die Datenbearbeitung durch Privatpersonen (Ziff. 4.8) und für die Datenbearbeitung durch Bundesorgane (Ziff. 4.9) vorgesehen. Ein zentraler Teil der Revisionsvorschläge betrifft sodann die Organisation und Aufgaben der Datenschutzaufsicht (Ziff. 4.10). Schliesslich sind auch die Strafbestimmungen (Ziff. 4.11) und die Schlussbestimmungen (Ziff. 4.12) zu überprüfen.

Keine umfassende Auseinandersetzung findet in diesem Normkonzept dagegen mit dem Thema «Big Data» statt. Der Begriff «Big Data» steht für eine grosse Datenmenge aus vielfältigen Quellen, die aufgrund des technologischen Fortschritts mit hoher Verarbeitungsgeschwindigkeit erfasst, gespeichert und für unbestimmte Zwecke auf unbestimmte Zeit für Auswertungen und Analysen verfügbar gemacht werden kann.[13] «Big Data» birgt in verschiedener Hinsicht neue Herausforderungen für das Datenschutzrecht (z.B. bezüglich der Grundsätze der Erkennbarkeit und Zweckbindung oder der Re-Individualisierung von

---

[12] Datenschutzrechtliche Massnahmen können mit anderen Interessen kollidieren. Bei der Prüfung möglicher gesetzgeberischer Massnahmen sind deshalb neben dem Persönlichkeitsschutz auch weitere betroffene Interessen (insbesondere die Interessen der Wirtschaft, das Recht auf Meinungs- und Informationsfreiheit sowie andere private und öffentliche Interessen) einzubeziehen; vgl. dazu den Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335, 336 und 351.

[13] Vgl. zur Begriffsdefinition die Erläuterungen des EDÖB zu «Big Data»; online einsehbar unter <http://www.e-doeb.admin.ch/datenschutz/00683/01169/index.html?lang=de>.

anonymen Daten). Allerdings besteht zum heutigen Zeitpunkt noch nicht ausreichend Klarheit über die Auswirkungen von «Big Data». So sind in der Rechtswissenschaft bisher erst ansatzweise einzelne Fragen des Datenschutzrechts vertiefter behandelt worden.[14] Aus diesem Grund sind im vorliegenden Normkonzept keine umfassenden Lösungsansätze, sondern nur punktuelle Massnahmen vorgesehen, mit welchen die datenschutzrechtlichen Herausforderungen von «Big Data» angegangen werden können.[15] Eine grundsätzliche Untersuchung der datenschutzrechtlichen Implikationen von «Big Data» könnte im Rahmen der Umsetzungsarbeiten zur Motion Rechsteiner 13.3841 «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit»[16] stattfinden.

4.1 Konzept und Umsetzung

4.1.1 Konzept

Die Begleitgruppe schlägt vor, ein einheitliches Datenschutzgesetz, das sowohl den privaten als auch den öffentlichen Bereich normiert, beizubehalten. Eine harmonische, gegenseitig abgestimmte Entwicklung von privatem und öffentlichem Datenschutzrecht wird am ehesten dadurch gewährleistet, dass die in beiden Bereichen bestehenden Probleme gemeinsam geregelt werden. Vor diesem Hintergrund werden im vorliegenden Normkonzept die Bestimmungen für den privaten und öffentlich-rechtlichen Sektor soweit als möglich vereinheitlicht, um einen gemeinsamen Rahmen für die Bearbeitung personenbezogener Daten zu schaffen. Unterschiedliche Lösungen werden nur vorgesehen, wenn dies unumgänglich ist.

Der Zweck des Gesetzes soll unverändert bleiben. Das Gesetz soll auch inskünftig technologieneutral ausgestaltet sein und sich auf Grundsatzregelungen beschränken, so dass es auf einen möglichst breiten Bereich von Situationen Anwendung finden kann.

Die Idee, alle oder einen Teil der in der Spezialgesetzgebung normierten datenschutzrechtlichen Bestimmungen in einem einzigen Gesetz zusammenzufassen (im Sinne einer Gesamtkodifikation des Datenschutzrechts auf Bundesebene), wurde aufgegeben: Nach Ansicht der Begleitgruppe wäre damit kein Mehrwert verbunden. Eine Überprüfung der Bundesgesetzgebung hat ergeben, dass die grosse Mehrheit der in den Spezialgesetzen enthaltenen Datenschutzbestimmungen darauf ausgerichtet ist, für das jeweilige Sachgebiet eine spezifische gesetzliche Grundlage zu schaffen oder die Grundsätze des DSG zu konkretisieren. Diese bereichsspezifischen Datenschutzvorschriften können daher nicht durch allgemeine Bestimmungen im DSG ersetzt werden und eine Bündelung dieser Normen in einem einzigen Datenschutzerlass würde aus legistischer Sicht keinerlei Vorteile mit sich bringen.

---

[14] Vgl. BAERISWYL, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber/Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich u.a. 2014, S. 46 ff.

[15] Dazu gehören beispielsweise die Regelungsvorschläge zum Grundsatz «Privacy by Design» (vgl. Ziff. 4.3.2), zur Datenschutzfolgenabschätzung (vgl. Ziff. 4.3.2), zum Auskunftsrecht über den logischen Aufbau der Datenbearbeitung (vgl. Ziff. 4.4.3) oder zu den automatisierten Einzelentscheidungen (vgl. Ziff. 4.4.6).

[16] Mit der Motion Rechsteiner 13.3841 «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit», die das Parlament am 4. Juni 2014 überwiesen hat, wird der Bundesrat beauftragt, eine interdisziplinäre Expertenkommission einzusetzen, welche sich mit den technologischen und politischen Entwicklungen auf dem Gebiet der Datenbearbeitung und Datensicherheit sowie deren Bedeutung für die schweizerische Wirtschaft, Gesellschaft und den Staat auseinandersetzt. Dabei soll die Expertengruppe auch Empfehlungen für die Schweiz erarbeiten. Die Federführung liegt beim Eidgenössischen Finanzdepartement (EFD).

4.1.2 Umsetzung

a) Stärkung der Kompetenzen der Aufsichtsbehörde und Erleichterung des gerichtlichen Zugangs für die betroffenen Personen

Nach der Meinung einer *Mehrheit der Begleitgruppe* hat der Evaluationsbericht des Bundesrates Mängel bei der Durchsetzung des DSG aufgezeigt. Diese Mängel führt die Mehrheit der Begleitgruppe hauptsächlich darauf zurück, dass einerseits das Aufsichtsorgan des schweizerischen Datenschutzgesetzes,[17] d.h. der EDÖB, gegenwärtig nur mit beschränkten Kompetenzen ausgestattet sei. Andererseits sieht sie Unzulänglichkeiten darin, dass die betroffenen Personen ihre Rechte nur in seltenen Fällen vor Gericht geltend machen, da ein Missverhältnis zwischen dem Nutzen eines allfälligen Obsiegens vor Gericht und den – in erster Linie finanziellen – Risiken und Anstrengungen, die mit der Eröffnung eines Gerichtsverfahrens verbunden sind, bestehe. Diese beiden Defizite beeinträchtigen gemäss der Mehrheit der Begleitgruppe die wirksame Anwendung des Datenschutzgesetzes und führen zu einem Verlust an Datenkontrolle und -herrschaft. Dies habe zur Folge, dass ein grosser Teil der Verstösse gegen das DSG nicht festgestellt werde und fortdauere. Zudem werde die präventive Wirkung des Gesetzes stark vermindert, da die für die Datenbearbeitung Verantwortlichen bei Verstössen kaum Sanktionen befürchten müssen und sie ihr Verhalten unter Umständen nicht entsprechend anpassen. Für eine bessere Durchsetzung des Gesetzes müssten deshalb die Befugnisse der Datenschutzaufsichtsbehörde durch die Einräumung von Verfügungs- oder sogar Sanktionskompetenzen ausgebaut werden. Ausserdem müssten gegebenenfalls die Rechte der betroffenen Personen, vor allem deren Verfahrensrechte, erweitert werden.

Die *Mehrheit der Begleitgruppe* spricht sich dafür aus, die Kompetenzen der Datenschutzaufsichtsbehörde zu stärken. Es bestehe ein zunehmendes und systematisches Ungleichgewicht in der Beziehung zwischen den betroffenen Personen und den Datenbearbeitenden, bei denen es sich in vielen Fällen um Grossunternehmen handle. Dieses Ungleichgewicht komme insbesondere durch wenig transparente Datenbearbeitungskonzepte oder gar durch die fehlende Möglichkeit, frei über die Nutzung der persönlichen Daten zu bestimmen, zum Ausdruck. Vor diesem Hintergrund reicht nach Auffassung der Mehrheit der Begleitgruppe die blosse Empfehlungsbefugnis der Datenschutzaufsichtsbehörde nicht aus. Die gleiche Feststellung sei bereits in zahlreichen europäischen Ländern gemacht worden, beispielsweise in Frankreich, Italien, Grossbritannien, Schweden und Spanien. In diesen Staaten haben die Aufsichtsbehörden die Möglichkeit, verbindliche Verfügungen zu erlassen oder Bussen zu verhängen[18]. In einer globalisierten Welt, in welcher der internationale Datenverkehr immer umfangreicher wird, sei es von ausschlaggebender Bedeutung, dass die schweizerische Datenschutzaufsichtsbehörde über Kontrollinstrumente verfüge, die mit den Möglichkeiten ihrer ausländischen Partnerinstanzen vergleichbar seien. Ferner ist darauf hinzuweisen, dass im Modernisierungsentwurf zur Datenschutzkonvention SEV 108 Verfügungsbefugnisse

---

[17] Im vorliegenden Normkonzept werden in Ziff. 4.10 Vorschläge für eine Anpassung der Aufgaben und Kompetenzen bzw. der Organisation der Datenschutzaufsicht präsentiert. Um die Organisationsform sprachlich nicht vorwegzunehmen, wird für die Bezeichnung der zukünftigen Datenschutzaufsicht nachfolgend die Terminologie, die auch in den Reformen der EU und des Europarates verwendet wird, übernommen und von der (Datenschutz-)«Aufsichtsbehörde» gesprochen.

[18] Vgl. dazu den Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz vom 10. März 2011, S. 172 f. und 213; online einsehbar unter <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

der Aufsichtsbehörden vorgeschrieben sind (und solche Befugnisse im Übrigen auch im Entwurf zur EU-Datenschutz-Richtlinie [Art. 46] sowie im Entwurf zur EU-Datenschutz-Grundverordnung [Art. 53] vorgesehen werden). Wenn die Revision der Datenschutzkonvention SEV 108 verabschiedet wird und von der Schweiz ratifizieren werden soll, müsste sie ihre Gesetzgebung entsprechend anpassen. Schliesslich hat die EU der Schweiz im Rahmen der zweiten Schengen-Evaluation empfohlen, dem EDÖB die Kompetenz zum Erlass von verbindlichen Verfügungen einzuräumen. In ihren Bemerkungen hat die EU ausserdem hinzugefügt, dass ein Ausbau der Sanktionsbefugnisse des EDÖB begrüsst würde.

Hinsichtlich der Frage, ob auch die Rechte der betroffenen Personen zu stärken sind, herrschen in der Begleitgruppe unterschiedliche Ansichten. Ein *Teil der Begleitgruppe* vertritt die Auffassung, es sei zu kompliziert, einen erleichterten Zugang zur Justiz für die betroffenen Personen in die Praxis umzusetzen, und die vorhandenen Möglichkeiten seien zu wenig wirksam (vgl. dazu Ziff. 4.8.3 und 4.9.5). Aus diesem Grund lohne es sich nicht, umfangreiche Arbeiten in die Wege zu leiten. Ausserdem habe die Evaluation des DSG ergeben, dass die im Gesetz verankerten Durchsetzungsrechte der Betroffenen im internationalen Vergleich bereits gut entwickelt seien.[19] Dieser Teil der Begleitgruppe spricht sich deshalb dafür aus, einem bedeutenden Ausbau der Kompetenzen der Datenschutzaufsichtsbehörde den Vorzug zu geben und den individuellen Rechtsschutz punktuell zu verbessern. Ein *anderer Teil der Begleitgruppe* ist dagegen der Ansicht, es bestünden wirksame Massnahmen zur Erleichterung des gerichtlichen Zugangs für die betroffenen Personen, welche deshalb auch vorgeschlagen werden müssten. Laut dem Evaluationsbericht des Bundesrates sei der Schutz der Individualrechte ein bekanntes Problem. Nach der Auffassung dieser Mitglieder der Begleitgruppe geht es zudem darum, Handlungsmöglichkeiten für den Fall zu finden, dass die Vorschläge für eine Erweiterung der Rolle der Datenschutzaufsichtsbehörde im Verlauf des Gesetzgebungsprozesses abgelehnt werden, weil diese zusätzliche Ressourcen erfordern.

Eine Minderheit der Begleitgruppe ist der Meinung, es sei nicht notwendig, die Befugnisse der Datenschutzaufsichtsbehörde oder die Durchsetzungsrechte der betroffenen Personen auszubauen. Allfällige Gesetzesänderungen sind nach Auffassung dieser Mitglieder der Begleitgruppe nur insoweit vorzunehmen, als sie unter Berücksichtigung des EU-Rechts und des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 für den Marktzugang notwendig sind (vgl. Ziff. 3).

b) Detailliertere Regelungen

Der allgemeine und technologieneutrale Charakter der Bestimmungen des DSG führt insbesondere im privaten Bereich sowohl für die Datenbearbeitenden als auch für die betroffenen Personen zu einer gewissen Verunsicherung über die richtigen Verhaltensweisen. Dadurch wird eine wirksame Durchsetzung des Gesetzes erschwert. Um diesem Problem zu begegnen und die Vorhersehbarkeit des Datenschutzrechts zu verbessern, schlägt die Begleitgruppe vor, die allgemeinen Grundsätze des DSG durch detailliertere Bestimmungen zu ergänzen, die im privaten Bereich und gegebenenfalls auch im öffentlichen Bereich anwendbar sind. Auf diese Weise könnten ausführlichere Regelungen zu Themen entwickelt werden, die heutzutage zahlreiche Fragen aufwerfen, wie beispielsweise die Videoüberwachung, «Big Data», der elektronische Handel oder das «Cloud Computing». Ausserdem könnten auch be-

[19] Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz vom 10. März 2011, S. 72 ff., 212; online einsehbar unter <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

stimmte im Gesetz verwendete Begriffe (z.B. «erhöhtes Risiko», vgl. Ziff. 4.3.2) oder die Modalitäten gewisser durch das Gesetz eingeräumter Rechte präzisiert werden (z.B. das Recht auf Löschung, vgl. Ziff. 4.4.5).

Es stellt sich die Frage, ob diese Detailregelungen als verbindlich ausgestaltet werden sollen oder nicht. In der Begleitgruppe werden beide Auffassungen vertreten:

- Verbindliche Regeln hätten den Vorteil, dass sie ihre Adressaten direkt verpflichten. Doch bei ihrer Erarbeitung ergäben sich zahlreiche Fragen im Zusammenhang mit dem Legalitätsprinzip (Delegation von Kompetenzen, normative Dichte, Legitimität der erlassenden Behörde) und ihre Änderung wäre zeitaufwendig, da das ordentliche Verfahren für die Revision von Verordnungen innerhalb der Bundesverwaltung durchlaufen werden müsste.
- Bei nicht verbindlichen Regeln (Regeln der «Guten Praxis») würden sich die vorangehend aufgeworfenen Fragen zum Legalitätsprinzip weniger stellen. Nicht verbindliche Regeln könnten sehr rasch angepasst werden und würden den für die Datenbearbeitung Verantwortlichen einen gewissen Spielraum einräumen. Diese könnten auch andere Bestimmungen anwenden. Um für die Datenbearbeitenden Anreize zur Befolgung der Regeln der Guten Praxis zu setzen, könnte eine gesetzliche Vermutung geschaffen werden, wonach die Bearbeitung von Personendaten rechtmässig ist, sofern sich der Datenbearbeitende an die Regeln der Guten Praxis gehalten hat. Diese gesetzliche Vermutung würde sowohl für private Datenbearbeitende als auch für datenbearbeitende Bundesorgane gelten. Dabei könnte man sich beispielsweise an Art. 52*a* der Verordnung über die Verhütung von Unfällen und Berufskrankheiten (VUV; SR 832.30) orientieren. Gemäss dieser Bestimmung wird vermutet, dass der Arbeitgeber die Vorschriften über die Arbeitssicherheit erfüllt, wenn er die von der Koordinationskommission aufgestellten Richtlinien befolgt (Abs. 2). Der Arbeitgeber kann die Vorschriften über die Arbeitssicherheit jedoch auf andere Weise erfüllen, als dies die Richtlinien vorsehen, wenn er nachweist, dass die Sicherheit der Arbeitnehmer gleichermassen gewährleistet ist (Abs. 3). Da die Regeln der Guten Praxis nicht verbindlich wären, würden sie hauptsächlich auf dem guten Willen ihrer Adressaten beruhen, was ihre Wirksamkeit verringern könnte.

Eine *Mehrheit der Begleitgruppe* schlägt vor, die (verbindlichen oder nicht verbindlichen) Detailregeln von einem spezialisierten Expertenkomitee (nachfolgend «Komitee») erarbeiten zu lassen, das sich von der Datenschutzaufsichtsbehörde im engeren Sinn unterscheidet (vgl. auch Ziff. 4.10.2 lit. c und Ziff. 4.10.3). Dieses Organ sollte sich aus unabhängigen Sachverständigen und nicht aus Vertretern der interessierten Kreise zusammensetzen.[20] Die interessierten Kreise würden zur Ausarbeitung der Regeln allerdings konsultiert. Das Komitee könnte ihnen auch den Auftrag erteilen, selbst solche Regeln zu erstellen. Im Übrigen könnten die interessierten Kreise dem Komitee auf eigene Initiative hin ihre Regeln zur Genehmigung unterbreiten.[21] Diese Regeln würden in allen Fällen den Konsumentenschutzorganisationen zur Stellungnahme vorgelegt.

---

[20] Das Gesetz bzw. die Verordnung sollten insbesondere Bestimmungen zur Wahl, zur Amtszeit, zu den Interessenkonflikten der Komiteemitglieder und zur Stellung des Komitees gegenüber der Datenschutzaufsichtsbehörde enthalten.

[21] Ein Verfahren, das in diese Richtung geht, kennt beispielsweise das österreichische Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000) in § 6 Abs. 4: «Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem

- Variante: Das Komitee soll nur dann für die Erarbeitung von Detailregelungen zuständig sein, wenn die interessierten Kreise ihren Auftrag zum Erlass solcher Regeln nicht innerhalb einer bestimmten Frist ausgeführt haben.

Eine *Minderheit der Begleitgruppe* lehnt die Schaffung eines Expertenkomitees ab, da dieses ihrer Auffassung nach zusätzlichen administrativen und finanziellen Aufwand verursachen und den Datenschutz schwächen würde. Diese Minderheit schlägt vor, die Kompetenz zum Erlass bzw. zur Genehmigung von Regeln, welche das Datenschutzgesetz konkretisieren, der Datenschutzaufsichtsbehörde zu übertragen (vgl. Ziff. 4.10.3).

4.2 Geltungsbereich und Begriffe

4.2.1 Geltungsbereich

a) Persönlicher Geltungsbereich

Das Datenschutzgesetz regelt die Bearbeitung von Personendaten sowohl durch private Personen als auch durch Bundesorgane (Art. 2 Abs. 1 DSG). Auf die Bearbeitung von Personendaten durch kantonale Organe ist das DSG – unter Vorbehalt von Art. 37 DSG – dagegen nicht anwendbar. Im Rahmen der vorliegenden Arbeiten wurde die Frage geprüft, ob diese Kompetenzverteilung zwischen Bund und Kantonen im Bereich des Datenschutzes noch adäquat ist[22] oder ob eine Harmonisierung angestrebt werden soll, welche den Anwendungsbereich des DSG auf die kantonalen Organe ausweiten würde. Eine solche Erweiterung der Gesetzgebungskompetenz des Bundes im Bereich Datenschutz würde eine Teilrevision der Bundesverfassung voraussetzen.

Auf Ersuchen der Vorsteherin des EJPD hat die Konferenz der Kantonsregierungen (KdK) zu dieser Frage eine Anhörung bei den Kantonen durchgeführt. Die Anhörung hat ergeben, dass eine Mehrheit der Kantone einer Ausdehnung des Geltungsbereichs des DSG auf Datenbearbeitungen durch kantonale Organe ablehnend gegenübersteht. Anlässlich des Föderalistischen Dialogs vom Herbst 2013 hat die Vorsteherin des EJPD den Kantonen bereits mitgeteilt, dass sie die Idee einer solchen gesamtschweizerischen Vereinheitlichung des Datenschutzrechts nicht weiterführe. Der persönliche Geltungsbereich des DSG soll somit auch künftig auf Datenbearbeitungen begrenzt bleiben, die von Bundesorganen und privaten Personen vorgenommen werden. Für das Bearbeiten von Personendaten durch kantonale Organe soll das DSG nur unter den Voraussetzungen von Art. 37 beim Vollzug von Bundesrecht Anwendung finden.

Vom Anwendungsbereich des DSG werden auch die Medien erfasst. Dies soll weiterhin gelten. Allerdings ist dem Schutz des Redaktionsgeheimnisses – insbesondere im Rahmen der Bestimmungen zum Auskunftsrecht (vgl. Ziff. 4.4.3) – speziell Rechnung zu tragen. Zudem sind die besonderen Interessen der Medien auch mit Blick auf das «Recht auf Vergessen» zu berücksichtigen (vgl. Ziff. 4.4.5).

b) Sachlicher Geltungsbereich

Gegenwärtig gilt das Datenschutzgesetz für das Bearbeiten von Personendaten natürlicher und juristischer Personen (Art. 2 Abs. 1 DSG). Damit unterscheidet sich das DSG

---

sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes begutachtet und als gegeben erachtet hat.»

[22] Vgl. den Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335, 350.

massgeblich von der Datenschutzkonvention SEV 108 und verschiedenen Gesetzgebungen europäischer Staaten, in welchen ausschliesslich natürliche Personen Schutzobjekte der Datenschutzregelungen sind. Die Begleitgruppe hat daher untersucht, ob juristische Personen weiterhin im gleichen Mass geschützt werden sollen wie natürliche Personen.

Eine *Mehrheit der Begleitgruppe* ist zur Auffassung gelangt, dass das DSG auch künftig auf Personendaten juristischer Personen Anwendung finden soll. Eine Ausklammerung der Daten juristischer Personen aus dem Geltungsbereich des DSG erachtet sie als inkohärent zum schweizerischen Rechtssystem, wonach juristische Personen vom Persönlichkeitsschutz des Zivilgesetzbuches (Art. 53 i.V.m. Art. 28 ff. ZGB [SR 210]) erfasst werden. Aber auch in der Sache selbst könnte eine Nichtunterstellung der Daten juristischer Personen unter das DSG nach Ansicht der Mehrheit der Begleitgruppe zu unbefriedigenden Ergebnissen führen. Insbesondere kleine Unternehmen oder Familienunternehmen können bei der Bearbeitung ihrer Daten ähnliche Schutzbedürfnisse aufweisen wie natürliche Personen, namentlich wenn die Angaben über die juristischen Personen auch einen Bezug zu den natürlichen Personen hinter den Unternehmen aufweisen.

Allerdings sollte gemäss dem Vorschlag der Mehrheit der Begleitgruppe das Bearbeiten von Daten juristischer Personen im Rahmen ihrer Geschäftstätigkeit als Rechtfertigungsgrund des überwiegenden privaten Interesses in Art. 13 Abs. 2 DSG aufgenommen werden (vgl. nachfolgend Ziff. 4.8.2). Dieser Rechtfertigungsgrund würde praktische Erleichterungen im Geschäftsverkehr erlauben, ohne den Schutz der Daten der juristischen Personen allzu stark zu beeinträchtigen. Denn einerseits handelt es sich bei diesem Vorschlag – wie bei den weiteren in Art. 13 Abs. 2 DSG genannten Tatbeständen – nicht um einen absoluten Rechtfertigungsgrund, bei dessen Vorliegen eine Datenbearbeitung per se gerechtfertigt wäre. Vielmehr wäre auch in einer solchen Konstellation eine wertende Interessenabwägung unter Berücksichtigung aller Umstände des Einzelfalls durchzuführen. Ausserdem stünden den juristischen Personen bei Datenbearbeitungen, die nicht ihre Geschäftstätigkeit betreffen, unverändert sämtliche Rechtsbehelfe des Datenschutzes zur Verfügung.

Um schliesslich den grenzüberschreitenden Datenverkehr mit Ländern, deren Rechtsordnungen Personendaten von juristischen Personen nicht schützen, zu erleichtern, schlägt die Mehrheit der Begleitgruppe vor, gesetzlich festzulegen, dass die Angemessenheit des Datenschutzes nach Art. 6 DSG nicht den Schutz von Personendaten juristischer Personen voraussetzt (vgl. nachfolgend Ziff. 4.5).

Eine *Minderheit der Begleitgruppe* spricht sich für die vollständige Ausklammerung der Personendaten juristischer Personen aus dem Geltungsbereich des DSG aus. Zur Begründung verweist sie auf die Rechtslage in zahlreichen europäischen Staaten sowie auf den Modernisierungsentwurf zur Datenschutzkonvention SEV 108, welche ausschliesslich die Daten natürlicher Personen schützen. Überdies erachtet die Minderheit der Begleitgruppe den Persönlichkeitsschutz juristischer Personen bereits durch das ZGB (Art. 28 ff.), das Bundesgesetz gegen den unlauteren Wettbewerb (UWG; SR 241) sowie das Geschäftsgeheimnis als ausreichend gewährleistet. Eine Unterstellung unter das Datenschutzgesetz hält sie allenfalls für Fälle denkbar, in welchen eine Person als Inhaberin eines Einzelunternehmens erkennbar ist.

c) Räumlicher Geltungsbereich

Wie die Evaluation des DSG gezeigt hat, gewinnt die internationale Dimension von Datenbearbeitungen angesichts der fortschreitenden technologischen Entwicklungen immer mehr an Bedeutung. Datenbearbeitungen erfolgen zunehmend grenzüberschreitend, was zu komplexen und intransparenten Situationen für die betroffenen Personen und die

Datenschutzaufsichtsbehörde, aber auch für die Datenbearbeitenden führen kann.[23] Die Begleitgruppe hat deshalb überprüft, ob diese neuen Herausforderungen Anpassungen des räumlichen Geltungsbereichs des DSG (insbesondere hinsichtlich seiner Anwendung auf internationale Sachverhalte) erforderlich machen.

Das DSG enthält bislang keine ausdrücklichen Bestimmungen zu seinem territorialen Geltungsbereich. Für die zivilrechtlichen Vorschriften des DSG steht mit dem Internationalen Privatrecht ein spezielles Kollisionsrecht zur Verfügung. Das Bundesgesetz über das Internationale Privatrecht (IPRG; SR 291) regelt für den privatrechtlichen Datenschutz – unter Vorbehalt völkerrechtlicher Verträge – unter anderem die Zuständigkeit der schweizerischen Gerichte oder Behörden (vgl. Art. 129 Abs. 1[24] und Art. 130 Abs. 3 IPRG[25]) sowie das auf Ansprüche aus Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten anzuwendende Recht (vgl. insbesondere Art. 139 IPRG[26]). Nach dem Eindruck der Begleitgruppe führt diese Regelung zu einem breiten räumlichen Geltungsbereich des DSG, mit dem die privatrechtlichen Datenschutzvorschriften auch auf gewisse Datenbearbeitungen im Ausland anwendbar werden können. Die Begleitgruppe schlägt diesbezüglich keine Änderungen vor.

Das öffentliche Recht kennt dagegen kein spezielles internationales Kollisionsrecht. Für die öffentlich-rechtlichen Bestimmungen des DSG gilt das Territorialitätsprinzip, wonach schweizerisches Recht grundsätzlich nur anwendbar ist auf Sachverhalte, die sich in der Schweiz zutragen. Nach der Praxis des Bundesgerichts kann das schweizerische öffentliche Recht unter Umständen aber auch auf Sachverhalte Anwendung finden, die sich zwar im Ausland zutragen, aber in einem ausreichenden Mass auf dem Territorium der Schweiz auswirken (Auswirkungsprinzip).[27] Eine *Mehrheit der Begleitgruppe* schlägt vor, diese bundesgerichtliche Rechtsprechung im DSG für das öffentlich-rechtliche Datenschutzrecht

---

[23] Vgl. den Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335, 341 f., 349.

[24] Art. 129 Abs. 1 IPRG: «Für Klagen aus unerlaubter Handlung sind die schweizerischen Gerichte am Wohnsitz des Beklagten oder, wenn ein solcher fehlt, diejenigen an seinem gewöhnlichen Aufenthaltsort zuständig. Überdies sind die schweizerischen Gerichte am Handlungs- oder Erfolgsort sowie für Klagen aufgrund der Tätigkeit einer Niederlassung in der Schweiz die Gerichte am Ort der Niederlassung zuständig.»

[25] Art. 130 Abs. 3 IPRG: «Klagen zur Durchsetzung des Auskunftsrechts gegen den Inhaber einer Datensammlung können bei den in Artikel 129 genannten Gerichten oder bei den schweizerischen Gerichten am Ort, wo die Datensammlung geführt oder verwendet wird, eingereicht werden.»

[26] Nach Art. 139 Abs. 3 i.V.m. Abs. 1 IPRG unterstehen Ansprüche aus Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten sowie aus Beeinträchtigung des Rechts auf Auskunft über Personendaten «nach Wahl des Geschädigten: a. dem Recht des Staates, in dem der Geschädigte seinen gewöhnlichen Aufenthalt hat, sofern der Schädiger mit dem Eintritt des Erfolges in diesem Staat rechnen musste; b. dem Recht des Staates, in dem der Urheber der Verletzung seine Niederlassung oder seinen gewöhnlichen Aufenthalt hat, oder c. dem Recht des Staates, in dem der Erfolg der verletzenden Handlung eintritt, sofern der Schädiger mit dem Eintritt des Erfolges in diesem Staat rechnen musste.»

[27] Zum Auswirkungsprinzip als spezielle Ausprägung des Territorialitätsprinzips vgl. insbesondere BGE 133 II 331, 341 f. E. 6.1. Für das Datenschutzrecht hat das Bundesgericht z.B. in BGE 138 II 346, 352 f. E. 3.3 («Google Street View») festgehalten, dass für Bilder, die in der Schweiz aufgenommen und so veröffentlicht werden, dass sie in der Schweiz abrufbar sind, ein überwiegender Anknüpfungspunkt zur Schweiz vorliegt, selbst wenn die Bilder im Ausland weiterbearbeitet und nicht direkt von der Schweiz aus ins Internet gestellt werden.

ausdrücklich zu kodifizieren.[28] Damit soll klargestellt werden, dass das DSG auch auf Sachverhalte anwendbar ist, die Auswirkungen in der Schweiz entfalten, selbst wenn die Datenbearbeitung im Ausland veranlasst wird. Solche Sachverhalte sollen ausserdem in die Zuständigkeit der Datenschutzaufsichtsbehörde fallen. Eine *Minderheit der Begleitgruppe* spricht sich gegen diesen Vorschlag aus. Nach ihrer Ansicht würde eine Kodifizierung der bundesgerichtlichen Rechtsprechung zum Territorialitäts- bzw. Auswirkungsprinzip Rechtsunsicherheiten schaffen. Auch in anderen Rechtsbereichen werde keine Legaldefinition des Territorialitätsprinzips verwendet. Unklar wäre insbesondere, ob und inwiefern die differenzierte Rechtsprechung des Bundesgerichts für das öffentliche Datenschutzrecht weitergelten würde. Es bestehe die Gefahr, dass es zu – von der Begleitgruppe nicht beabsichtigten – Diskrepanzen zur Bundesgerichtspraxis kommen könnte.

Da das DSG auch gegenüber Datenbearbeitenden, die keinen (Wohn-)Sitz in der Schweiz haben, zur Anwendung gelangen kann, schlägt die Begleitgruppe ferner vor, diese Personen in bestimmten Fällen im Interesse der Verfahrensbeschleunigung zu verpflichten, eine Zustelladresse in der Schweiz zu bezeichnen (vgl. nachfolgend Ziff. 4.10.2 lit. a/aa).

d) Ausnahmen vom Geltungsbereich

da) Datenbearbeitung zu ausschliesslich persönlichen Zwecken

Der Ausnahmetatbestand gemäss Art. 2 Abs. 2 lit. a DSG ist an Art. 3 Abs. 1bis des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108[29] anzupassen. Die Begleitgruppe schlägt vor, das Tatbestandsmerkmal der Nichtbekanntgabe an Aussenstehende aufzuheben und die Bestimmung so umzuformulieren, dass das DSG nicht für Datenbearbeitungen gilt, die von einer natürlichen Person im Zusammenhang mit der Ausübung ausschliesslich persönlicher Tätigkeiten vorgenommen werden. Dabei geht es hauptsächlich um die Verwendung von Personendaten im Familien- und engen Freundeskreis. Sofern keine enge Beziehung besteht, gehören «Freunde» in sozialen Netzwerken[30] nicht zu dieser Kategorie.

db) Weitere Ausnahmen

Aufgrund des speziellen Status des Internationalen Komitees vom Roten Kreuz (IKRK) schlägt die Begleitgruppe vor, die Ausnahmeklausel von Art. 2 Abs. 2 lit. e DSG, welche Personendaten, die das IKRK bearbeitet, vom Geltungsbereich des DSG ausnimmt, beizubehalten. Dabei geht die Begleitgruppe davon aus, dass der Modernisierungsentwurf zur Datenschutzkonvention SEV 108 eine solche Ausnahmeregelung weiterhin zulässt. Der Hintergrund dieser Ausnahme liegt darin, dass das IKRK zunehmend als Subjekt des Völkerrechts anerkannt wird und dass Subjekte des Völkerrechts nicht ohne Weiteres einem innerstaatlichen Recht unterworfen werden können.[31] In der Lehre wird unter anderem

---

[28] Eine ähnliche Vorschrift findet sich beispielsweise für das Wettbewerbsrecht in Art. 2 Abs. 2 des Kartellgesetzes (KG; SR 251): «Das Gesetz ist auf Sachverhalte anwendbar, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.»

[29] Art. 3 Abs. 1bis des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108: «La présente Convention ne s'applique pas aux traitements de données effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.»

[30] Zur Problematik der sozialen Netzwerke siehe den Bericht des Bundesrates «Rechtliche Basis für Social Media: Bericht des Bundesrates in Erfüllung des Postulats Amherd 11.3912 vom 29. September 2011».

[31] Vgl. dazu die Botschaft des Bundesrates vom 23. März 1988 zum Bundesgesetz über den Datenschutz (DSG), BBl 1988 II 413, 440.

kritisiert, dass nicht auch andere internationale Organisationen unter diesem Ausnahmetatbestand zum DSG aufgeführt werden, was mit Blick auf das verfassungsrechtliche Gleichbehandlungsgebot (Art. 8 BV) problematisch sei.[32] In der Botschaft zur Änderung des DSG vom 19. Februar 2003 hat der Bundesrat vorgesehen, alle internationalen Organisationen, welche in der Schweiz ansässig sind und mit denen ein Sitzabkommen besteht, ausdrücklich vom Geltungsbereich des DSG auszunehmen.[33] Diese Regelung ist vom Parlament jedoch nicht übernommen worden, weshalb die Begleitgruppe im Rahmen der vorliegenden Arbeiten ebenfalls keine solche Erweiterung von Art. 2 Abs. 2 lit. e DSG vorschlägt.

Die übrigen Ausnahmen zum Geltungsbereich des DSG können nach Ansicht der Begleitgruppe nur beibehalten werden, soweit auch in diesen Bereichen die Anforderungen des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 erfüllt werden. Die revidierte Datenschutzkonvention SEV 108 wird den Staaten voraussichtlich keine Möglichkeit mehr einräumen, Vorbehalte zum Geltungsbereich des Übereinkommens abzugeben.[34]

- Die Ausnahme der öffentlichen Register des Privatrechtsverkehrs (Art. 2 Abs. 2 lit. d DSG) sollte nach Auffassung der Begleitgruppe aus mehreren Gründen aufgehoben werden. Zunächst rechtfertigt der Umstand, dass diese Register durch Spezialgesetze geregelt werden, keine Ausklammerung des DSG. So unterliegen auch andere Bereiche (wie beispielsweise das Strafregister) dem DSG, obwohl für sie spezifische Bestimmungen bestehen. Sodann entspricht die Ausnahme für öffentliche Register des Privatrechts insofern nicht praktischen Bedürfnissen, als der EDÖB diesbezüglich sehr häufig zu Fragen kontaktiert wird, die mit dem DSG zusammenhängen. Ausserdem bestehen im Registerrecht oftmals Verknüpfungen zu anderen Gebieten, auf die das DSG anwendbar ist, womit diese Dichotomie schwierig umzusetzen ist. Selbst wenn die öffentlichen Register des Privatrechtsverkehrs dem Geltungsbereich des DSG unterstellt werden, kann den Besonderheiten der jeweiligen Register immer noch mit spezialgesetzlichen Vorschriften Rechnung getragen werden.
- Hinsichtlich der übrigen Ausnahmen (Art. 2 Abs. 2 lit. b und c DSG) ist abzuklären, ob diese weiterhin gültig bleiben, ob sie geändert werden müssen oder ob die Anforderungen des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 (bzw. des EU-Rechts) im Rahmen der Spezialgesetzgebung umgesetzt werden sollen. Die Begleitgruppe hat dazu zwei konkrete Vorgehensweisen erörtert. Entweder sollen die Ausnahmetatbestände aufgehoben und dem DSG unterstellt werden, oder die Ausnahmen werden beibehalten und es wird überprüft, ob die ihnen zugrundeliegenden Spezialerlasse den datenschutzrechtlichen Anforderungen genügen.

4.2.2 Begriffe

Die Begleitgruppe schlägt vor, die Legaldefinitionen für die Ausdrücke «Personendaten» (Art. 3 lit. a DSG), «Datensammlung» (Art. 3 lit. g DSG) und «Bekanntgeben» (Art. 3 lit. f DSG) beizubehalten. Es besteht kein Grund, diese Begriffe zu ändern, da sie in der Praxis

---

[32] Vgl. MAURER-LAMBROU/KUNZ, in: Basler Kommentar DSG/BGÖ, 3. Aufl., Basel 2014, N 41 zu Art. 2 DSG.

[33] Vgl. BBl 2003 2101, 2123 f.

[34] Anlässlich ihres Beitritt zur geltenden Datenschutzkonvention SEV 108 hat die Schweiz erklärt, dass das Übereinkommen keine Anwendung finde auf Datensammlungen, die von den eidgenössischen Räten und den kantonalen Parlamenten im Rahmen ihrer Beratungen angelegt und benutzt werden, sowie auf Datensammlungen des Internationalen Komitees vom Roten Kreuz; vgl. AS 2002 2847, 2867.

der Datenschutzaufsichtsbehörde und der schweizerischen Gerichten gut integriert sind.

Falls erforderlich sind die Begriffsbestimmungen und die Terminologie an den Modernisierungsentwurf zur Datenschutzkonvention SEV 108 anzupassen. Dies gilt insbesondere für die Definition der «besonders schützenswerten Personendaten» (Art. 3 lit. c DSG). Im Konventionsentwurf ist vorgesehen, genetische und biometrische Daten in diesen Begriff einzuschliessen. Um die Definition nicht zu weit zu fassen (damit beispielsweise nicht jedes Foto *per se* zu den besonders schützenswerten Personendaten gezählt wird), könnte sie nach dem Vorbild von Art. 6 Abs. 1 des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108[35] eingeschränkt werden. Für den Fall, dass das DSG auch inskünftig auf die Daten juristischer Personen Anwendung findet (vgl. Ziff. 4.2.1 lit. b), schlägt die Begleitgruppe vor, nur die Daten von natürlichen Personen als besonders schützenswerte Personendaten zu betrachten.

Mit Bezug auf den Begriff des «Inhabers der Datensammlung» (Art. 3 lit. i DSG) hat die Begleitgruppe diskutiert, inwiefern eine Angleichung an die Terminologie der Datenschutzkonvention SEV 108 bzw. des EU-Rechts, welche die Figur des «responsable du traitement»[36] bzw. des «für die Verarbeitung Verantwortlichen»[37] kennen, zweckmässig sein könnte. Dabei ist allerdings noch vertieft zu prüfen, welche materiell-rechtlichen Konsequenzen eine solche Anpassung der Terminologie nach sich ziehen würde, da die Begriffe im schweizerischen und europäischen Recht nicht deckungsgleich verwendet werden. Eine begriffliche Angleichung soll nicht zu Rechtsunsicherheiten führen.

Neu könnten die Begriffe «Auftragsdatenbearbeitender» und «Datenempfänger» definiert werden. Andernfalls könnte die Formulierung des derzeitigen Art. 10*a* DSG überarbeitet werden, um eine Verwechslung mit dem Begriff der «Dritten» in anderen Bestimmungen zu vermeiden (z.B. Art. 9, 12, 13 oder 14 DSG).

Schliesslich schlägt die Begleitgruppe vor, den Begriff des «Persönlichkeitsprofils» (Art. 3 lit. d DSG) aufzugeben. Dieser Begriff wird nur in der Schweiz verwendet und hat in der Praxis geringe Auswirkungen, da die sich für die Bearbeitung von Persönlichkeitsprofilen ergebenden besonderen Rechtsfolgen (vgl. etwa Art. 4 Abs. 5 und Art. 14 DSG) – vor allem im privaten Bereich – nur selten eingehalten werden. Diese Problematik soll mit wirksameren Mitteln wie einer Regelung zu den automatisierten Einzelentscheidungen (vgl. Ziff. 4.4.6) oder einem risikobasierten Ansatz (vgl. Ziff. 4.3.2) angegangen werden.

---

[35] Art. 6 Abs. 1 des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108: «Le traitement de données génétiques ou de données concernant des infractions, condamnations pénales et mesures de sûreté connexes, le traitement de données biométriques identifiant un individu de façon unique, ainsi que le traitement de données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle, n'est autorisé qu'à la condition que la loi applicable prévoit des garanties appropriées, venant compléter celles de la présente Convention».

[36] Vgl. Art. 2 lit. d des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108.

[37] Vgl. Art. 4 Abs. 5 des Entwurfs zur EU-Datenschutz-Grundverordnung sowie Art. 3 Abs. 6 des Entwurfs zur EU-Datenschutz-Richtlinie.

4.3 Allgemeine Grundsätze des Datenschutzes

4.3.1 Transparenz der Datenbearbeitung

Gegenwärtig werden der Grundsatz der Erkennbarkeit und die Informationspflicht beim Beschaffen von Personendaten an verschiedenen Stellen des Gesetzes geregelt, nämlich in Art. 4 Abs. 4 DSG sowie in Art. 14 DSG (für private Datenbearbeitende) und Art. 18–18*b* DSG (für datenbearbeitende Bundesorgane). Eine *Mehrheit der Begleitgruppe* schlägt vor, diese beiden Themen in einer einzigen Bestimmung zu behandeln, die sowohl für den privaten als auch für den öffentlichen Bereich gelten soll. Dies hätte den Vorteil, dass das Gesetz vereinfacht und Doppelspurigkeiten vermieden würden. Dabei würde eine *Informationspflicht* vorgesehen, die für alle Arten von Daten greift, wie dies derzeit bereits im öffentlichen Sektor der Fall ist (vgl. auch die Regelungen im Modernisierungsentwurf zur Datenschutzkonvention SEV 108[38] sowie im EU-Recht[39]). Es würde somit auf eine unterschiedliche Behandlung von besonders schützenswerten und gewöhnlichen Personendaten verzichtet. Soweit die betroffene Person nicht bereits darüber informiert ist, müssten ihr die beschafften Daten, der Zweck, allfällige Kategorien von Datenempfängern sowie die Rechte, die ihr von Gesetzes wegen eingeräumt werden, mitgeteilt werden. Ausserdem müssten ihr die Kontaktdaten der für die Datenbearbeitung verantwortlichen Person bekannt gegeben werden, damit sie sich mit dieser in Verbindung setzen kann. Die Informationspflicht würde als erfüllt gelten, wenn aus den Umständen klar hervorgeht, dass die betroffene Person von allen massgebenden Aspekten Kenntnis haben sollte. Die Modalitäten der Informationspflicht könnten in Regeln der Guten Praxis oder in verbindlichen Detailregeln konkretisiert werden (vgl. Ziff. 4.1.2 lit. b). Abgesehen vom Fall, dass die betroffene Person bereits informiert worden ist, sollten Ausnahmen von der Informationspflicht eingeräumt werden, wenn die Datenbearbeitung im Gesetz vorgesehen ist, wenn die Information mit unverhältnismässigem Aufwand verbunden ist oder wenn es darum geht, das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen. Die Bestimmung zur Informationspflicht wäre als Datenbearbeitungsgrundsatz auszugestalten.

Eine *Minderheit der Begleitgruppe* lehnt die Einführung einer allgemeinen Informationspflicht ab. Sie ist insbesondere der Auffassung, dass Unternehmen dadurch in einem unverhältnismässigen Umfang belastet würden.

Ein weiteres wesentliches Instrument zur Herstellung von Transparenz bei Datenbearbeitungen ist das Auskunftsrecht der betroffenen Person, das diese beim Inhaber einer Datensammlung ausüben kann. Die Begleitgruppe schlägt vor, dieses Recht zu stärken. Dieses Thema wird nachfolgend unter Ziff. 4.4.3 behandelt.

4.3.2 Sorgfaltspflichten

Entsprechend der Art. 7 und 8bis Abs. 2, 3 und 4 des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 sowie im Hinblick auf die Umsetzung der Postulate Schwaab 13.3806 «Schutz der Privatsphäre durch „privacy by default“» und 13.3807 «Verstärkung des Datenschutzes durch „privacy by design“»[40] und des Postulats Recor-

[38] Vgl. Art. 7bis des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108.

[39] Vgl. Art. 14 des Entwurfs zur EU-Datenschutz-Grundverordnung und Art. 11 des Entwurfs zur EU-Datenschutz-Richtlinie.

[40] Die Postulate Schwaab 13.3806 und 13.3807 vom 25. September 2013 wurden vom Nationalrat noch nicht behandelt.

don 13.3989 «Verletzungen der Persönlichkeitsrechte im Zuge des Fortschritts der Informations- und Kommunikationstechnik»[41] schlägt die Begleitgruppe vor, Verpflichtungen der für die Datenbearbeitung Verantwortlichen oder allfälliger Auftragsdatenbearbeitender einzuführen, wonach diese bestimmte Massnahmen ergreifen müssen, um Gesetzesverstösse zu verhindern [42] und zu beseitigen bzw. um die damit verbundenen Konsequenzen zu verringern.[43]

Dazu gehören insbesondere folgende Sorgfaltspflichten:

- Sicherstellung technischer und organisatorischer Massnahmen zur Gewährleistung der Datensicherheit.
- Grundsatz «Privacy by Design»: Verpflichtung der für die Datenbearbeitung Verantwortlichen (oder allfälliger Auftragsdatenbearbeitender), bereits bei der Konzeption einer Datenbearbeitung – soweit diese der Bearbeitung von Personendaten dient – die datenschutzrechtlichen Anforderungen zu berücksichtigen[44] und angemessene Schutzmassnahmen einzubauen (z.B. Beschränkung der durch die Anwendung bearbeiteten Daten auf das für die Zweckerreichung zwingende Minimum; dezentrale Speicherung von beschafften Personendaten; Einbau von technischen Sicherheitsmassnahmen, um das Risiko von missbräuchlichen Bearbeitungen zu minimieren). Bei der Umsetzung dieser Verpflichtung sind unter anderem die mit der jeweiligen Datenbearbeitung einhergehenden Risiken für den Persönlichkeitsschutz, die technischen Möglichkeiten, die anerkannten Standards sowie die mit der Massnahme verbundenen Kosten zu berücksichtigen. Dabei ist den Schutzbedürfnissen der Minderjährigen und anderer besonders verletzlicher Personengruppen speziell Rechnung zu tragen.
- Grundsatz «Privacy by Default»: Wird bei einer Anwendung, welche Personendaten bearbeitet, den Nutzenden die Wahlmöglichkeit zwischen mehreren unterschiedlich datenschutzfreundlichen Systemeinstellungen gegeben, so ist als Standardeinstellung die datenschutzfreundlichste vorzugeben.[45] Speziell zu berücksichtigen sind die

---

[41] Das Postulat Recordon 13.3989 vom 27. September 2013 wurde vom Ständerat am 11. Dezember 2013 angenommen.

[42] Im Verlauf der weiteren Revisionsarbeiten zum DSG ist in diesem Zusammenhang zu prüfen, ob das Vorsorgeprinzip, das seine Wurzeln im Umweltrecht hat, auch im Datenschutzrecht als allgemeiner Grundsatz implementiert werden könnte. Zum Vorsorgeprinzip im Umweltrecht vgl. insbesondere Art. 1 Abs. 2 des Umweltschutzgesetzes (USG; SR 814.01): «Im Sinne der Vorsorge sind Einwirkungen, die schädlich oder lästig werden könnten, frühzeitig zu begrenzen». Siehe dazu auch das Synthesepapier der interdepartementalen Arbeitsgruppe «Vorsorgeprinzip» von August 2003 «Das Vorsorgeprinzip aus schweizerischer und internationaler Sicht».

[43] Am 17. September 2014 wurde das Postulat Schwaab 14.3739 «Control by Design. Die Rechte auf Eigentum im Falle von unerwünschten Verbindungen verstärken» eingereicht. Der Bundesrat beantragt die Annahme des Postulats. Die in diesem Kapitel vorgesehenen Massnahmen im Zusammenhang mit den Sorgfaltspflichten könnten zum Teil zur Umsetzung des Postulats beitragen, falls es vom Parlament angenommen wird.

[44] Ein ähnlicher Regelungsansatz findet sich im Bereich des Umwelt- und Raumplanungsrechts z.B. in Art. 3 der Eisenbahnverordnung (EBV; SR 742.141.1): «Den Belangen der Raumplanung, des Umweltschutzes und des Natur- und Heimatschutzes ist bereits bei der Planung und Projektierung Rechnung zu tragen.» (Abs. 1). «Die Bedürfnisse der Behinderten sind angemessen zu beachten.» (Abs. 2).

[45] Der Grundsatz «Privacy by Default» steht in engem Zusammenhang zum Verhältnismässigkeitsprinzip sowie zum Grundsatz «Privacy by Design». Aus diesen Prinzipen kann sich für Datenbearbeitende in gewissen Fällen

Schutzbedürfnisse von Minderjährigen und anderen besonders verletzlichen Personengruppen.

- Pflicht zur angemessen Dokumentation der Datenbearbeitungsvorgänge: Hintergrund ist die Überlegung, dass Datenschutz nur betreiben kann, wer weiss, welche Daten er wie bearbeitet, und dass dies mit wachsender Betriebsgrösse, Komplexität des Betriebs und Umfang der Datenbearbeitungen nur noch mit entsprechender Dokumentation möglich ist. Eine angemessene Dokumentation muss gerade bei grösseren Unternehmen die Datenbearbeitung, die Verfahren und Abläufe, die Organisation und Zuständigkeiten und auch die Mittel in einer gewissen Granularität darstellen. Ähnliche Regelungen finden sich auch in anderen Erlassen (vgl. z.B. Art. 4 der Geschäftsbücherverordnung [GeBüV; SR 221.431]). Diese Dokumentation könnte das bestehende Konzept der Inventarliste im Sinne von Art. 11*a* DSG (vgl. Ziff. 4.7) und möglicherweise des Bearbeitungsreglements ablösen. Ein Recht auf Einblick in die Dokumentation sollte gemäss der Begleitgruppe aber nicht vorgesehen sein, da der Einblick der Transparenz nicht wirklich dienen würde und eine solche Dokumentation in aller Regel etliche Geschäftsgeheimnisse und auch sicherheitsrelevante Informationen enthält. Der Zugang für die Datenschutzaufsichtsbehörde bleibt vorbehalten.
- Durchführung von Datenschutzfolgenabschätzungen: Besteht im Zusammenhang mit einer Datenbearbeitung ein erhöhtes Risiko für Persönlichkeitsverletzungen, muss der für die Datenbearbeitung Verantwortliche eine Analyse zu den potenziellen Auswirkungen der geplanten Datenbearbeitung (RFA) auf die Rechte der betroffenen Personen durchführen und diese Analyse auf Verlangen der Datenschutzaufsichtsbehörde vorlegen. Dabei muss den Auswirkungen auf Minderjährige und andere schutzbedürftige Personen besondere Beachtung geschenkt werden. In der schweizerischen Gesetzgebung lassen sich verschiedene Beispiele für RFA finden[46] (z.B. in Art. 7 der Verordnung über die Umweltverträglichkeitsprüfung[47], in Art. 5 des Chemikaliengesetzes[48] oder in Art. 5 der Verordnung der Eidgenössischen Spielbankenkommission über die Sorgfaltspflichten der Spielbanken zur Bekämpfung der Geldwäscherei[49]).
- Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzaufsichtsbehörde: Analog zu den Reformbestrebungen im Europarat schlägt die Begleitgruppe die Einführung einer Meldepflicht bei Datenschutzverletzungen vor («data breaches»; zur Begrifflichkeit vgl. Art. 4 Abs. 9 des Entwurfs zur EU-Datenschutz-

---

auch die Pflicht ergeben, bei einer Anwendung den Nutzenden eine Wahlmöglichkeit zwischen verschiedenen Systemeinstellungen einzuräumen.

[46] Siehe auch den britischen Bericht online unter <https://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment>.

[47] UVPV; SR 814.011.

[48] ChemG; SR 813.1.

[49] GwV ESBK; SR 955.021.

Grundverordnung[50]). Art. 7 Abs. 2 des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 schreibt – in Anlehnung an das Recht der EU[51] – vor, dass (zumindest) die Datenschutzaufsichtsbehörde ohne unangemessene Verzögerung über Datenschutzverletzungen, welche die (Persönlichkeits-)Rechte der betroffenen Personen schwer beeinträchtigten können, benachrichtigt werden muss. Um zu bestimmen, wann eine solche meldepflichtige Datenschutzverletzung vorliegt, sollten entsprechende Kriterien im Gesetz oder im Rahmen konkretisierender Handlungsanweisungen (z.B. in den Regeln der Guten Praxis; vgl. Ziff. 4.1.2 lit. b) aufgelistet werden. Ein *Teil der Begleitgruppe* ist der Ansicht, dass die Pflicht zur Notifikation der Aufsichtsbehörde nur ausgelöst werden soll, wenn eine grosse Anzahl von Personen von der Datenschutzverletzung betroffen ist. *Andere Mitglieder der Begleitgruppe* haben Zweifel, ob damit die Anforderungen des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 erfüllt werden und ziehen einen nicht abschliessenden Kriterienkatalog vor, der unter anderem auch die Art der betroffenen Daten sowie die Gefahr für die Persönlichkeitsrechte der betroffenen Personen berücksichtigt. Neben der Meldepflicht gegenüber der Aufsichtsbehörde schlägt die Begleitgruppe vor, die Datenbearbeitenden (bzw. allfällige Auftragsdatenbearbeitende) allgemein zu verpflichten, bei einer Datenschutzverletzung angemessene Massnahmen zur Schadensbegrenzung zu treffen. Dazu kann auch die Information der betroffenen Personen über die Datenschutzverletzung gehören.

– Einsetzung eines Datenschutzverantwortlichen: Ein *Teil der Mitglieder der Begleitgruppe* schlägt vor, im Rahmen der Sorgfaltsmassnahmen für Unternehmen ab einer bestimmten Grösse (z.B. über 250 Angestellte in Vollzeitäquivalenten) die Verpflichtung vorzusehen, einen Datenschutzverantwortlichen einzusetzen. Der Bundesrat könnte diese Verpflichtung auf kleinere Unternehmen ausweiten, bei denen ein erhöhtes Risiko besteht. Der Begriff «erhöhtes Risiko» wäre in der Botschaft, in der Verordnung oder in den Regeln der Guten Praxis bzw. in verbindliche Detailregeln (vgl. Ziff. 4.1.2 lit. b) zu präzisieren. Voraussichtlich könnte es sich dabei um Fälle handeln, in denen besonders schützenswerte Daten und Personendaten über Minderjährige oder andere schutzbedürftige Personen betroffen sind, die für die Erstellung von Profilen dienen oder mit anderen Daten verknüpft werden (siehe z.B. Art. 21 der Verordnung zum Bundesgesetz über den Datenschutz [VDSG; SR 235.11]). Die Unternehmen könnten auf externe Datenschutzverantwortliche zurückgreifen, insbesondere um von einem Know-how zu profitieren, über das sie sonst nicht verfügen würden, es sei denn, sie würden eine entsprechende Person anstellen oder einen Angestellten zu diesem Zweck ausbilden, was jedoch mit einem erheblichen finanziellen Aufwand verbunden sein könnte. Ein *anderer Teil der Begleitgruppe* ist der Meinung, dass die Verpflichtung zur Einsetzung eines Datenschutzverantwortlichen nicht

[50] Im Sinne von Art. 4 Abs. 9 des Entwurfs zur EU-Datenschutz-Grundverordnung bezeichnet der Ausdruck «Verletzung des Schutzes personenbezogener Daten» eine «Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder widerrechtlich, oder zur unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden».

[51] Vgl. zur geltenden Rechtslage Art. 4 Abs. 3 der Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) sowie die Verordnung (EU) Nr. 611/2013 vom 24. Juni 2013 über die Massnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäss der Richtlinie 2002/58/EG. De lege ferenda siehe Art. 31 f. des Entwurfs zur EU-Datenschutz-Grundverordnung und Art. 28 f. des Entwurfs zur EU-Datenschutz-Richtlinie.

im Gesetz festgehalten werden solle. Stattdessen könne es den Regeln der Guten Praxis (vgl. Ziff. 4.1.2 lit. b) überlassen werden, je nach Unternehmen angemessene Mittel vorzusehen, um eine Datenbearbeitung zu gewährleisten, mit welcher den Rechten der betroffenen Personen Rechnung getragen wird (z.B. durch die Bestimmung eines Datenschutzverantwortlichen).

Bei den Bundesorganen soll (anstelle des heutigen «Beraters für den Datenschutz» gemäss Art. 23 VDSG) immer ein Datenschutzverantwortlicher im Sinne von Art. 12*a* und 12*b* VDSG, der seine Funktion fachlich unabhängig und weisungsungebunden ausübt, eingesetzt werden müssen[52] (vgl. nachfolgend Ziff. 4.9.4). Diese Verpflichtung soll zumindest die Stufe Departement betreffen. Ob auch auf Amtsstufe ein Datenschutzverantwortlicher einzusetzen ist, könnte von der Art und Menge der von den jeweiligen Ämtern bearbeiteten Daten abhängig gemacht werden.

- Um den Einbezug des Datenschutzes insbesondere bei Informatikprojekten zu verbessern, schlägt ein *Teil der Begleitgruppe* vor, zu prüfen, ob die Bundesorgane verpflichtet werden sollten, in den Departementen Datenschutz- und Informationssicherheits-Managementsysteme aufzubauen. Diese Massnahme könnte sich allerdings bereits aus anderen Sorgfaltspflichten (wie dem Grundsatz «Privacy by Design» oder der Verpflichtung zur Datenschutzfolgenabschätzung) ergeben und ist eher auf Verordnungsstufe zu regeln.

4.3.3 Einwilligung

Bezüglich der Anforderungen an die Einwilligung, die bei den Datenbearbeitungsgrundsätzen geregelt sind (Art. 4 Abs. 5 DSG), schlägt die Begleitgruppe vor, das geltende System beizubehalten, sofern diese Lösung mit dem Modernisierungsentwurf zur Datenschutzkonvention SEV 108 vereinbar ist. Im Übrigen sollten nach Ansicht der Begleitgruppe Massnahmen ergriffen werden, um die Qualität der Einwilligung zu erhöhen. Denn aufgrund fehlender Informationen oder eines zu komplexen Informationsverfahrens, bisweilen aber auch wegen eines Mangels an Interesse erteilen die betroffenen Personen heute ihre Einwilligung zu Datenbearbeitungen, mit denen sie nicht vertraut sind, die sie nicht verstehen, die sie nicht interessieren und manchmal sogar zu denen sie sich nicht entschieden haben. Mit einem Ausbau der Informationspflicht (Ziff. 4.3.1), der systematischen Berücksichtigung von datenschutzfreundlichen Technologien (Ziff. 4.3.2) oder einer stärkeren Sensibilisierung durch die Datenschutzaufsichtsbehörde (Ziff. 4.10.2 lit. d) könnte die Situation verbessert werden. Diese Massnahmen könnten durch Regeln der Guten Praxis oder durch verbindliche Regelungen konkretisiert werden (Ziff. 4.1.2 lit. b).

4.3.4 Weitere Grundsätze

Soweit sie sich bewährt haben, sollten die übrigen datenschutzrechtlichen Grundsätze in den Art. 4 und 5 Abs. 1 und 7 DSG beibehalten werden.

4.4 Rechte der betroffenen Personen

4.4.1 Einleitung

Für die Sicherstellung der Einhaltung des Datenschutzrechts ist neben der Datenschutzaufsicht insbesondere der Individualrechtsschutz zentral. Wie einleitend

---

[52] Zur Aufgabe und Stellung der Datenschutzverantwortlichen vgl. die Erläuterungen des EDÖB; online einsehbar unter <http://www.edoeb.admin.ch/datenschutz/00626/00743/00874/01051/index.html?lang=de>.

dargelegt, sieht ein *Teil der Begleitgruppe* nur einen begrenzten Handlungsspielraum, um den Individualrechtsschutz in datenschutzrechtlichen Angelegenheiten zu stärken (vgl. Ziff. 4.1.2 lit. a sowie ferner Ziff. 4.8.3 und 4.9.5). Allerdings hat die Evaluation des Datenschutzgesetzes ergeben, dass die betroffenen Personen ihre Rechte gegenüber den Datenbearbeitenden – vor allem im privatrechtlichen Bereich – nur selten beanspruchen. Als mögliche Erklärung für dieses Verhalten werden unter anderem die vermutlich eher tiefe Bekanntheit sowie das fehlende Wissen über die Anwendung der Individualrechte angeführt.[53] Die Begleitgruppe schlägt daher vor:

- den Aufbau und die Lesbarkeit des DSG zu verbessern, so dass für die betroffenen Personen klar ersichtlich wird, welche Rechtsansprüche ihnen gegenüber den Datenbearbeitenden zustehen (vgl. nachfolgend Ziff. 4.4.2), und
- die verschiedenen Rechtsansprüche der betroffenen Personen (vgl. nachfolgend Ziff. 4.4.3 ff.) sowie die Verfahren zur Rechtsdurchsetzung (siehe weiter unten Ziff. 4.8.3 lit. b und 4.9.5 lit. c) zumindest punktuell zu stärken, namentlich dort wo im Vergleich zu den Datenschutzreformarbeiten des Europarates noch Lücken bestehen.

4.4.2 Katalog der Rechtsansprüche

Derzeit regelt das DSG die datenschutzrechtlichen Ansprüche der betroffenen Personen in verschiedenen Bestimmungen und in unterschiedlichen Abschnitten des Gesetzes (so findet sich das Berichtigungsrecht etwa in Art. 5 Abs. 2, Art. 15 Abs. 1 und Art. 25 Abs. 3 lit. a DSG). Zum Teil sind die Rechtsansprüche auch als verfahrensrechtliche Behelfe formuliert, die sich nicht immer scharf voneinander abgrenzen lassen, sondern sich teilweise überlagern. Dies erschwert den Betroffenen die Übersicht über die ihnen zustehenden Rechte. Ausserdem geht nach Erachten der Begleitgruppe aus der aktuellen Struktur des DSG zu wenig klar hervor, dass die betroffenen Personen ihre Rechte (auf Auskunft, Widerspruch, Berichtigung, Löschung, Sperrung etc.) zunächst selbstverantwortlich gegenüber den Datenbearbeitenden geltend machen können (und sollen), d.h. dass dazu nicht erst eine Klage vor Gericht erforderlich ist. Die Begleitgruppe schlägt daher vor, ähnlich wie in den Reformvorlagen des Europarates[54] und der EU[55] oder in Art. 25 DSG (Ansprüche und Verfahren bei Datenbearbeitungen durch Bundesorgane) einen Katalog der verschiedenen Rechtsansprüche der betroffenen Personen aufzustellen. Daraus wäre für die betroffenen Personen einfacher erkennbar, welche Rechte sie gegenüber den Datenbearbeitenden geltend machen und – falls erforderlich – vor Gericht einklagen können. Soweit möglich sollen im öffentlichen und privaten Sektor die gleichen Datenschutzrechte zur Verfügung stehen. Dazu gehören insbesondere:

- das Auskunftsrecht (vgl. nachfolgend Ziff. 4.4.3);
- das Recht auf Berichtigung unrichtiger Personendaten (vgl. nachfolgend Ziff. 4.4.4);
- das Recht auf Löschung bzw. Vernichtung widerrechtlich bearbeiteter Personendaten (vgl. nachfolgend Ziff. 4.4.5);
- das Recht auf Sperrung einer widerrechtlichen Datenbearbeitung bzw. Sperrung der

---

[53] Vgl. den Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335, 342 f.

[54] Vgl. Art. 8 des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108.

[55] Vgl. Kapitel III des Entwurfs zur EU-Datenschutz-Grundverordnung und des Entwurfs zur EU-Datenschutzrichtline.

Bekanntgabe von bestimmten Personendaten an Dritte;

- das Recht auf einen Bestreitungsvermerk, wenn weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden kann;
- das Recht auf Widerspruch gegen eine Datenbearbeitung ohne Rechtfertigungsgrund;
- das Recht, keiner auf einer rein automatisierten Bearbeitung von Daten basierenden Entscheidung unterworfen zu werden, welche die Person in massgeblicher Weise betrifft, ohne dass ihrem Standpunkt Rechnung getragen wird (vgl. nachfolgend Ziff. 4.4.6).

Mit einem solchen Katalog der Datenschutzrechte strebt die Begleitgruppe eine bessere Verständlichkeit für die Adressaten des Datenschutzgesetzes an. Am geltenden System der Rechtsdurchsetzung (z.B. hinsichtlich der Aktiv- und Passivlegitimation) soll dagegen materiell grundsätzlich nichts geändert werden. Auch die Geltendmachung von reparatorischen Ansprüchen (Schadenersatz, Genugtuung und Gewinnherausgabe) soll sich weiterhin nach den allgemeinen Voraussetzungen des Haftpflichtrechts (bei privaten Datenbearbeitenden) bzw. des Staatshaftungsrechts (bei datenbearbeitenden Bundesorganen) richten (vgl. zum Ganzen Ziff. 4.8.3 und 4.9.5).

Zur Stärkung der einzelnen datenschutzspezifischen Rechte der betroffenen Personen werden nachfolgend verschiedene Massnahmen vorgeschlagen.

4.4.3 Auskunftsrecht

Die Begleitgruppe schlägt vor, die Bestimmungen zum Auskunftsrecht zu ergänzen, um die Transparenz von Datenbearbeitungen zu verbessern. Gemäss den Anforderungen des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 soll der für die Datenbearbeitung Verantwortliche der betroffenen Person inskünftig auch die Aufbewahrungsdauer der Daten sowie den (logischen) Aufbau bzw. Hintergrund einer Datenbearbeitung, deren Ergebnisse auf die betroffene Person angewandt werden, mitteilen müssen (vgl. Art. 8 lit. c und d des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108).

Personendaten werden immer häufiger je nach Applikationen strukturiert, um ephemere Profile zu erstellen. In solchen Fällen bestehen keine permanenten Datensammlungen, wodurch das Auskunftsrecht unwirksam wird. Die Begleitgruppe ist sich dieser Problematik bewusst. Nach Auffassung eines *Teils der Begleitgruppe* ist dieses Problem nicht mittels des Auskunftsrechts, sondern über die Informationspflicht zu lösen (siehe Ziff. 4.4.3).

Weiter ist zu prüfen, ob die Modalitäten des Auskunftsrechts nach Art. 8 Abs. 5 DSG zu konkretisieren sind. Es könnte beispielsweise festgehalten werden, dass sich der mit der Auskunftserteilung verbundene Aufwand (inkl. Kosten) im Hinblick auf den Zweck des Auskunftsrechts in einem vernünftigen Rahmen halten soll (etwa durch Einsichtnahme vor Ort statt schriftlicher Auskunftserteilung).

In Bezug auf Art. 8 Abs. 6 DSG soll – durch Anpassung der Formulierung oder der Struktur der Bestimmung – klargestellt werden, dass auf die Auskunftserteilung in schriftlicher Form im Voraus verzichtet werden kann, sofern angemessen Einsicht geboten wird.

Ein *Teil der Begleitgruppe* möchte grundsätzlich eine Interessenabwägung für die Ausübung des Auskunftsrechts einführen, wenn die Daten aufgrund einer gesetzlichen Verpflichtung archiviert oder gespeichert werden. Es muss überprüft werden, ob diese Lösung mit dem Modernisierungsentwurf zur Datenschutzkonvention SEV 108 vereinbar ist, was von einigen Mitgliedern der Begleitgruppe bezweifelt wird.

Hinsichtlich der Einschränkungen des Auskunftsrechts vertritt ein *Teil der Begleitgruppe* die Auffassung, dass das in Art. 9 Abs. 4 DSG angeführte Tatbestandsmerkmal der Nichtbe-

kanntgabe der Personendaten an Dritte aufgehoben werden soll, da dieses Kriterium in keiner Weise mit den überwiegenden Interessen des Inhabers einer Datensammlung zusammenhänge. Das Gesetz könnte in diesem Fall um eine Aufzählung von Beispielen, bei welchen ein solches überwiegendes Interesse in Betracht fällt, ergänzt werden. Dabei würde es sich etwa um die Wahrung von geschäftlichen oder industriellen Interessen, um die Verhinderung einer schwerwiegenden Gefährdung der Interessen der Informationsquelle, um die Nichtoffenlegung einer Strategie in einem gerichtlichen Verfahren zwischen dem für die Datenbearbeitung Verantwortlichen und der betroffenen Person oder um schikanöse Auskunftsbegehren handeln. Nach Ansicht eines *anderen Teils der Begleitgruppe* würde die Stellung der betroffenen Person durch eine solche Gesetzesänderung geschwächt. Deshalb schlagen die betreffenden Mitglieder der Begleitgruppe vor, die Bedingung der Nichtbekanntgabe der Personendaten gegenüber Dritten beizubehalten. Einschränkungen des Auskunftsrechts durch das Gesetz oder die Verordnung sollten unter Beachtung von Art. 9 des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 vorgesehen werden.

Schliesslich ist zu überlegen, die Vorschrift von Art. 1 Abs. 7 VDSG, in der es um die Auskunft über Daten von verstorbenen Personen geht, in das Gesetz zu integrieren. Diese Bestimmung hat derzeit keine gesetzliche Grundlage, da die Daten von verstorbenen Personen nicht im DSG geregelt werden.

4.4.4 Recht auf Berichtigung

Der Berichtigungsanspruch der betroffenen Person soll folgendermassen ergänzt werden: Soweit die für die Datenbearbeitung verantwortliche Person ein Begehren um Berichtigung falscher Daten als begründet erachtet, hat sie etwaige, ihr noch bekannte Empfänger der falschen Daten darüber zu informieren, damit die falschen Daten auch dort berichtigt werden können. Dieser Anspruch soll nicht absolut gelten, sondern es können Einschränkungen vorgesehen werden (z.B. wenn die Information unmöglich oder im Verhältnis zur Relevanz des Fehlers zu aufwendig ist).

4.4.5 Recht auf Löschung

Das Recht auf Löschung ist bereits heute im DSG verankert. Soweit kein Rechtfertigungsgrund besteht, können Personen, deren Daten unter Verletzung des DSG bearbeitet werden, vom Datenbearbeitenden und vor Gericht verlangen, dass ihre Daten gelöscht oder beispielsweise von einer Internetseite oder aus einem Computerprogramm entfernt werden (vgl. Art. 15 und 25 DSG). Es geht daher beim vorliegenden Vorschlag mehr darum, dieses Recht auf symbolische Weise ausdrücklich im DSG zu erwähnen, um den betroffenen Personen das Verständnis des Gesetzes zu erleichtern. Dies ändert aber nichts auf materieller Ebene. So wird es beispielsweise weiterhin möglich sein, beim Vorliegen von überwiegenden Interessen – zum Beispiel der Medien oder der historischen Forschung – Daten gegen den Willen der betroffenen Personen zu bearbeiten[56].

Die Begleitgruppe würde es vorziehen, den Begriff «Recht auf Löschung» statt den Begriff «Recht auf Vergessen» zu verwenden – dies in erster Linie, um die Terminologie des Europarates zu übernehmen (vgl. Art. 8 lit. e des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108). Gestärkt werden soll das Recht auf Löschung durch die Einführung von Massnahmen im Zusammenhang mit den Sorgfaltspflichten der für die Datenbearbeitung

[56] Siehe für einen Entscheid in diesem Sinne das Urteil des EGMR Nr. 33846/07 «Wegrzynowski und Smolczewski gegen Polen» vom 16. Juli 2013.

Verantwortlichen (Ziff. 4.3.2) sowie dem Ausbau des Auskunftsrechts (Ziff. 4.4.3). Ausserdem könnten die Modalitäten des Rechts auf Löschung durch Regeln der Guten Praxis bzw. verbindliche Detailregeln konkretisiert werden (vgl. Ziff. 4.1.2 lit. b).

Nach Ansicht *der Begleitgruppe* würde mit diesen Massnahmen das Postulat Schwaab 12.3152 «Recht auf Vergessen im Internet»[57] umgesetzt und das Postulat Recordon 13.3989 «Verletzungen der Persönlichkeitsrechte im Zuge des Fortschritts der Informations- und Kommunikationstechnik» teilweise erfüllt.

4.4.6 Automatisierte Einzelentscheidungen

Aufgrund neuer Informations- und Kommunikationstechniken werden Entscheide, welche für die betroffenen Personen rechtliche Folgen haben oder sie sonst wesentlich beeinträchtigen, zunehmend in automatisierten Verfahren gefällt, oft auch auf der Basis von Profilen, die auf statistischen Angaben und Berechnungen beruhen (Profiling). Insbesondere wenn solche Entscheidverfahren die Bewertung von einzelnen Merkmalen einer Person, wie z.B. der Kreditwürdigkeit[58], der Zuverlässigkeit, des Verhaltens oder von spezifischen Risiken[59] beinhalten, besteht nach der Einschätzung einer *Mehrheit der Begleitgruppe* ein erhöhtes Schutzbedürfnis. Die EU verfügt bereits seit einiger Zeit über Vorschriften zur Zulässigkeit von automatisierten Einzelentscheidungen.[60] Die Umsetzung dieser Vorschriften bereitet in den Mitgliedstaaten – soweit bekannt – keine gewichtigen Probleme.

Die *Mehrheit der Begleitgruppe* schlägt daher vor, jeder Person – in Übereinstimmung mit Art. 8 lit. a des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108[61] – das Recht einzuräumen, keiner auf einer rein automatisierten Bearbeitung von Daten basierenden Entscheidung unterworfen zu werden, die sie in massgeblicher Weise betrifft, ohne dass ihrem Standpunkt vor oder nach der automatisierten Entscheidung Rechnung getragen wird. Damit soll verhindert werden, dass die Bewertung von Persönlichkeitsaspekten ausschliesslich in automatisierter Form erfolgt, ohne dass eine Beurteilung durch Menschen vorgenommen wird und ohne dass die betroffene Person erfährt, wie dieser Entscheid gefällt wird. Der betroffenen Person soll die Möglichkeit eingeräumt werden, ihre Argumente und allfällige im Entscheidprozess unberücksichtigt gebliebene Gesichtspunkte einzubringen, so dass trotz automatisierter Datenbearbeitung das menschliche Element Berücksichtigung findet.

Dabei ist allerdings noch vertieft zu prüfen, welche Vorgänge als automatisierte Einzelentscheidungen im vorangehend erläuterten Sinn zu qualifizieren sind. So sollten etwa

---

[57] Das Postulat Schwaab 12.3152 vom 14. März 2012 wurde vom Nationalrat am 15. Juni 2012 angenommen.

[58] Im Bankensektor wird Profiling beispielsweise im Zusammenhang mit der Gewährung von Darlehen angewendet, um eine Risikoanalyse zukünftiger oder bestehender Kunden durchzuführen (Credit-Scoring).

[59] Vgl. die Botschaft des Bundesrates vom 19. Februar 2003 zur Änderung des Bundesgesetzes über den Datenschutz (DSG), BBl 2003 2101, 2134: Dies wäre etwa dann der Fall, wenn bei einer Privathaftpflichtversicherung eine Lenkerin, die ein wenig sportliches Fahrzeug fährt, automatisch in eine bessere Risikoklasse eingestuft würde als der Lenker eines Sportwagens.

[60] Siehe insbesondere Art. 15 der Richtlinie 95/46/EG sowie Art. 7 des Rahmenbeschlusses 2008/977/JI. Auch der Entwurf zur EU-Datenschutz-Grundverordnung sieht in Art. 20 Regelungen für «auf Profiling basierende Massnahmen» vor; ebenso Art. 9 des Entwurfs zur EU-Datenschutz-Richtlinie.

[61] Art. 8 lit. a des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108: «Toute personne doit pouvoir: (...) ne pas être soumise à une décision l'affectant de manière significative, qui serait prise sur le seul fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte».

Abhebungen am Geldautomaten oder der Versand von Prospekten an eine Reihe durch Computer bestimmte Personen ähnlich wie in der Praxis zum EU-Recht nicht unter die vorgeschlagene Regelung fallen. Ausserdem soll es sich auch beim Recht auf Stellungnahme in automatisierten Entscheidverfahren nicht um ein absolutes Recht handeln, so dass Ausnahmebestimmungen vorgesehen werden können. Im Übrigen soll mit der vorgeschlagenen Regelung weder in die Entscheidungs- bzw. Vertragsfreiheit eingegriffen (kein Kontrahierungszwang) noch eine Begründungspflicht für automatisierte Einzelentscheidungen vorgeschrieben werden.

Eine *Minderheit der Begleitgruppe* möchte den Betroffenen ergänzend das Recht zugestehen, sich dem automatisierten «Predictive Profiling» zu widersetzen, unter Vorbehalt von Ausnahmen, wie sie in Art. 20 des Entwurfs zur EU-Datenschutz-Grundverordnung vorgesehen sind. Profile, die aus solchen Verfahren entstehen, bergen die Gefahr von Beurteilungsfehlern und Diskriminierungen.

Eine *andere Minderheit der Begleitgruppe* lehnt die Einführung solcher Rechte ab.

Zum Auskunftsrecht über den logischen Aufbau einer Datenbearbeitung vgl. vorne Ziff. 4.4.3.

4.4.7 Recht auf Datenübertragbarkeit

Ein *Teil der Begleitgruppe* schlägt vor, im DSG ein Recht auf Datenübertragbarkeit für die betroffenen Personen einzuführen, wie dies im Entwurf zur EU-Datenschutz-Grundverordnung geplant ist (vgl. Art. 18 des Kommissionsentwurfs). Ein *anderer Teil der Begleitgruppe* ist der Auffassung, dass ein solcher Rechtsanspruch eher dem Wettbewerbsrecht oder Medienrecht[62] als dem Datenschutzrecht zuzuordnen ist, und steht dessen Einführung in das DSG ablehnend gegenüber. Es wird daher vorgeschlagen, die Entwicklungen auf europäischer Ebene weiterzuverfolgen und die Frage zu einem späteren Zeitpunkt nochmals zu prüfen, wenn das Recht auf Datenübertragbarkeit im Entwurf zur EU-Datenschutz-Grundverordnung beibehalten wird.

4.5 Grenzüberschreitende Datenbekanntgabe

Die in Art. 6 DSG enthaltenen Vorschriften haben sich im Wesentlichen bewährt. Die Begleitgruppe sieht dennoch einige Änderungen vor.

Gemäss Art. 6 Abs. 2 lit. d DSG können Personendaten trotz Fehlens einer angemessenen Gesetzgebung ins Ausland bekannt gegeben werden, wenn die Bekanntgabe im Einzelfall für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist. Mit dieser Bestimmung ist ein Auslegungsproblem verbunden. Der deutsche Wortlaut weicht von der französischen und italienischen Fassung ab. Während in den letzteren Beiden von «la constatation, l'exercice ou la défense d'un droit en justice» bzw. «accertare, esercitare o far valere un diritto in giustizia» die Rede ist, wird in der deutschen Version von der «Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht» gesprochen.

---

[62] Zur Problematik der Datenübertragbarkeit im Rahmen der Nutzung der sozialen Netzwerke und zum Gesetzgebungsbedarf in diesem Bereich ist auf den Bericht des Bundesrates «Rechtliche Basis für Social Media: Bericht des Bundesrates in Erfüllung des Postulats Amherd 11.3912 vom 29. September 2011», S. 34 ff. und 75, zu verweisen.

Gemäss einem Teil der konsultierten Rechtslehre ist diese Ausnahmebestimmung weit auszulegen, da das Verfahren nicht unbedingt vor einem Gericht durchgeführt werden müsse[63]. Ein *Teil der Begleitgruppe* teilt diese Auffassung und ist der Ansicht, die deutsche Fassung sei an die französische und italienische Version anzupassen. Im Gegensatz dazu ist ein *anderer Teil der Begleitgruppe* der Meinung, dass sich die Ausnahme nur auf Verfahren vor einem Gericht beziehen dürfe, da andernfalls der Datenschutz beim Datenverkehr mit dem Ausland seines Gehalts beraubt würde. Dieser Teil der Begleitgruppe plädiert daher dafür, die französische und italienische Fassung an die deutsche Version anzugleichen.

Sodann schlägt *die Begleitgruppe* vor, den Ausnahmetatbestand des Art. 6 Abs. 2 lit. e DSG auf den Schutz des Lebens oder der körperlichen Integrität von Dritten zu erweitern. Es ist durchaus denkbar, dass Personendaten der betroffenen Person (z.B. eine Adresse, eine Telefonnummer oder medizinische Daten) für die Wahrung solcher Interessen unerlässlich sind, diese aber nicht erreichbar ist.

Mit Bezug auf Art. 6 Abs. 3 DSG könnte sodann vorgesehen werden, dass die Garantien nach Art. 6 Abs. 2 lit. a DSG und die Datenschutzregeln nach Art. 6 Abs. 2 lit. g DSG als angemessener Schutz gelten, wenn die Genehmigung der Datenschutzaufsichtsbehörde dazu vorliegt. Das Einholen der Genehmigung der Aufsichtsbehörde wäre freiwillig. Unternehmen, welche eine solche Genehmigung erhalten möchten, könnten ihre «Binding Corporate Rules» (BCR)[64] vorlegen. Die zu erfüllenden Voraussetzungen und das Verfahren könnten durch Regeln der Guten Praxis bzw. konkretisierende verbindliche Regeln (vgl. Ziff. 4.1.2 lit. b) festgelegt werden.

Im Übrigen soll die deutsche Formulierung des einleitenden Satzes von Art. 6 Abs. 2 DSG an die französische Fassung angepasst werden (nach «wenn» ist der Satzteil «eine der folgenden Bedingungen erfüllt ist» hinzuzufügen).

Schliesslich soll festgelegt werden, dass die Angemessenheit des Datenschutzes im Rahmen der grenzüberschreitenden Datenbekanntgabe nach Art. 6 Abs. 1 DSG nicht den Schutz von Personendaten juristischer Personen voraussetzt (vgl. Ziff. 4.2.1 lit. b).

4.6 Zertifizierungsverfahren

Die Möglichkeit der Zertifizierung gemäss Art. 11 DSG soll beibehalten werden. Allerdings soll die Formulierung der Bestimmung nochmals überprüft werden. Mit Bezug auf die Produktezertifizierung, bei deren praktischen Umsetzung sich Schwierigkeiten gezeigt haben, soll der Auftrag der Datenschutzaufsichtsbehörde, Richtlinien zu erlassen (vgl. Art. 5 Abs. 3 der Verordnung über die Datenschutzzertifizierungen [VDSZ; SR 235.13]), in eine Kann-Vorschrift umgewandelt werden. Damit erhält die Datenschutzaufsichtsbehörde mehr Handlungsspielraum. Ausserdem ist – unter Berücksichtigung der Entwicklungen auf europäischer Ebene – zu prüfen, ob eine Zertifizierung von Dienstleistungen eingeführt werden soll. Die Datenschutzzertifizierung soll grundsätzlich auch weiterhin freiwillig bleiben. Daneben besteht aber die Möglichkeit, spezialgesetzlich eine Zertifizierungspflicht vorzusehen (vgl.

---

[63] MEIER, Protection des données. Fondements, principes généraux et droit privé, Bern 2011, N 1375, wonach es um «toute procédure pendante devant un organe étatique (y compris de juridiction administrative interne) ou reconnu par l'Etat» geht; MAURER-LAMBROU/STEINER, in: Basler Kommentar DSG/BGÖ, 3. Aufl., Basel 2014, N 33 zu Art. 6 DSG, welche «jede Instanz mit Rechtsprechungsfunktion» unter die Bestimmung subsumieren.

[64] In der EU entsprechen die «Binding Corporate Rules» einem Verhaltenskodex, der die interne Politik eines Konzerns im Bereich der Übermittlung personenbezogener Daten in Länder ausserhalb der EU festlegt.

z.B. Art. 59*a* der Verordnung über die Krankenversicherung [KVV; SR 832.102]).

4.7 Register der Datensammlungen

Die Begleitgruppe schlägt vor, auf das Führen eines Registers der Datensammlungen gemäss Art. 11*a* DSG zu verzichten. Denn die Registerführung ist mit einem grossen bürokratischen Aufwand verbunden, der im privaten Sektor nur geringen praktischen Nutzen hat, vor allem da bereits das geltende Gesetz Ausnahmen von der Verpflichtung zur Anmeldung von Datensammlungen vorsieht. Stattdessen regt die Begleitgruppe an, im Rahmen der Sorgfaltspflichten der für die Datenbearbeitung Verantwortlichen eine Pflicht zur angemessenen Dokumentation von Datenbearbeitungsvorgängen vorzusehen (vgl. Ziff. 4.3.2). Das Führen eines Registers könnte für den Bereich der Bundesverwaltung beibehalten werden.

4.8 Besondere Bestimmungen betreffend das Bearbeiten von Personendaten durch private Personen

4.8.1 Regelungskonzeption

Nach der geltenden Konzeption des DSG stellt der privatrechtliche Datenschutz eine Ergänzung und Konkretisierung des Persönlichkeitsschutzes des Zivilgesetzbuches dar. Persönlichkeitsrechte sind unverzichtbar bei der Person ihres Trägers angeknüpft. Es handelt sich um absolute, höchstpersönliche und unveräusserliche Rechte. Das Gesetz legt beispielhaft fest, unter welchen Voraussetzungen eine Datenbearbeitung zu einer Persönlichkeitsverletzung führt, und zeigt auf, in welchen Fällen eine solche Persönlichkeitsverletzung gerechtfertigt sein kann. Dieses System soll beibehalten werden. Insbesondere wird derzeit kein Wechsel zu einem Modell, welches den Schutz personenbezogener Daten durch die Gewährung von Eigentumsrechten (d.h. dinglichen Verfügungs- und Nutzungsrechten an Personendaten[65]) vorsieht, angestrebt. Die Zweckmässigkeit eines solchen Systemwechsels scheint der Begleitgruppe nicht ausgewiesen. Ein absolutes Herrschaftsrecht des Einzelnen an seinen Daten würde stark mit anderen Interessen wie der Meinungs- und Informationsfreiheit kollidieren. Die Begleitgruppe schlägt stattdessen verschiedene andere Massnahmen vor, um den betroffenen Personen bessere Kontrollmöglichkeiten über ihre Daten einzuräumen (vgl. z.B. die Regelungsvorschläge zur Verstärkung der Informationspflicht [Ziff. 4.3.1], zu den Grundsätzen «Privacy by Design» und «Privacy by Default» [Ziff. 4.3.2] sowie zur Aufgabe der Datenschutzaufsichtsbehörde, die Bevölkerung in datenschutzrechtlichen

---

[65] In der rechtswissenschaftlichen Lehre ist in jüngster Zeit im Zusammenhang mit der Forderung nach einer Verbesserung der Datenkontrolle über die Einführung von Herrschaftsrechten bzw. eigentumsähnlichen Rechten an Daten diskutiert worden. Damit könnte dem Einzelnen ein absolutes, uneingeschränktes Verfügungsrecht über seine Daten eingeräumt werden. Als Vorteile eines solchen Systems werden etwa bessere Kontrollmöglichkeiten und die Partizipation des Einzelnen am finanziellen Ertrag der Verwertung seiner Daten genannt. Kritisiert wird dagegen, dass absolute Herrschaftsrechte an Daten zu einer Monopolisierung von Wissen bzw. Informationen führen könnten. Ausserdem wird geltend gemacht, dass auch in diesem System nicht von egalitären Vertragspartnern im «Datenhandel» ausgegangen werden kann. Vgl. zum Ganzen z.B. FLÜCKIGER, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, AJP 2013, S. 837–864 sowie SCHUNCK, Propertisierung von Personendaten?, digma 2013, S. 66–72. Zu beachten ist in diesem Zusammenhang sodann die parlamentarische Initiative Derder 14.434 «Schutz der digitalen Identität von Bürgerinnen und Bürgern», welche unter anderem in Art. 13 Abs. 2 BV vorsehen will, dass «Daten (...) Eigentum der betreffenden Person» sind. Die Initiative ist im Parlament noch nicht behandelt worden.

Angelegenheiten zu sensibilisieren [Ziff. 4.10.2 lit. d]).

4.8.2 Persönlichkeitsverletzungen und Rechtfertigungsgründe

An den Bestimmungen von Art. 12 und 13 DSG, welche die Voraussetzungen festlegen, unter denen das Bearbeiten von Personendaten durch Private rechtmässig ist, soll im Grundsatz festgehalten werden. Die Begleitgruppe schlägt jedoch folgende Änderungen vor:

Beweislastverteilung: Nach den allgemein geltenden Regeln der Beweislastverteilung (Art. 8 ZGB) muss heute prinzipiell die betroffene Person den Nachweis einer Persönlichkeitsverletzung erbringen, während die Datenbearbeitenden die Beweislast für das Vorliegen eines hinreichenden Rechtfertigungsgrundes tragen. Dem Umstand, dass es der betroffenen Person angesichts der mit den technologischen Entwicklungen gestiegenen Komplexität der Datenbearbeitungsmethoden regelmässig nicht leicht fallen dürfte, eine Persönlichkeitsverletzung nachzuweisen, möchte eine *Mehrheit der Begleitgruppe* inskünftig mit einer Beweislasterleichterung Rechnung tragen. Dazu schlägt sie eine Beweislastumkehr nach dem Beispiel des Art. 13*a* Abs. 1 UWG[66] vor, wonach das Gericht von den Datenbearbeitenden im Einzelfall den Nachweis einer datenschutzkonformen Bearbeitung verlangen kann, wenn dies unter Berücksichtigung der berechtigten Interessen der am Verfahren beteiligten Parteien angemessen erscheint (zur gesetzlichen Vermutung der Rechtmässigkeit einer Datenbearbeitung bei Einhaltung der Regeln der Guten Praxis vgl. oben Ziff. 4.1.2 lit. b). Dies könnte beispielsweise dann der Fall sein, wenn die Beweisführung für die betroffene Person besonders schwierig ist, weil Tatsachen nachzuweisen sind, die im Einflussbereich der Datenbearbeitenden liegen (z.B. im Zusammenhang mit der Einhaltung von datenschutzrechtlichen Sorgfaltspflichten gemäss Ziff. 4.3.2). Eine *Minderheit der Begleitgruppe* erachtet eine solche Regelung dagegen nicht als notwendig, da die Beweisführung in der Praxis kein zentrales Problem darstelle. Soweit Beweisprobleme über Tatsachen bestehen, die sich im Machtbereich der Datenbearbeitenden abspielen, werde dies von den Zivilgerichten im Rahmen der Mitwirkungsobliegenheit und Beweiswürdigung berücksichtigt.

Persönlichkeitsverletzung*:* Gemäss einem *Teil der Begleitgruppe* sollte in Art. 12 Abs. 2 lit. a DSG, wonach ein Verstoss gegen die allgemeinen Datenbearbeitungsgrundsätze immer als Persönlichkeitsverletzung zu qualifizieren ist, die Möglichkeit, Rechtfertigungsgründe zuzulassen, wieder ausdrücklich aufgenommen werden. Der Vorbehalt von Rechtfertigungsgründen ist in Art. 12 Abs. 2 lit. a DSG – anders als bei den Bestimmungen von Art. 12 Abs. 2 lit. b und c DSG – im Zuge der Gesetzesrevision vom 24. März 2006[67] gestrichen worden. Zur Begründung dieses Änderungsvorschlages ist (z.B. in den Erläuterungen zu einem allfälligen Gesetzesentwurf) darauf hinzuweisen, dass die herrschende Lehre und das Bundesgericht davon ausgehen, dass eine Rechtfertigung der Bearbeitung von Personendaten entgegen den allgemeinen Bearbeitungsgrundsätze nicht generell ausgeschlossen ist, dass Rechtfertigungsgründe im konkreten Fall allerdings nur mit grosser Zurückhaltung bejaht werden können. *Andere Mitglieder der Begleitgruppe* möchten dagegen an der aktuellen Formulierung festhalten. Eine Änderung von Art. 12 Abs. 2 lit. a DSG erachten sie nicht als erforderlich, da das Bundesgericht auch beim geltenden Wortlaut in gewissen Fällen Rechtfertigungsgründe zulasse.

---

[66] Art. 13*a* Abs. 1 UWG: «Der Richter kann vom Werbenden den Beweis für die Richtigkeit von in der Werbung enthaltenen Tatsachenbehauptungen verlangen, wenn dies unter Berücksichtigung der berechtigten Interessen des Werbenden und anderer am Verfahren beteiligter Personen im Einzelfall angemessen erscheint.»

[67] Vgl. AS 2007 4983, 4987.

Rechtfertigungsgründe: Schliesslich schlägt die Begleitgrupppe vor, die beispielhafte Aufzählung von Konstellationen, bei welchen eine Datenbearbeitung durch überwiegende private Interessen gerechtfertigt sein kann, in Art. 13 Abs. 2 DSG um folgende Rechtfertigungsgründe zu ergänzen:

- Bearbeitung von Daten juristischer Personen im Rahmen ihrer Geschäftstätigkeit (z.B. wenn eine Person Daten über ihre Anbieter und Lieferanten bearbeitet oder es um die Vertragsabwicklung mit diesen geht; vgl. Ziff. 4.2.1 lit. b). Ein *Teil der Begleitgruppe* empfiehlt, diesen Rechtfertigungsgrund auch auf Unternehmen auszudehnen, welche nicht als juristische Personen konstituiert sind (z.B. einfache Gesellschaften oder Erbengemeinschaften). Es ist noch zu prüfen, welche rechtlichen Konsequenzen eine solche Erweiterung hätte.
- Bearbeitung von Personendaten für die Zwecke von (in- und ausländischen) Gerichts- und Behördenverfahren (analog Art. 6 Abs. 2 lit. d DSG: wenn die Datenbearbeitung für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen unerlässlich ist). Allerdings ist in der Begleitgruppe *umstritten*, ob auch Behördenverfahren erfasst werden sollen; vgl. Ziff. 4.5.
- Mit Bezug auf den Rechtfertigungsgrund des Vertragsabschlusses gemäss Art. 13 Abs. 2 lit. a DSG ist nach einem *Teil der Begleitgruppe* zu prüfen, ob inskünftig zwar ein Zusammenhang zwischen der Datenbearbeitung und dem Abschluss oder der Abwicklung eines Vertrags vorausgesetzt, die Anforderungen aber nicht mehr so streng ausgestaltet werden sollen wie gegenwärtig. Ausserdem könnte dieser Rechtfertigungsgrund auch auf Konstellationen ausgedehnt werden, in welchen ein Vertrag zwar formal nicht mit der betroffenen Person abgeschlossen wurde, dieser aber (z.B. aufgrund eines Arbeitsverhältnisses) zu Gute kommt.[68] Im Rahmen der Arbeiten der Begleitgruppe ist die Frage nach solchen Erweiterungen von Art. 13 Abs. 2 lit. a DSG[69] noch offen gelassen worden.[70]
- Ein *Teil der Begleitgruppe* möchte ausserdem die Bearbeitung von Personendaten zu Archivierungs- und Sicherungszwecken als Rechtfertigungsgrund einführen.

4.8.3 Rechtsansprüche und Verfahren

a) Rechtsansprüche

Wie in Ziff. 4.4.1 und 4.4.2 dargelegt, sollen Struktur und Übersichtlichkeit des DSG

---

[68] Im Zusammenhang mit der Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen hält beispielsweise das deutsche Bundesdatenschutzgesetz (BDSG) in § 4*c* Abs. 1 Ziff. 3 fest: «Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4*b* Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll».

[69] Bei einer allfälligen Anpassung von Art. 13 Abs. 2 lit. a DSG wäre aus Kohärenzgründen auch Art. 6 Abs. 2 lit. c DSG anzugleichen.

[70] Zur Rechtslage in der EU vgl. Art. 6 Ziff. 1 lit. b des Entwurfs zur Datenschutz-Grundverordnung: «Die Verarbeitung personenbezogener Daten ist nur rechtmässig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: (...) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich oder zur Durchführung vorvertraglicher Massnahmen, die auf Antrag der betroffenen Person erfolgen» (ähnlich Art. 7 lit. b der Richtlinie 95/46/EG).

angepasst werden, um für die betroffenen Personen besser ersichtlich zu machen, über welche datenschutzspezifischen Rechtsansprüche sie verfügen. Dabei soll auch klarer zum Ausdruck kommen, dass die betroffenen Personen ihre Rechte zunächst selbstverantwortlich gegenüber den privaten Datenbearbeitenden geltend machen können, ohne ein Gerichtsverfahren einleiten zu müssen. Zu diesem Zweck soll insbesondere ein Katalog der verschiedenen Rechte der betroffenen Personen aufgestellt werden, welcher beispielsweise das Auskunfts-, Widerspruchs-, Berichtigungs- oder Löschungsrecht beinhaltet.

Am geltenden System der Rechtsdurchsetzung (z.B. hinsichtlich der Aktiv- und Passivlegitimation sowie der Rechtsbehelfe) soll nach einer *Mehrheit der Begleitgruppe* dagegen materiell grundsätzlich nichts geändert werden. Auch die Geltendmachung von Schadenersatz- und Genugtuungsansprüchen soll sich weiterhin nach den allgemeinen Voraussetzungen des Haftpflichtrechts richten. Für den Anspruch auf Gewinnherausgabe sollen ebenfalls unverändert die Bestimmungen des OR über die Geschäftsführung ohne Auftrag[71] Anwendung finden (vgl. Art. 15 Abs. 1 DSG i.V.m. Art. 28*a* Abs. 3 ZGB und Art. 41 ff., Art. 49 sowie Art. 423 des Obligationenrechts [OR; SR 220]*). Einige Mitglieder der Begleitgruppe* schlagen hingegen vor, die Verbindung mit den Bestimmungen des ZGB und des OR aufzuheben und die dort stipulierten Ansprüche im DSG selbstständig zu regeln.

Was die reparatorischen Ansprüche betrifft, ist die Begleitgruppe geteilter Meinung, ob eine Kausalhaftung eingeführt werden soll. *Einige Mitglieder der Begleitgruppe* vertreten die Auffassung, im Bereich des Datenschutzes gebe es zu wenige Fälle von finanziellen oder immateriellen Schäden, um die Einführung einer solchen Haftung zu rechtfertigen. Ein *anderer Teil der Begleitgruppe* macht dagegen geltend, dass ausgehend von der geringen Zahl der Gerichtsverfahren keine Schlussfolgerungen in Bezug auf die Bedeutung und Häufigkeit der Fälle gezogen werden können, in denen eine Entschädigung gerechtfertigt wäre. Diese Mitglieder der Begleitgruppe sind der Ansicht, dass den betroffenen Personen mit der Einführung einer Kausalhaftung die Durchsetzung ihrer Rechte erleichtert werden könnte. *Einige Mitglieder der Begleitgruppe* plädieren sogar dafür, eine pauschale Entschädigung analog der arbeitsrechtlichen Entschädigung bei missbräuchlicher Kündigung nach Art. 336*a* OR zu schaffen.

b) Verfahrensbestimmungen

Die Ergebnisse der Evaluation des DSG haben gezeigt, dass die im DSG verankerten Durchsetzungsrechte gegenüber privaten Datenbearbeitenden nur selten beansprucht werden. Als mögliche Erklärung werden im Evaluationsbericht des Bundesrates einerseits die vermutlich eher geringe Bekanntheit dieser Rechtsansprüche sowie das geringe Wissen über deren Anwendung genannt (vgl. Ziff. 4.4.1). Andererseits dürfte das Kosten- und Prozessrisiko von den betroffenen Personen oftmals als zu hoch empfunden werden, insbesondere da der Nutzen eines gerichtlichen Vorgehens als diffus und nicht gesichert eingestuft wird.[72] Im Rahmen der Arbeiten der Begleitgruppe wurden daher verschiedene Modelle geprüft, um die individuelle Durchsetzung von Ansprüchen nach DSG zu erleichtern, so etwa die Stärkung der verfahrensmässigen Stellung der betroffenen Personen bei der Wahrnehmung ihres Widerspruchrechts, die Einführung des Untersuchungsgrundsatzes bzw. die Anwendbarkeit des vereinfachten Verfahrens i.S.v. Art. 243 ff. der

[71] Im Verlauf der weiteren Revisionsarbeiten zum DSG ist vertieft zu prüfen, ob es sich beim Verweis auf Art. 423 OR um einen Rechtsfolge- oder einen Rechtsgrundverweis handelt.

[72] Vgl. den Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335, 342 f.

Zivilprozessordnung (ZPO; SR 272) auf alle datenschutzrechtlichen Klagen[73], Kostenerleichterungen sowie der Ausbau der kollektiven Rechtsdurchsetzung durch datenschutzspezifische Verbandsklagen, Gruppenklagen oder Muster- und Testverfahren.

Ein *Teil der Begleitgruppe* schätzt die Wirkungen der geprüften Instrumente für den Bereich des Datenschutzes eher als gering ein, so dass damit die Durchsetzungsrechte der Betroffenen nur begrenzt gefördert werden könnten. Ausserdem werden diese Instrumente auch insofern als problematisch erachtet, als sie zu einer Entkoppelung des DSG vom allgemeinen Persönlichkeitsschutz nach Art. 28 ZGB führen könnten, mit der Folge, dass im schweizerischen Recht zwei unterschiedliche Systeme zur zivilrechtlichen Durchsetzung des Persönlichkeitsschutzes geschaffen würden. Dieser Teil der Begleitgruppe ist daher der Ansicht, dass für die Sicherstellung der Einhaltung der datenschutzrechtlichen Vorschriften durch private Datenbearbeitende hauptsächlich die Datenschutzaufsicht zu stärken sei und die Kompetenzen der Datenschutzaufsichtsbehörde entsprechend ausgebaut werden sollten (Ziff. 4.10.2).

Ein *anderer Teil der Begleitgruppe* vertritt hingegen die Auffassung, dass auch Massnahmen vorgeschlagen werden sollten, um die Stellung der betroffenen Personen bedeutend zu stärken. Aus dem Evaluationsbericht des Bundesrates gehe klar hervor, dass der Schutz der Individualrechte ein bekanntes Problem sei. Ausserdem sei es im aktuellen Umfeld der von den eidgenössischen Räten auferlegten Budgetkürzungen heikel, nur einen Ausbau der Befugnisse der Aufsichtsbehörde vorzuschlagen, welcher beträchtliche Ressourcen erfordere.

Um den Individualrechtsschutz immerhin punktuell zu vereinfachen und für die betroffenen Personen zugänglicher auszugestalten, werden folgende Massnahmen vorgeschlagen:

Kostenerleichterungen im Schlichtungs- und Entscheidverfahren sowie im Rechtsmittelverfahren: Die Meinungen in der Begleitgruppe zur Einführung von Kostenerleichterungen im Zivilverfahren sind geteilt. Verschiedentlich wird geltend gemacht, dass weniger die Gerichtskosten als vielmehr der Gerichtskostenvorschuss und potentielle Parteientschädigungen die Parteien von der Nutzung des Rechtswegs abhalten. Ein *Teil der Begleitgruppe* schlägt vor, für datenschutzrechtliche Streitigkeiten nach dem Vorbild von Art. 65 Abs. 4 und 5 des Bundesgerichtsgesetzes (BGG; SR 173.110) einen erheblich reduzierten Gerichtskosten-Rahmen festzulegen.[74] Zusätzlich soll abgeklärt werden, welche Massnahmen bezüglich der Regelung des Kostenvorschusses getroffen werden können, um den gerichtlichen Zugang zu erleichtern. Ein *anderer Teil der Begleitgruppe* spricht sich gegen besondere Kostenregelungen für den Bereich des Datenschutzrechts aus. Für den Fall, dass dennoch Kostenerleichterungen vorgesehen werden, wird vorgeschlagen, diese aus Gründen der Einheit der Rechtsordnung nicht nur für Ansprüche gestützt auf das DSG,

---

[73] De lege lata findet das vereinfachte Verfahren – soweit keine vermögensrechtliche Streitigkeit mit einem Streitwert von unter CHF 30'000.-- vorliegt (Art. 243 Abs. 1 ZPO) – nur auf Streitigkeiten zur Durchsetzung des Auskunftsrechts nach Art. 8 DSG Anwendung (Art. 15 Abs. 4 DSG i.V.m. Art. 243 Abs. 2 lit. d ZPO). Im Übrigen gilt für datenschutzrechtliche Streitigkeiten das ordentliche Verfahren nach Art. 219 ff. ZPO.

[74] Art. 65 Abs. 4 und 5 BGG lauten: «Sie [die Gerichtsgebühr] beträgt 200–1'000 Franken und wird nicht nach dem Streitwert bemessen in Streitigkeiten: a. über Sozialversicherungsleistungen; b. über Diskriminierungen auf Grund des Geschlechts; c. aus einem Arbeitsverhältnis mit einem Streitwert bis zu 30'000 Franken; d. nach den Artikeln 7 und 8 des Behindertengleichstellungsgesetzes vom 13. Dezember 2002.» (Abs. 4). «Wenn besondere Gründe es rechtfertigen, kann das Bundesgericht bei der Bestimmung der Gerichtsgebühr über die Höchstbeträge hinausgehen, jedoch höchstens bis zum doppelten Betrag in den Fällen von Absatz 3 und bis zu 10'000 Franken in den Fällen von Absatz 4.» (Abs. 5).

sondern auch für Ansprüche gestützt auf Art. 28 ff. ZGB und die Bestimmungen des UWG vorzusehen, wobei nur Konsumenten davon profitieren können sollen. Allerdings sind *verschiedene Mitglieder der Begleitgruppe* der Ansicht, dass nicht nur natürliche Personen, sondern auch Unternehmen von allfälligen Kostenerleichterungen in Datenschutzverfahren profitieren können sollen.

Stellungnahmen durch die Datenschutzaufsichtsbehörde: Aufgrund der besonderen Technizität der Materie können sich in datenschutzrechtlichen Streitigkeiten Schwierigkeiten bei der rechtlichen Beurteilung eines Falles ergeben. Da mit der Datenschutzaufsichtsbehörde eine spezialisierte Behörde zur Verfügung steht, sollen bei dieser in zivilrechtlichen Verfahren Stellungnahmen eingeholt werden können. Die Begleitgruppe schlägt dazu folgendes Vorgehen vor: Steht in einem Zivilprozess die Zulässigkeit einer Datenbearbeitung in Frage, kann das Gericht von Amtes wegen oder auf Antrag einer Partei die Sache der Datenschutzaufsichtsbehörde zur Stellungnahme vorlegen. Die Aufsichtsbehörde ist nicht zur Abgabe einer Stellungnahme verpflichtet. Nimmt die Aufsichtsbehörde Stellung, ist das Gericht nicht daran gebunden und verliert somit seine Entscheidungskompetenz nicht (Grundsatz der richterlichen Unabhängigkeit).

Kollektiver Rechtsschutz: Das DSG enthält keine besonderen Vorschriften zum kollektiven Rechtsschutz der betroffenen Personen. Somit gelangen die allgemeinen Bestimmungen des Zivilprozessrechts zur Anwendung.

Im Jahr 2013 hat der Bundesrat einen Bericht zum kollektiven Rechtsschutz in der Schweiz vorgelegt[75]. Darin hält er fest, dass im schweizerischen Zivilprozessrecht bereits einige Instrumente der kollektiven Rechtsdurchsetzung existieren, wie beispielsweise die subjektive und objektive Klagenhäufung (Art. 71 und 90 ZPO), die Prozessvereinigung, -sistierung und -überweisung (Art. 125 lit. c, Art. 126 und Art. 127 ZPO) oder die Verbandsklage (Art. 89 ZPO). Nach Auffassung des Bundesrates sind diese Instrumente jedoch nicht immer geeignet, wenn es um den Ersatz von Massen- und Streuschäden geht. Deshalb schlägt er mehrere Massnahmen vor, um die Situation zu verbessern. Dazu gehört die Erweiterung des Anwendungsbereichs der Verbandsklage auf sämtliche Rechtsbereiche und allenfalls sogar auf die Geltendmachung reparatorischer Ansprüche. Daneben erachtet der Bundesrat auch die Einführung von eigentlichen Instrumenten der kollektiven Rechtsdurchsetzung als denkbar. Diesbezüglich erwähnt er die Schaffung von gesetzlichen Grundlagen für Muster- oder Testklagen[76] zur Durchsetzung von Massenschäden in der Schweiz oder die Einführung einer

[75] Bericht des Bundesrates «Kollektiver Rechtsschutz in der Schweiz – Bestandesaufnahme und Handlungsmöglichkeiten» vom 3. Juli 2013.

[76] Bei einer Muster- oder Testklage kommt es zu einer kollektiven Interessenwahrung, indem zunächst ein einziges typisches «Musterverfahren» zwischen zwei Parteien über eine bestimmte Streitfrage durchgeführt wird. Dem zwischen diesen beiden Parteien ergehenden Entscheid bezüglich bestimmter Tat- und/oder Rechtsfragen kommt eine Wirkung als prozessuales Exempel für bestimmte nachfolgende Prozesse zwischen weiteren Parteien zu, sodass in diesen Verfahren nicht mehr über die identische Streitfrage prozessiert werden muss. Es handelt sich stets um eine Individualklage des Musterklägers, deren Ziel die Herbeiführung einer externen Wirkung der im Musterverfahren entschiedenen Tat- bzw. Rechtsfragen auf eine Vielzahl von Fällen ist. Voraussetzung dieser externen Rechtskraftwirkung ist entweder eine entsprechende gesetzliche Grundlage oder – falls (wie in der Schweiz) keine solche gesetzliche Grundlage besteht – eine entsprechende Vereinbarung zwischen den Parteien (Bericht des Bundesrates vom 3. Juli 2013, S. 28).

Gruppenklage[77]. Dabei würden zwei Formen der Gruppenklage in Frage kommen:

- einerseits die Einführung einer Gruppenklage auf der Basis eines opt in-Modells (im schweizerischen Recht bestehen bereits Rechtsinstrumente, die der Gruppenklage sehr ähnlich sind)[78];
- andererseits die Schaffung eines besonderen Gruppenvergleichsverfahrens nach dem Vorbild der niederländischen Regelung (gerichtlich für verbindlich erklärter Vergleich für alle Geschädigten).

Hingegen ist es nie um die Übernahme der US-amerikanischen «class action» gegangen, vor allem aufgrund des damit verbundenen Missbrauchspotentials, welches teilweise auf die geltenden materiell- und prozessrechtlichen Rahmenbedingungen in den USA zurückzuführen ist[79].

Im Anschluss an den vorangehend dargestellten Bericht des Bundesrates hat Nationalrätin Birrer-Heimo eine Motion[80] eingereicht, die den Bundesrat mit der Ausarbeitung der notwendigen Gesetzesänderungen beauftragt, um es einer grossen Anzahl gleichartig Geschädigter zu erleichtern, ihre Ansprüche gemeinsam vor Gericht geltend zu machen. In seiner Antwort hat der Bundesrat festgehalten, dass er es nicht als opportun erachte, einen eigenständigen Erlass zum kollektiven Rechtsschutz («Sammelklagengesetz») zu erarbeiten. Hingegen hat er sich bereit erklärt, punktuelle Gesetzesänderungen vorzuschlagen, die in die Richtung seines Berichts zum kollektiven Rechtsschutz gehen, oder die im Bericht enthaltenen Aspekte im Rahmen laufender Gesetzgebungsprojekte zu berücksichtigen, zum Beispiel bei der Revision des Aktienrechts und oder bei den Arbeiten an einem Finanzdienstleistungsgesetz. Die Motion ist am 12. Juni 2014 angenommen worden.

Es stellt sich die Frage, ob auch im DSG Instrumente für den kollektiven Rechtsschutz eingeführt werden sollen, wie dies etwa mit der Motion Schwaab 13.3052 «Recht zur Sammelklage bei Datenschutzverletzungen, insbesondere im Internet»[81] verlangt wird.

---

[77] Unter Gruppenklagen sind repräsentative Klagen zu verstehen, bei denen es zu einer Bündelung von Individualansprüchen kommt, indem ein Gruppenkläger eine Klage für weitere Personen führt. Letztere sind selbst formell nicht am Verfahren beteiligt, haben aber dennoch am Ergebnis teil, da über ihre Ansprüche ebenfalls mit Rechtskraft entschieden wird. Die bekannteste Form der Gruppenklage ist die Sammelklage US-amerikanischer Prägung («class action»). Je nach Funktionsweise, wie neben dem Gruppenkläger weitere Personen am Verfahrensergebnis teilhaben können, wird zwischen opt in-Gruppenklagen und opt out-Gruppenklagen unterschieden. Beide Modelle setzen eine Benachrichtigung von Gruppenmitgliedern voraus, wobei dieser in den beiden Modellen ganz unterschiedliche Bedeutung zukommt. Neben selbst betroffenen Einzelpersonen kommen als Gruppenkläger auch (ideelle) Vereine oder auch Behörden in Betracht. An Gruppenkläger werden grundsätzlich besondere Anforderungen gestellt, weil sie über ihre eigenen Interessen hinaus auch als Repräsentanten mit Wirkung für sämtliche Gruppenmitglieder handeln (Bericht des Bundesrates vom 3. Juli 2013, S. 32).

[78] Ausgleichs- bzw. Überprüfungsklage nach Art. 105 Fusionsgesetz (FusG; SR 221.301); Vertretung der Anlegergemeinschaft nach Art. 86 Kollektivanlagengesetz (KAG; SR 951.31); Sonderregelung zur Erledigung von Ansprüchen wegen Haftung für nukleare Schäden (vgl. Art. 20 ff. des Kernenergiehaftpflichtgesetzes vom 13. Juni 2008 [nKHG; BBl 2008 5339, 5341; noch nicht in Kraft getreten]); siehe dazu den Bericht des Bundesrates vom 3. Juli 2013, S. 33 ff.

[79] Zu diesen Fragen siehe den Bericht des Bundesrates vom 3. Juli 2013, S. 32 ff.

[80] Motion Birrer-Heimo 13.3931 vom 27. September 2013 «Förderung und Ausbau der Instrumente der kollektiven Rechtsdurchsetzung».

[81] Die Motion Schwaab 13.3052 vom 7. März 2013 wurde im Nationalrat noch nicht behandelt.

Nach der *Mehrheit der Begleitgruppe* sollte vor allem aus zwei Gründen auf die Einführung solcher besonderer Massnahmen im DSG verzichtet werden. Erstens ermögliche Art. 89 ZPO bereits heute gewissen Organisationen, im Fall einer Verletzung der Persönlichkeit der Angehörigen bestimmter Personengruppen Abwehrklagen einzureichen und dem Gericht zu beantragen, die Verletzung zu verbieten oder zu beseitigen, ihre Widerrechtlichkeit festzustellen, eine Berichtigung oder das Urteil zu veröffentlichen sowie das Gegendarstellungsrecht geltend zu machen. Zweitens seien Fälle von Massen- und Streuschäden finanzieller oder immaterieller Art im Datenschutzrecht eher selten, weshalb es nicht angebracht erscheine, dafür besondere Instrumente zu schaffen. Die Mehrheit der Begleitgruppe erachtet stattdessen den Ausbau der Kompetenzen und Befugnisse der Datenschutzaufsichtsbehörde als geeigneteres Mittel, um die Durchsetzung des Gesetzes sicherzustellen (vgl. Ziff. 4.10.2).

Demgegenüber ist eine *Minderheit der Begleitgruppe* der Ansicht, dass die Instrumente für den kollektiven Rechtsschutz ausgebaut werden sollten. Sie schlägt vor, die Möglichkeit zu prüfen, Art. 89 ZPO auf jene Fälle auszudehnen, in denen nur ein oder wenige Angehörige einer Personengruppe in ihrer Persönlichkeit verletzt werden (insbesondere wenn sich die Streitigkeit wiederholen und/oder eine grosse Personenzahl betreffen könnte). Die einzelnen Personen könnten so vom Prozessrisiko entlastet werden und ihre Sache einer Organisation übertragen, welche über die erforderlichen technischen und rechtlichen Mittel verfügt. Ausserdem soll Art. 89 ZPO auf reparatorische Klagen ausgedehnt werden. Kumulativ dazu wünscht dieser Teil der Begleitgruppe, dass sowohl für negatorische als auch für reparatorische Klagen eine Gruppenklage auf der Basis eines opt in-Modells oder ein spezielles Gruppenvergleichsverfahren gemäss niederländischem Modell eingeführt wird.

c) Alternative Streitbeilegungsmechanismen

Neben den vorangehend dargestellten Massnahmen hat die Begleitgruppe schliesslich auch spezifisch auf datenschutzrechtliche Streitigkeiten ausgerichtete alternative Streiterledigungsmechanismen (insbesondere Mediation, Ombudsstelle) untersucht[82]. Solche Verfahren könnten dazu beitragen, datenschutzrechtliche Auseinandersetzungen in einem möglichst frühen Stadium gütlich zu regeln und den Parteien damit Kosten und andere Belastungen zu ersparen. Indem pragmatisch und lösungsorientiert eine Einigung zu erreichen versucht wird, könnten die Betroffenen ihre Rechte wahren, ohne ein förmliches Verfahren anstrengen zu müssen. Ein niederschwelliges Vermittlungsverfahren könnte auch den Bedürfnissen von Minderjährigen besonders Rechnung tragen. Mit einem Schlichtungsverfahren könnte zudem eine wesentliche Entlastung der im Datenschutzrecht mit Aufsicht und Rechtspflege betrauten Behörden (Datenschutzaufsichtsbehörde, Zivilgerichte und Verwaltungsrechtspflege) verbunden sein.

Bei Inkrafttreten des DSG war es die Absicht des Gesetzgebers, dass der EDÖB die Rolle eines Ombudsmanns bzw. Vermittlungsaufgaben bei Differenzen zwischen privaten Parteien und datenbearbeitenden Bundesorganen übernehmen soll.[83] Mit Blick auf die der Datenschutzaufsichtsstelle inskünftig allenfalls einzuräumenden Verfügungs- und Sanktionskom-

[82] Siehe auch Art. 10 des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108: «Chaque Partie s'engage à établir des sanctions et recours juridictionnels et non-juridictionnels appropriés visant les violations du droit interne donnant effet aux dispositions de la présente Convention.»

[83] Vgl. dazu die Botschaft des Bundesrates vom 23. März 1988 zum Bundesgesetz über den Datenschutz (DSG), BBl 1988 II 413, 481.

petenzen (vgl. nachfolgend Ziff. 4.10.2) wurden im Rahmen der Begleitgruppe jedoch Bedenken geäussert, dass eine Kombination von Mediationstätigkeit und Verfügungsgewalt bei der gleichen Stelle zu Zielkonflikten führen könnte. Allerdings könnte die Datenschutzaufsichtsbehörde im Rahmen ihrer Aufgaben jeweils soweit möglich auf eine Vermittlung zwischen den Parteien hinwirken, ohne dass es sich dabei um eine Mediation im klassischen Sinn handeln würde.

Um daneben ein alternatives Konfliktlösungsverfahren zu schaffen, hat die Begleitgruppe folgenden Vorschlag erarbeitet: Den verschiedenen Wirtschaftszweigen soll die Möglichkeit eingeräumt werden, im Rahmen der Selbstregulierung (vgl. Ziff. 4.1.2 lit. b) eine Stelle zu schaffen bzw. zu bezeichnen, welche in datenschutzrechtlichen Streitigkeiten Schlichtungs- bzw. Mediationsverfahren durchführt. Soweit diese Aufgabe bestehenden Ombudsstellen übertragen wird, müssten diese ihr Personal im Bereich des Datenschutzes weiterbilden. Für den Fall, dass eine Branchenlösung fehlt, soll – ähnlich wie in der Radio- und Fernsehgesetzgebung[84] – die Datenschutzaufsichtsbehörde eine Mediations- bzw. Ombudsstelle bestimmen können. Das Vermittlungsverfahren soll fakultativ sein.

Die Begleitgruppe hat sodann den Vorschlag, die kantonalen Datenschutzbehörden als Ombudsstellen einzusetzen, geprüft, aber abgelehnt. Verschiedene Mitglieder der Begleitgruppe sind der Ansicht, dass eine solche Lösung zu einer Kompetenzvermischung zwischen Bund und Kantonen führen würde. Sie bezweifeln, dass die Kantone mit einer Änderung der geltenden Kompetenzordnung einverstanden wären. Zudem haben auch die Kantone Ressourcenprobleme im Bereich der Datenschutzaufsicht.

4.9 Besondere Bestimmungen betreffend das Bearbeiten von Personendaten durch Bundesorgane

4.9.1 Regelungskonzeption

Das für die Bearbeitung von Personendaten durch Bundesorgane relevante Datenschutzrecht ergibt sich neben der allgemeinen Datenschutzgesetzgebung (DSG und VDSG) insbesondere aus den bereichsspezifischen Datenschutzvorschriften des öffentlichen Rechts. Dieses System soll beibehalten werden. Zwar wurde im Rahmen der vorliegenden Arbeiten geprüft, ob die datenschutzrechtlichen Bestimmungen in den Spezialgesetzen in einem einzigen Gesetz gebündelt werden sollen, welches alsdann die Rechtsgrundlagen für die Datenbearbeitung in den verschiedenen staatlichen Tätigkeitsgebieten enthielte. Die Begleitgruppe ist jedoch zum Schluss gekommen, dass eine solche Massnahme aus legistischen Gesichtspunkten nicht erforderlich ist. Im Übrigen kann mit einer fachspezifischen Datenschutzgesetzgebung den unterschiedlichen Zielsetzungen in den Spezialgesetzen besser Rechnung getragen werden (vgl. vorangehend Ziff. 4.1.1).

Auch bezüglich des sachlichen Geltungsbereichs der öffentlich-rechtlichen Datenschutzvorschriften sowie der Ausnahmebestimmung für privatrechtliche Tätigkeiten von Bundesorganen (Art. 23 DSG) besteht kein Handlungsbedarf.

4.9.2 Zulässigkeit der Datenbearbeitung (insbesondere genügende Rechtsgrundlage)

An den Anforderungen, welche Art. 17 DSG an die Rechtsgrundlage für eine Datenbearbeitung stellt, sowie am Prinzip der Spezialermächtigung, wonach die verlangte Rechtsgrundlage nicht durch das DSG bereitgestellt wird, sondern einer bereichsspezifischen Regelung

[84] Vgl. z.B. Art. 18 ff. des Geschäftsreglements der Unabhängigen Beschwerdeinstanz für Radio und Fernsehen (SR 784.409).

bedarf, soll im Grundsatz festgehalten werden. Allerdings erachtet die Begleitgruppe die Konzeption von Art. 17 Abs. 2 DSG, welcher die ausnahmsweise zulässigen Surrogate für eine Rechtsgrundlage regelt, als unklar. Die Begleitgruppe schlägt vor, diese Bestimmung redaktionell zu überprüfen und insbesondere zu verdeutlichen, dass sich die in Art. 17 Abs. 2 lit. c DSG genannte Ausnahme vom Erfordernis der Rechtsgrundlage über die besonders schützenswerten Personendaten hinaus auch auf die Bearbeitung von «gewöhnlichen» Personendaten nach Art. 17 Abs. 1 DSG bezieht.

Weitergehende Vorgaben im DSG an die Formulierung von bereichsspezifischen gesetzlichen Grundlagen für Datenbearbeitungen erscheinen der Begleitgruppe nicht zweckmässig. Sie verweist in diesem Zusammenhang einerseits auf die verwaltungsinterne Rechtsetzungsbegleitung durch das Bundesamt für Justiz, in welcher die spezialgesetzlichen Grundlagen unter rechtlichen Gesichtspunkten kontrolliert werden. Andererseits wird die Datenschutzaufsichtsbehörde im Gesetzgebungsprozess zur Stellungnahme eingeladen (vgl. Art. 31 Abs. 1 lit. b DSG). Diese Instrumente tragen dazu bei, den allgemeinen datenschutzrechtlichen Anforderungen auch im Rahmen sektorspezifischer Vorschriften Rechnung zu tragen.

Ein *Teil der Begleitgruppe* schlägt allerdings vor, dass in diesem Zusammenhang geprüft werden sollte, ob die Anforderungen an die formell-gesetzlichen Rechtsgrundlagen von Informationssystemen nicht in den Grundzügen im DSG vorgegeben werden sollten. Die gegenwärtige Praxis[85] führt dazu, dass sehr viele Details auf der Stufe des formellen Gesetzes festgeschrieben werden müssen.

Die Bestimmung betreffend automatisierte Datenbearbeitung im Rahmen von Pilotversuchen (Art. 17*a* DSG) hat in der Praxis nur marginale Bedeutung erlangt. Es erscheint der Begleitgruppe daher sinnvoll, dieses Verfahren zu vereinfachen. Sie schlägt vor, anstelle des Bundesrates inskünftig die Datenschutzaufsichtsbehörde zur Bewilligungserteilung (mittels Verfügung) zu ermächtigen. Ausserdem sollte die Bestimmung gekürzt bzw. überwiegend auf Verordnungsstufe geregelt werden. Da es sich bei Art. 17*a* DSG um eine Ausnahme vom Erfordernis einer Rechtsgrundlage für das Bearbeiten von besonders schützenswerten Personendaten handelt, sollte dieser Ausnahmetatbestand aus systematischen Gründen nicht separat, sondern bei den weiteren Surrogaten für eine Rechtsgrundlage in Art. 17 Abs. 2 DSG geregelt werden.

4.9.3 Besondere Bestimmungen für bestimmte Datenbearbeitungsformen

Für verschiedene Bearbeitungsformen (z.B. Beschaffen, Bekanntgabe, Anonymisieren und Vernichten) macht das DSG den Bundesorganen besondere Vorschriften. Diese Bestimmungen haben sich grundsätzlich bewährt.

Besondere Bestimmungen zur Bekanntgabe von Personendaten: Allerdings ist das Verhältnis von Art. 19 DSG (Bekanntgabe von Personendaten) zu Art. 17 DSG (Rechtsgrundlagen) insbesondere in Bezug auf die Ausnahmen vom Erfordernis der gesetzlichen Grundlagen bei der Bekanntgabe von besonders schützenswerten Personendaten zu klären. Nach Erachten der Begleitgruppe soll sich Art. 19 DSG auf alle Personendaten, einschliesslich auf besonders schützenswerte Personendaten beziehen. Sodann schlägt die Begleitgruppe vor, den Ausnahmekatalog in Art. 19 Abs. 1 DSG insofern zu erweitern, als die Bekanntgabe von Personendaten durch Bundesorgane trotz fehlender Rechtsgrundlage erlaubt sein soll, wenn

[85] Vgl. dazu den Leitfaden des BJ für die Erarbeitung der Rechtsgrundlagen für den Betrieb eines Systems zur automatisierten Bearbeitung von Personendaten vom 16. Dezember 2010.

dies zum Schutz besonders gewichtiger bzw. vitaler Interessen (wie das Leben oder die körperliche Integrität) der betroffenen Person oder von Drittpersonen erforderlich ist. Schliesslich ist die Begleitgruppe der Auffassung, dass Art. 19 Abs. 3 DSG betreffend Abrufverfahren aufgehoben werden kann. Solche Verfahren sind aufgrund des Stands der Technik gängiger geworden und für die betroffenen Personen nicht mehr gleich unerwartet wie noch zum Zeitpunkt der Einführung dieser Bestimmung. Für diesen Sonderfall der Datenbekanntgabe genügen daher nach der Ansicht der Begleitgruppe die Anforderungen an die gesetzliche Grundlage gemäss Art. 19 Abs. 1 DSG.

Besondere Bestimmungen zur Informationspflicht beim Beschaffen von Personendaten*:* Vgl. Ziff. 4.3.1. Dabei ist zu berücksichtigen, dass Art. 18 DSG inhaltlich bereits durch Art. 18*a* DSG abgedeckt wird und daher aufgehoben werden kann.

4.9.4 Organisatorische Massnahmen

Die Eigenverantwortung der öffentlichen Datenbearbeitenden für die Einhaltung der datenschutzrechtlichen Vorschriften soll gestärkt und gefördert werden, indem die gemäss Art. 23 VDSG von Bundeskanzlei und Departementen zu bezeichnenden «Berater für den Datenschutz» künftig den Anforderungen an Aufgaben und Stellung der «Datenschutzverantwortlichen» i.S.v. Art. 12*a* und 12*b* VDSG zu genügen haben sollen (vgl. vorangehend Ziff. 4.3.2).[86] Dies bedeutet insbesondere, dass die Datenschutzberater ihre Tätigkeit in organisatorischer und fachlicher Hinsicht unabhängig ausüben können müssen und über die dazu erforderlichen Ressourcen verfügen sollten. Eine Stärkung der verwaltungsinternen Datenschutzberater könnte auch zur Entlastung der Datenschutzaufsichtsbehörde beitragen.

4.9.5 Rechtsansprüche und Verfahren

a) Rechtsansprüche

Wie in Ziff. 4.4.1 und 4.4.2 ausgeführt, sollen die verschiedenen datenschutzspezifischen Rechtsansprüche in einem Katalog für den öffentlichen und privaten Sektor zusammengestellt werden. Damit soll die Lesbarkeit des DSG verbessert und den betroffenen Personen eine nachvollziehbare Übersicht über die ihnen gegenüber den Datenbearbeitenden zur Verfügung stehenden Rechte ermöglicht werden. Am geltenden System der Rechtsdurchsetzung (z.B. hinsichtlich der Aktiv- und Passivlegitimation sowie der Rechtsbehelfe) soll dagegen materiell grundsätzlich nichts geändert werden. Was die Datenbearbeitung durch Bundesorgane betrifft, ist jedoch noch vertieft zu prüfen, ob sich – analog zum privatrechtlichen Datenschutz – ein Widerspruchsrecht für sämtliche Datenbearbeitungen einführen lässt. Nach Art. 20 DSG können die betroffenen Personen vom verantwortlichen Bundesorgan derzeit lediglich verlangen, dass es die Bekanntgabe von bestimmten Personendaten an Dritte sperrt.

Die Geltendmachung von Schadenersatz und Genugtuungsansprüchen soll sich weiterhin nach den allgemeinen Voraussetzungen des Staatshaftungsrechts richten. Die finanziellen Auswirkungen von unzulässigen Datenbearbeitungen beurteilen sich damit auch inskünftig nach Art. 3 ff. des Verantwortlichkeitsgesetzes (VG; SR 170.32).

b) Beweislastverteilung

Bei der Durchsetzung datenschutzrechtlicher Ansprüche gegenüber Bundesorganen sollen die betroffenen Personen ebenso von einer Beweislasterleichterung profitieren können, wie

---

[86] Zur Aufgabe und Stellung der Datenschutzverantwortlichen vgl. die Erläuterungen des EDÖB; online einsehbar unter <http://www.edoeb.admin.ch/datenschutz/00626/00743/00874/01051/index.html?lang=de>.

die Begleitgruppe sie im Rahmen der Bestimmungen zu den privaten Datenbearbeitungen vorgeschlagen hat (vgl. Ziff. 4.8.2). Dabei handelt es sich um eine Beweislastumkehr nach dem Beispiel des Art. 13*a* Abs. 1 UWG[87], wonach von den Datenbearbeitenden im Einzelfall der Nachweis einer datenschutzkonformen Bearbeitung verlangt werden kann, wenn dies unter Berücksichtigung der berechtigten Interessen der am Verfahren beteiligten Parteien angemessen erscheint (zur gesetzlichen Vermutung der Rechtmässigkeit einer Datenbearbeitung bei Einhaltung der Regeln der Guten Praxis vgl. oben Ziff. 4.1.2 lit. b). Dies könnte beispielsweise dann der Fall sein, wenn die Beweisführung für die betroffene Person besonders schwierig ist, weil Tatsachen nachzuweisen sind, die im Einflussbereich der Datenbearbeitenden liegen (z.B. im Zusammenhang mit der Einhaltung von datenschutzrechtlichen Sorgfaltspflichten gemäss Ziff. 4.3.2).

c) Verfahrensbestimmungen

Die Evaluation des Datenschutzgesetzes hat gezeigt, dass der Verfahrensweg von den Betroffenen im Zusammenhang mit Datenbearbeitungen durch Bundesorgane häufiger beansprucht wird als gegenüber privaten Datenbearbeitenden. Absolut gesehen werden jedoch auch im öffentlichen Sektor die Durchsetzungsrechte nur selten genutzt.[88] Dabei gibt es nach der Auffassung der Begleitgruppe im öffentlichen Verfahren – ebenso wie im Privatrecht – nur wenig Spielraum zur Verbesserung des Individualrechtsschutzes, so dass die Durchsetzung der öffentlich-rechtlichen Datenschutzbestimmungen vor allem durch eine Erweiterung der Kompetenzen der Datenschutzaufsicht gestärkt werden soll (vgl. Ziff. 4.10.2).

Wie für das Zivilverfahren schlägt die Begleitgruppe aber ergänzend vor, den erstinstanzlich verfügenden Verwaltungsbehörden oder den Beschwerdeinstanzen die Möglichkeit einzuräumen, bei der Datenschutzaufsichtsbehörde eine *Stellungnahme* einzuholen (vgl. Ziff. 4.8.3 lit. b): Steht in einem öffentlich-rechtlichen Verfahren die Zulässigkeit einer Datenbearbeitung in Frage, kann die zuständige Verwaltungsbehörde bzw. Beschwerdeinstanz von Amtes wegen oder auf Antrag einer Partei die Sache der Datenschutzaufsichtsbehörde zur Stellungnahme vorlegen. Die Datenschutzaufsichtsbehörde ist nicht zur Abgabe einer Stellungnahme verpflichtet. Nimmt die Datenschutzaufsichtsbehörde Stellung, ist dies nicht bindend.

d) Alternative Streitbeilegungsmechanismen

Für Streitigkeiten im Zusammenhang mit Datenbearbeitungen durch Bundesorgane soll – wie im privaten Bereich – ein alternatives Konfliktlösungsverfahren zur Verfügung gestellt werden. Für das (fakultative) Vermittlungsverfahren soll die von der Datenschutzaufsichtsbehörde zu bezeichnende Mediations- bzw. Ombudsstelle zuständig sein (vgl. Ziff. 4.8.3 lit. c).

4.9.6 Verhältnis zwischen den Vorschriften des DSG und des BGÖ

Das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (BGÖ; SR 152.3) weist verschiedene Schnittstellen zum DSG auf. Da das BGÖ momentan hinsichtlich seiner Umsetzung und Wirkung evaluiert wird, sind Vorschläge, mit denen in den Geltungsbereich des

---

[87] Art. 13*a* Abs. 1 UWG: «Der Richter kann vom Werbenden den Beweis für die Richtigkeit von in der Werbung enthaltenen Tatsachenbehauptungen verlangen, wenn dies unter Berücksichtigung der berechtigten Interessen des Werbenden und anderer am Verfahren beteiligter Personen im Einzelfall angemessen erscheint.»

[88] Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz vom 10. März 2011, S. 86 ff., 133 ff., 208; online einsehbar unter <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

BGÖ eingegriffen wird, gemäss der Begleitgruppe zum jetzigen Zeitpunkt nicht zweckmässig.[89]

4.10 Aufsichtsbehörden

4.10.1 Einleitung

Wie bereits erwähnt, hat die Evaluation des DSG aus der Sicht einer *Mehrheit der Begleitgruppe* Lücken in der Durchsetzung des Gesetzes aufgezeigt. Diesen Mängeln lässt sich zwar durch einen Ausbau der Verfahrensrechte und des gerichtlichen Zugangs für die betroffenen Personen teilweise abhelfen. Doch nach der Auffassung der Mehrheit der Begleitgruppe kann die Wirksamkeit des Gesetzes nur dann tatsächlich verbessert werden, wenn die Befugnisse der Datenschutzaufsichtsbehörde durch Verfügungskompetenzen massgeblich gestärkt werden (siehe dazu die Überlegungen in Ziff. 4.1.2 lit. a). Auch im Modernisierungsentwurf zur Datenschutzkonvention SEV 108 sind solche Kompetenzen vorgesehen. Dabei ist besonders darauf zu achten, dass die Unabhängigkeit der Aufsichtsbehörde erhalten bleibt oder gar verbessert wird. Es handelt sich um ein Thema, das in der Schweiz[90], aber auch auf europäischer Ebene[91] weiterhin aktuell ist.

Angesichts der erweiterten Kompetenzen und Befugnisse, die dem EDÖB übertragen werden sollen, hat die Begleitgruppe darüber diskutiert, ob es nicht angebracht wäre, dessen Organisation anzupassen und als Kollegialbehörde auszugestalten. Entsprechende Vorschläge sind nachfolgend in Ziff. 4.10.3 angeführt.

Eine Minderheit der Begleitgruppe lehnt einen Ausbau der Befugnisse (insbesondere der Verfügungs- und Sanktionsbefugnisse) der Datenschutzaufsichtsbehörde ab. Allfällige Gesetzesänderungen sollen ihres Erachtens nur vorgenommen werden, soweit sie in Anbetracht des EU-Rechts und des Modernisierungsentwurfs zur Datenschutzkonvention SEV 108 für den Marktzugang notwendig sind (vgl. Ziff. 3).

4.10.2 Aufgaben und Kompetenzen der Aufsichtsbehörde

a) Im Privatrechtsbereich

aa) Aufsicht über die privaten Datenbearbeitenden

Durchführung einer Vorabklärung*:* Die Begleitgruppe schlägt vor, ein Vorabklärungsverfahren nach dem Vorbild von Art. 26 KG[92] einzuführen. Dieses Verfahren sollte sehr informell und möglichst einfach ausgestaltet werden, um einvernehmliche Lösungen zu erleichtern. Die Vorabklärung wäre keine obligatorische Verfahrensetappe und in bestimmten Fällen könnte die Datenschutzaufsichtsbehörde direkt ein formelles Verfahren einleiten.

---

[89] Vgl. zur Evaluation des BGÖ <http://www.admin.ch/aktuell/00089/index.html?lang=de&msg-id=52653>. Das BJ wird dem Bundesrat bis Ende 2014 über die Ergebnisse der Evaluation Bericht erstatten. Allenfalls sind diese Ergebnisse in den weiteren Verlauf der Revisionsarbeiten zum DSG einzubeziehen.

[90] Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335 ff., 350.

[91] Urteile des EuGH C-614/10 vom 16. Oktober 2012 und C-288/12 vom 8. April 2014.

[92] Art. 26 KG: «Das Sekretariat kann Vorabklärungen von Amtes wegen, auf Begehren von Beteiligten oder auf Anzeige von Dritten hin durchführen.» (Abs. 1). «Das Sekretariat kann Massnahmen zur Beseitigung oder Verhinderung von Wettbewerbsbeschränkungen anregen.» (Abs. 2). «Im Verfahren der Vorabklärung besteht kein Recht auf Akteneinsicht.» (Abs. 3).

Mit dem Vorabklärungsverfahren könnten jene Angelegenheiten ausgesondert werden, welche die Einleitung einer Untersuchung im eigentlichen Sinn erfordern. Es gäbe den Privatpersonen, insbesondere den Personen, deren Daten bearbeitet werden, eine einfache Möglichkeit, die Aufsichtsbehörde um Rat anzugehen. Für dieses Verfahren wäre das ständige Sekretariat der Datenschutzaufsichtsbehörde zuständig (vgl. Ziff. 4.10.3). Die Aufsichtsbehörde könnte Vorabklärungen von Amtes wegen, auf Begehren von Personen, die von einer Datenbearbeitung betroffen sind, oder auf Anzeige von Dritten hin einleiten. Sie wäre jedoch nicht dazu verpflichtet. Ausserdem gäbe es kein Rechtsmittel gegen einen Nichteintretensentscheid. Das Verfahren sollte unentgeltlich sein.

Am Ende der Vorabklärung hätte die Aufsichtsbehörde mehrere Möglichkeiten für das weitere Vorgehen zur Verfügung. Lägen keine Anhaltspunkte für einen Sachverhalt vor, welcher die Einleitung einer formellen Untersuchung rechtfertigen würde (Art. 29 DSG), würde sie die Beteiligten lediglich schriftlich darüber informieren. Bestünden dagegen Anhaltspunkten für einen Sachverhalt, welcher zur Eröffnung einer formellen Untersuchung Anlass gäbe, könnte sie:

- *Massnahmen zur Beseitigung oder Verhinderung einer Verletzung des DSG anregen*. Die Zustimmung des Datenbearbeitenden zu dieser Anregung würde keine einvernehmliche Regelung darstellen, deren Verletzung bestraft werden könnte. Es würde sich um einfache einseitige Verpflichtungen ohne jegliche Formerfordernisse handeln. Bei Einhaltung der eingegangenen Verpflichtungen würde die Aufsichtsbehörde keine Untersuchung einleiten.
- eine *formelle Untersuchung eröffnen*.

Die Information und die Anregungen durch die Aufsichtsbehörde wären ebenso wenig anfechtbar wie die Eröffnung einer formellen Untersuchung.

Eröffnung einer formellen Untersuchung: Es wird vorgeschlagen, den Umfang der Untersuchungsbefugnisse der Aufsichtsbehörde nicht mehr auf die Sachverhalte zu beschränken, welche gegenwärtig in Art. 29 DSG vorgegeben sind. Aufgrund ihrer beschränkten Mittel wird die Aufsichtsbehörde Prioritäten setzen und sich auf jene Fälle konzentrieren müssen, die von öffentlichem Interesse sind.

Informationsbeschaffungsbefugnisse im Rahmen des formellen Untersuchungsverfahrens: Damit die Aufsichtsbehörde den Sachverhalt möglichst rasch und exakt abklären kann, wird angeregt, ihre Informationsbeschaffungsbefugnisse auszubauen. Neben dem Recht, von den für die Datenbearbeitung Verantwortlichen Auskünfte einzuholen, Akten herauszuverlangen und sich Datenbearbeitungen vorführen zu lassen (Art. 29 Abs. 2 DSG), könnte die Datenschutzaufsichtsbehörde künftig ermächtigt werden, unter bestimmten Voraussetzungen Zugang zu den Räumlichkeiten und Informatikprogrammen zu erhalten sowie Beschlagnahmen durchzuführen oder Siegel anbringen zu lassen. Das Verfahren würde dem Verwaltungsverfahrensgesetz (VwVG; SR 172.021) oder sinngemäss je nach den vorgesehenen Massnahmen auch dem Bundesgesetz über das Verwaltungsstrafrecht (VStrR; SR 313.0; Art. 45 ff.) unterstehen.

Verfügungs- und Sanktionskompetenzen[93]: Der Aufsichtsbehörde könnten Verfügungskompetenzen eingeräumt werden, so dass sie Massnahmen wie zum Beispiel die Sistierung oder

[93] Die Staatspolitische Kommission des Nationalrates (SPK-NR) hat am 29. August 2014 beschlossen, der parlamentarischen Initiative Schwaab 14.404 vom 19. März 2014 «Für wirklich abschreckende Sanktionen bei Datenschutzverletzungen» nicht Folge zu geben.

Unterlassung einer Datenbearbeitung anordnen könnte. Ausserdem hätte sie die Befugnis, unter gewissen Voraussetzungen Geldsanktionen zu verhängen. Konkret: Kommt die Aufsichtsbehörde am Ende einer formellen Untersuchung zum Schluss, dass eine Datenbearbeitung nicht den Anforderungen des Gesetzes entspricht, würde sie dem Verantwortlichen eine Frist einräumen, um die Situation gesetzeskonform zu ordnen. Parallel dazu könnte sie eine einvernehmliche Regelung vorschlagen, ähnlich wie dies beispielsweise in Art. 29 KG[94] für das Wettbewerbsrecht vorgesehen ist. Wird der rechtmässige Zustand bis zum Ablauf der gesetzten Frist oder im Rahmen der Erfüllung einer einvernehmlichen Regelung nicht hergestellt, hätte die Aufsichtsbehörde die Möglichkeit, eine Verfügung zu erlassen, welche die Datenbearbeitung verbietet oder aussetzt und/oder dem für die Datenbearbeitung Verantwortlichen vorschreibt, bestimmte Massnahmen zu treffen. Wird eine rechtskräftige Verfügung oder eine einvernehmliche Regelung nicht beachtet, könnte die Aufsichtsbehörde eine Geldstrafe verhängen. In bestimmten Fällen krasser Gesetzesverstösse könnte die Behörde kumulativ zu einer Massnahme (wie dem Verbot oder der Sistierung einer Datenbearbeitung oder anderen Massnahmen) direkt (d.h. ohne Umweg über eine einvernehmliche Regelung oder das Ansetzen einer Frist) eine Geldsanktion verhängen. Zusätzlich könnte auch die Verweigerung der Mitwirkung bestraft werden. Die Aufsichtsbehörde könnte in jedem Fall die notwendigen vorsorglichen Massnahmen treffen.

- Variante: Ein *Teil der Begleitgruppe* schlägt vor, dass die Aufsichtsbehörde die Nichteinhaltung ihrer rechtskräftigen Verfügungen nicht selbst sanktionieren, sondern im Verfügungsdispositiv jeweils auf die Strafdrohung von Art. 292 des Schweizerischen Strafgesetzbuchs hinweisen soll (StGB; SR 311.0). In diesem Fall wäre die Strafverfolgung Sache der Kantone.

Personen, welche der Datenschutzaufsichtsbehörde einen Fall melden, sollen dadurch weder Parteistellung im Verfahren noch Beschwerdelegitimation erhalten, da die Aufsichtsbehörde auch künftig Garantin des öffentlichen Interesses bleiben und nicht einzelne Streitigkeiten entscheiden soll.

Um die Rechtsdurchsetzung gegenüber Datenbearbeitenden, die keinen (Wohn-)Sitz in der Schweiz haben, zu erleichtern, sollen diese im Rahmen der Abklärungen der Datenschutzaufsichtsbehörde gemäss Art. 29 DSG verpflichtet werden, eine Zustelladresse in der Schweiz zu bezeichnen, an welche insbesondere Mitteilungen und Verfügungen rechtsgültig zugestellt werden können[95]. Die Nichtbefolgung dieser Pflicht soll sanktioniert werden.

ab) Beratung Privater

Die in Art. 28 DSG vorgesehene Beratungstätigkeit der Datenschutzaufsichtsbehörde gegenüber privaten Personen soll beibehalten werden.

Insbesondere um zu verhindern, dass die gleichzeitige Beratungs- und Aufsichtstätigkeit der Datenschutzaufsichtsbehörde die Datenbearbeitenden davon abhält, sich zur Beratung an

---

[94] Art. 29 KG: «Erachtet das Sekretariat eine Wettbewerbsbeschränkung für unzulässig, so kann es den Beteiligten eine einvernehmliche Regelung über die Art und Weise ihrer Beseitigung vorschlagen.» (Abs. 1). «Die einvernehmliche Regelung wird schriftlich abgefasst und bedarf der Genehmigung durch die Wettbewerbskommission.» (Abs. 2).

[95] Eine ähnliche Vorschrift findet sich beispielsweise in Art. 5 der Verordnung über Fernmeldedienste (FDV, SR 784.101.1): «Meldepflichtige Anbieterinnen von Fernmeldediensten mit Sitz im Ausland müssen eine Korrespondenzadresse in der Schweiz bezeichnen, an welche insbesondere Mitteilungen, Vorladungen und Verfügungen rechtsgültig zugestellt werden können.»

die Behörde zu wenden, schlägt die Begleitgruppe die Einführung einer Art Vorprüfungsverfahren vor, ähnlich wie es im Kartellrecht besteht. Im Gegensatz zur Regelung im Kartellgesetz wäre das Vorprüfungsverfahren im Datenschutzrecht fakultativ. Es ginge darum, dem für die Datenbearbeitung Verantwortlichen zu ermöglichen, vor einem neuen Datenbearbeitungsvorgang die allfälligen Einwände der Aufsichtsbehörde in Erfahrung zu bringen und in der Folge Geldsanktionen zu vermeiden. Praktisch würde dies bedeuten, dass beabsichtigte Datenbearbeitungen der Aufsichtsbehörde vorgelegt werden können. Diese müsste dann – nach dem Vorbild von Art. 32 KG[96] – innerhalb einer bestimmten Frist (z.B. innerhalb eines Monats) entscheiden, ob eine Prüfung der Datenbearbeitung durchzuführen ist. Erfolgt innert dieser Frist keine Mitteilung der Datenschutzaufsichtsbehörde, dass eine Prüfung einzuleiten sei, könnte die Datenbearbeitung vorgenommen werden, ohne eine Sanktionierung durch die Aufsichtsbehörde zu riskieren, sofern die Datenbearbeitung wie angemeldet durchgeführt wird. Analog zu Art. 38 KG[97] sollten jedoch Gründe vorgesehen werden, die es der Datenschutzaufsichtsbehörde ermöglichen, trotz Ablauf der Frist eine Prüfung einzuleiten (z.B. wenn der für die Datenbearbeitung Verantwortliche unrichtige Angaben gemacht hat, wenn die Gefahr einer schwerwiegenden Widerhandlung besteht, die gestützt auf die abgegebenen Informationen nicht zu erkennen war, usw.). Falls einschlägige Regeln der Guten Praxis bestehen (vgl. Ziff. 4.1.2 lit. b) und der Datenbearbeitende sich daran hält, hätte er keine Geldsanktion zu vergewärtigen. Legt er seinen Fall der Datenschutzaufsichtsbehörde vor, obwohl Regeln der Guten Praxis bestehen, könnte sich die Behörde damit begnügen, ohne inhaltliche Prüfung auf diese Regeln zu verweisen. Liegen keine Regeln der Guten Praxis vor, könnte die Datenschutzaufsichtsbehörde beim für den Erlass von Regeln der Guten Praxis zuständigen Komitee anregen, für den betreffenden Fall solche Regeln zu erarbeiten.

b) Im öffentlich-rechtlichen Bereich

ba) Aufsicht über Bundesorgane

Die Begleitgruppe schlägt vor, auch die Datenschutzaufsicht über die Bundesorgane auszubauen, nach Möglichkeit analog zu den Vorschlägen für den Privatrechtsbereich (vgl. Ziff. 4.1.14.1.1).

Durchführung einer Vorabklärung: Die Begleitgruppe regt an, ebenso wie im Rahmen der Aufsicht über private Datenbearbeitende ein Vorabklärungsverfahren für Datenbearbeitungen durch Bundesorgane einzuführen (vgl. Ziff. 4.10.2 lit. a/aa).

Eröffnung einer formellen Untersuchung: Hat die Vorabklärung Hinweise auf eine Verletzung

---

[96] Art. 32 KG: «Wird ein Vorhaben über einen Unternehmenszusammenschluss gemeldet (...), so entscheidet die Wettbewerbskommission, ob eine Prüfung durchzuführen ist. Sie hat die Einleitung dieser Prüfung den beteiligten Unternehmen innerhalb eines Monats seit der Meldung mitzuteilen. Erfolgt innerhalb dieser Frist keine Mitteilung, so kann der Zusammenschluss ohne Vorbehalt vollzogen werden.» (Abs. 1). «Die beteiligten Unternehmen dürfen den Zusammenschluss innerhalb eines Monats seit der Meldung des Vorhabens nicht vollziehen, es sei denn, die Wettbewerbskommission habe dies auf Antrag dieser Unternehmen aus wichtigen Gründen bewilligt.» (Abs. 2).

[97] Art. 38 KG: «Die Wettbewerbskommission kann eine Zulassung widerrufen oder die Prüfung eines Zusammenschlusses trotz Ablauf der Frist von Artikel 32 Absatz 1 beschliessen, wenn: a. die beteiligten Unternehmen unrichtige Angaben gemacht haben; b. die Zulassung arglistig herbeigeführt worden ist; oder c. die beteiligten Unternehmen einer Auflage zu einer Zulassung in schwerwiegender Weise zuwiderhandeln.» (Abs. 1). «Der Bundesrat kann eine ausnahmsweise Zulassung aus denselben Gründen widerrufen.» (Abs. 2).

der Datenschutzvorschriften ergeben oder liegt ein eindeutiger Verstoss vor, soll die Datenschutzaufsichtsbehörde eine formelle Untersuchung einleiten können (vgl. Ziff. 4.10.2 lit. a/aa).

Informationsbeschaffungsbefugnisse im Rahmen des formellen Untersuchungsverfahrens: Neben den Befugnissen, über welche die Aufsichtsbehörde bereits verfügt, wird vorgeschlagen, sie zu ermächtigen, die von den Bundesorganen bearbeiteten Daten im Abrufverfahren einzusehen. Der Zugang würde sich auf die Dauer des Verfahrens beschränken.

Verfügungskompetenzen: Um die Kontrollinstrumente und Befugnisse der Datenschutzaufsichtsbehörde gegenüber Bundesorganen zu stärken, aber auch in der Bemühung mit Blick auf den Modernisierungsentwurf zur Datenschutzkonvention SEV 108 sowie die Weiterentwicklung des Schengen/Dublin-Besitzstandes im EU-Datenschutzrecht einen angemessenen Datenschutz zu gewährleisten, wird ein Modell vorgeschlagen, das auch von einigen Kantonen (z.B. Schaffhausen und Basel-Stadt) angewendet wird. Dabei soll der Datenschutzaufsichtsbehörde neben dem bisher in Art. 27 DSG vorgesehenen Instrument der Empfehlung auch Verfügungsbefugnis eingeräumt werden. Mit diesem Vorschlag könnten überdies die Datenschutzvorschriften im öffentlichen und privaten Bereich bis zu einem gewissen Grad harmonisiert werden. Im Einzelnen: Stellt die Aufsichtsbehörde eine Verletzung von Datenschutzvorschriften fest, so gibt sie dem verantwortlichen Bundesorgan eine Empfehlung ab und orientiert das zuständige Departement oder die Bundeskanzlei. Wird die Empfehlung abgelehnt oder nicht befolgt, kann die Datenschutzaufsichtsbehörde ihre Empfehlung oder Teile davon in Form einer anfechtbaren Verfügung erlassen[98]. Das betroffene Bundesorgan kann diese Verfügung nach den allgemeinen Bestimmungen über die Bundesrechtspflege anfechten. Zu prüfen wäre ausserdem, ob der Datenschutzaufsichtsbehörde die Befugnis eingeräumt werden soll, im Rahmen vorsorglicher Massnahmen die Einschränkung oder Einstellung einer Datenbearbeitung direkt anzuordnen[99]. Es ist noch vertieft abzuklären, inwiefern dieses Modell zu Koordinationsproblemen mit dem individuellen Rechtsschutz nach Art. 25 DSG führen könnte. Ausserdem ist zu prüfen, ob und wie sich ein solches Modell in das bestehende öffentliche Verfahrensrecht (VwVG, VGG, BGG) integrieren lässt.

Auf die Anordnung von Verwaltungsstrafen (z.B. Bussen) zur Durchsetzung der Verfügungen der Datenschutzaufsichtsbehörde, wie es in verschiedenen EU Länder praktiziert wird (vgl. Ziff. 4.1.2 lit. a), sollte nach der *Mehrheit der Begleitgruppe* verzichtet werden, soweit dies nicht im Rahmen der Weiterentwicklung des Schengen/Dublin-Besitzstandes vorgegeben wird.

Dritte, welche der Datenschutzaufsichtsbehörde einen Fall anzeigen, sollen dadurch weder Parteistellung noch Beschwerdelegitimation erhalten (vgl. Ziff. 4.10.2 lit. a/aa).

bb) Beratung der Bundesorgane (Art. 31 Abs. 2 DSG)

Die Beratungstätigkeit der Datenschutzaufsichtsbehörde gegenüber Bundesorganen soll beibehalten werden. Falls die Ausnahme vom Geltungsbereich des DSG in Art. 2 Abs. 2 lit. d DSG aufgehoben wird (siehe Ziff. 4.2.1 lit. d/db), wäre die Formulierung von Art. 31 Abs. 2

---

[98] Im Kanton BS wird dazu ein schwerwiegendes Interesse an der Durchsetzung der empfohlenen Massnahme vorausgesetzt. Vgl. zum Ganzen § 47 Abs. 1, 2 und 5 des Informations- und Datenschutzgesetzes des Kantons Basel-Stadt (IDG BS; SG 153.260) sowie Art. 26 f. des Datenschutzgesetzes des Kantons Schaffhausen (SHR 174.100).

[99] Vgl. § 47 Abs. 4 IDG BS: «Werden schutzwürdige Interessen offensichtlich gefährdet oder verletzt, so kann die oder der Datenschutzbeauftragte anordnen, dass das öffentliche Organ die Bearbeitung bis zur erfolgten Überprüfung durch das Appellationsgericht einschränkt oder einstellt.»

DSG anzupassen.

c) Erarbeitung von detaillierteren Regelungen

Wie bereits dargelegt (vgl. Ziff. 4.1.2 lit. b), liesse sich mit der Einführung von Regeln der Guten Praxis bzw. verbindlichen Regeln zur Konkretisierung des DSG die Rechtssicherheit erhöhen, da das DSG weiterhin sehr allgemein und technologieneutral bleiben soll.

Die *Mehrheit der Begleitgruppe* schlägt vor, diese Regeln von einem Komitee erarbeiten zu lassen, das sich von der Datenschutzaufsichtsbehörde im engeren Sinn unterscheidet. Die Regeln der Guten Praxis könnten überdies auch aus eigener Initiative oder auf Auftrag hin durch die betroffenen Kreise selbst erarbeitet werden, wobei sie die Regeln anschliessend dem Komitee oder der Datenschutzaufsichtsbehörde zur Genehmigung vorlegen würden (vgl. Ziff. 4.1.2 lit. b).

d) Information und Sensibilisierung der Öffentlichkeit

Die Aufgabe der Aufsichtsbehörde, in Fällen von allgemeinem Interesse die Öffentlichkeit über ihre Feststellungen zu informieren, soll beibehalten werden. Dabei handelt es sich um ein wichtiges Präventionsinstrument. Allfällige Geschäftsgeheimnisse dürfen jedoch nicht beeinträchtigt werden.

Der EDÖB sensibilisiert die Bevölkerung bereits heute, vor allem durch Informationen auf seiner Website. Der Evaluationsbericht des Bundesrates hat jedoch gezeigt, dass die Betroffenen trotzdem nicht immer die erforderlichen Vorsichtsmassnahmen treffen, entweder weil sie sich überfordert fühlen oder weil sie die bestehenden Möglichkeiten der Datenbearbeitung und deren Risiken unterschätzen.[100] Die Begleitgruppe schlägt vor, die Datenschutzaufsichtsbehörde – wie im Modernisierungsentwurf zur Datenschutzkonvention SEV 108 (Art. 12bis Abs. 2 lit. e) vorgesehen – damit zu beauftragen, die Bevölkerung für den Datenschutz zu sensibilisieren und entsprechend auszubilden. Diese Sensibilisierung könnte durch Regeln der Guten Praxis bzw. verbindliche Detailregelungen (vgl. Ziff. 4.1.2 lit. b), Informationskampagnen oder auch Ausbildungsbeiträge erfolgen. Besondere Anstrengungen sollten hinsichtlich der Frage der Einwilligung der betroffenen Personen unternommen werden (Ziff. 4.3.3). Ausserdem ist Minderjährigen und anderen Schutzbedürftigen besondere Beachtung zu schenken.

e) Stellungnahmen in zivil- und verwaltungsrechtlichen Verfahren

Neben den Aufgaben, welche die Datenschutzaufsichtsbehörde bereits wahrnimmt, schlägt die Begleitgruppe – nach dem Vorbild von Art. 15 KG[101] – vor, dass dieser in einem zivil- oder verwaltungsrechtlichen Verfahren auf Antrag einer Partei oder von Amtes wegen die Sache zur Stellungnahme vorgelegt werden können soll. Damit liesse sich verhindern, dass nicht spezialisierte Stellen, vor allem in erster Instanz, über zuweilen heikle und technische Fälle allein entscheiden müssen (vgl. dazu Ziff. 4.8.3 lit. b und 4.9.5 lit. c).

f) Aussergerichtliches Verfahren zur Streitbeilegung (alternative Streitbeilegungsmechanismen)

Vgl. dazu Ziff. 4.8.3 lit. c.

---

[100] Vgl. Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335 ff., 342.

[101] Art. 15 Abs. 1 KG: «Steht in einem zivilrechtlichen Verfahren die Zulässigkeit einer Wettbewerbsbeschränkung in Frage, so wird die Sache der Wettbewerbskommission zur Begutachtung vorgelegt.»

g) Funktion als erstinstanzliche Behörde für datenschutzrechtliche Streitigkeiten

Eine *Minderheit der Begleitgruppe* schlägt vor, der Datenschutzaufsichtsbehörde eine allgemeine Kompetenz zur erstinstanzlichen Entscheidung von datenschutzrechtlichen Streitigkeiten anstelle der Zivilgerichte und der Verwaltungsbehörden einzuräumen. Für reparatorische Klagen würden jedoch weiterhin Letztere zuständig bleiben. Diese Lösung hätte den Vorteil, dass die Streitigkeiten von einer spezialisierten Behörde mit Fachkenntnissen entschieden würden. Eine *Mehrheit der Begleitgruppe* ist jedoch der Auffassung, dass es nicht angebracht sei, vom ordentlichen System abzuweichen und eine spezialisierte Behörde einzusetzen. Eine solche Lösung würde einen Bruch in der schweizerischen Rechtsordnung darstellen und eine Reihe heikler Fragen aufwerfen, die vertieft geprüft werden müssten (Rollenkonflikte, verfahrensrechtliche Probleme usw.). Durch die vorangehend dargestellte Möglichkeit der Zivilgerichte und Verwaltungsbehörden, bei der Datenschutzaufsichtsbehörde Stellungnahmen einzuholen (vgl. Ziff. 4.8.3 lit. b und Ziff. 4.9.5 lit. c), könnte mangelnden Fachkenntnissen der allgemeinen Rechtspflegeinstanzen im Übrigen auf anderem Weg abgeholfen werden.

4.10.3 Organisation der Aufsichtsbehörde

Die Begleitgruppe ist geteilter Meinung über das Organisationsmodell, das für die Datenschutzaufsicht gewählt werden soll. Angesichts der vorgeschlagenen Kompetenzerweiterung (vgl. Ziff. 4.10.2) vertreten *einige Mitglieder der Begleitgruppe* die Auffassung, dass eine kollegiale Struktur am besten geeignet sei. *Andere* sind der Meinung, dass sich das derzeitige System bewährt habe, weshalb kein Grund zur Änderung bestehe. In beiden Fällen stellt sich die Frage, welche Behörde die Regeln der Guten Praxis bzw. die verbindlichen Regeln zur Konkretisierung des DSG zuhanden der Datenbearbeitenden erlassen oder genehmigen soll (siehe Ziff. 4.1.2 lit. b). Die *Mehrheit der Begleitgruppe* ist der Auffassung, dass diese Aufgabe einem Expertenkomitee übertragen werden soll, während eine *Minderheit* die Datenschutzaufsichtsbehörde selbst mit dieser Aufgabe betrauen möchte.

Da die Meinungen innerhalb der Begleitgruppe auseinandergehen, werden anschliessend die folgenden vier Organisationsmodelle vorgeschlagen: a) Schaffung einer Kollegialbehörde mit Komitee; b) Schaffung einer Kollegialbehörde ohne Komitee; c) Beibehaltung einer/eines Beauftragten mit Komitee und d) Beibehaltung einer/eines Beauftragten ohne Komitee.

a) Kollegialbehörde mit Komitee

Nach Ansicht eines *Teils der Begleitgruppe* führt das Modell der Kollegialbehörde zu einer höheren politischen Akzeptanz der im Rahmen der Datenschutzaufsicht allenfalls zu erlassenden Verfügungen und zu verhängenden Sanktionen. Es gewährleiste auch eine repräsentativere und ausgewogenere Entscheidungsfindung und ermögliche es, die Entscheidungen innerhalb eines Kollegiums zu festigen. Zudem stärke das Kollegialmodell die Unabhängigkeit der Aufsichtsbehörde, da sich allfällige äussere Einflüsse in gewisser Weise auf die verschiedenen Mitglieder verteilen.

Auf Bundesebene ist es im Übrigen üblicher, die Aufsichtsaufgaben an Kollegialbehörden zu übertragen, wie der Wettbewerbskommission (WEKO), der Eidgenössischen Spielbankenkommission (ESBK), der Eidgenössischen Elektrizitätskommission (ElCom), dem Schweizerischen Heilmittelinstitut (Swissmedic), der Eidgenössischen Finanzmarktaufsicht (FINMA)

oder dem Eidgenössischen Institut für Geistiges Eigentum (IGE).[102] Das einzige andere Beispiel einer eidgenössischen Behörde, die durch eine Einzelperson verkörpert wird, ist der Preisüberwacher. Seine Situation ist jedoch nicht mit jener des EDÖB vergleichbar, da der Preisüberwacher nicht unabhängig, sondern dem Eidgenössischen Departement für Wirtschaft, Bildung und Forschung (WBF) unterstellt ist. Auf kantonaler Ebene existiert das Modell der Kommission – mit teilweise unterschiedlichen Ausprägungen – in Neuenburg/Jura, im Tessin, in Freiburg und im Wallis. International sind die Modelle der Kommission (z.B. die «Commission Nationale de l'Informatique et des Libertés» [CNIL] in Frankreich) oder des Direktoriums (z.B. der «Garante per la protezione dei dati personali» in Italien [umfasst vier Mitglieder] oder die niederländische Behörde «College bescherming persoonsgegevens» [CBP; umfasst drei Mitglieder]) in mehreren Ländern anzutreffen.

Die Begleitgruppe hat drei Organisationsformen von Kollegialbehörden geprüft: die Anstalt, die Kommission und das Direktorium. Sie hat beschlossen, die ersten beiden Modelle nicht zu berücksichtigen, da diese administrativ zu schwerfällig sind und die Verfahrensabläufe verlangsamen könnten. Die Rechtsform der Anstalt erschien zudem aufgrund der eher geringen Grösse der Datenschutzaufsichtsbehörde nicht angebracht[103].

Es wird deshalb vorgeschlagen, für die Datenschutzaufsicht ein Direktorium einzusetzen. Diese Organisationsform gewährleistet eine rasche Entscheidungsfindung sowie einen effizienten Informationsfluss innerhalb der Behörde und lässt sich gut mit der Einsetzung eines Komitees für die Gute Praxis bzw. für verbindliche Detailregelungen vereinbaren (vgl. Ziff. 4.1.2 lit. b und Ziff. 4.10.2 lit. c). Die Vorteile, welche eine kollegiale Organisationsstruktur mit sich bringt, bleiben im Übrigen grösstenteils erhalten (Unabhängigkeit, politische Akzeptanz der Verfügungen und Sanktionen).

Das Direktorium würde sich aus einer Direktorin oder einem Direktor und zwei Stellvertretenden zusammensetzen, die alle drei unabhängig wären und vom Bundesrat – unter Vorbehalt der Genehmigung durch die Bundesversammlung – gewählt würden. Das Direktorium würde einem ständigen Sekretariat vorstehen, das die administrative Unterstützung sicherstellen, die Verfügungen vorbereiten, die Untersuchungen durchführen und die verfahrensleitenden Entscheidungen erlassen würde. Die wichtigen Entscheidungen müssten durch das Kollegium getroffen werden.

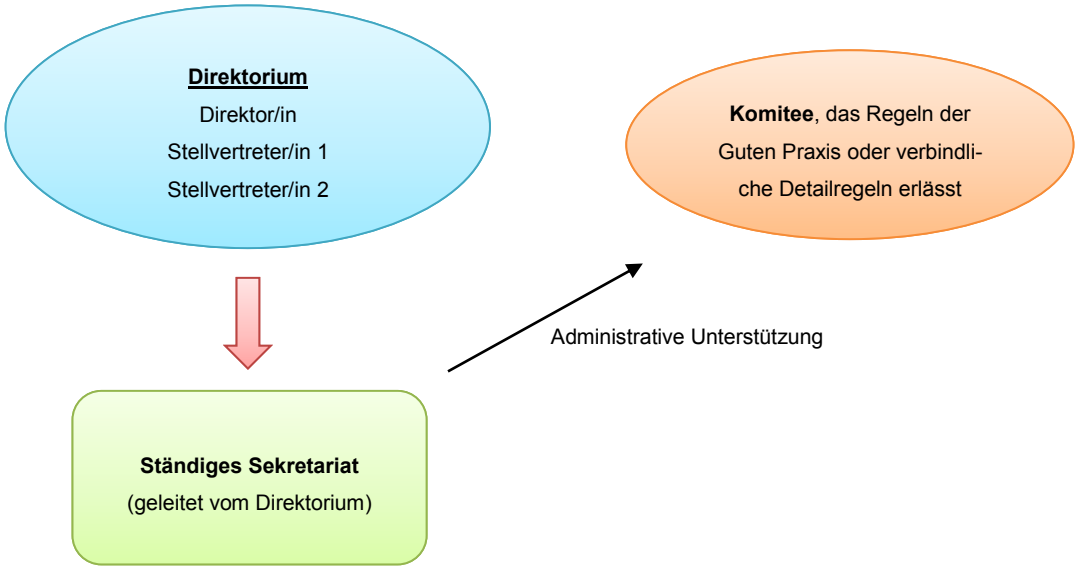
Die Aufgaben und Kompetenzen der Aufsichtsbehörde im Bereich des Datenschutzes und im Bereich des Öffentlichkeitsprinzips werden sich künftig womöglich noch stärker unterscheiden (Aufsicht mit Verfügungsbefugnis [DSG] gegenüber Schlichtungsbefugnis [Art. 13 ff. BGÖ]). Um nicht der bereits heute teilweise vertretenen Auffassung, die Organisation des EDÖB führe zu Interessenkonflikten und einer Schwächung des Öffentlichkeitsprinzips, Vorschub zu leisten, könnte in Betracht gezogen werden, dass je eine Stellvertreterin oder ein Stellvertreter die für den Datenschutz zuständige Abteilung bzw. die für das Öffentlichkeits-

---

[102] Siehe dazu den Bericht des Bundesrates zur Auslagerung und Steuerung von Bundesaufgaben vom 13. September 2006 (Corporate-Governance-Bericht), BBl 2006 8233 ff., insbesondere S. 8285 f.

[103] Siehe Corporate-Governance-Bericht des Bundesrates, BBl 2006 8233 ff., 8268 f.: «Die Organisationsform der Behördenkommission soll für jene Einheiten vorgesehen werden, die zur Erfüllung ihrer Aufgaben über ein gewisses Mass an Unabhängigkeit von der Politik bedürfen, deren rechtliche Verselbständigung jedoch weder als einzelne Einheiten (z.B. wegen fehlender Grösse) noch im Verbund mit andern Einheiten (z.B. wegen unerwünschter Interdependenzen oder fehlendem Synergiepotenzial) angezeigt ist.»

prinzip zuständige Abteilung leitet, nach dem Modell der Aufsichtsbehörde des Kantons Freiburg (Art. 29*a* des Gesetzes vom 25. November 1994 über den Datenschutz; SGF 17.1)[104]. Fälle von Konflikten zwischen dem Datenschutz und dem Öffentlichkeitsprinzip könnten dem Direktorium vorgelegt werden, das entscheiden würde, was im Einzelfall gilt.



b) Kollegialbehörde ohne Komitee

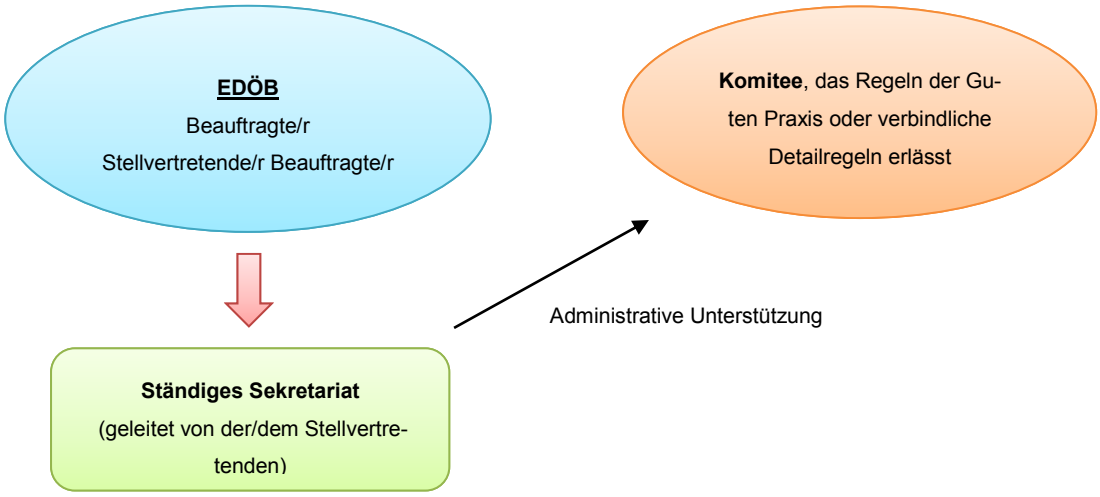
Wie bereits erwähnt, lehnt es eine *Minderheit der Begleitgruppe* ab, ein spezialisiertes Komitee einzusetzen, welches Regeln der Guten Praxis bzw. verbindliche Detailregeln zuhanden der Datenbearbeitenden erlässt oder genehmigt (siehe Ziff. 4.1.2 lit. b und Ziff. 4.10.2 lit. c). Diese Minderheit stellt sich auf den Standpunkt, dass damit nur zusätzlicher administrativer Aufwand verursacht und der Datenschutz letztlich geschwächt würde. Im Modell der Kollegialbehörde ohne Komitee würde die Erarbeitung und/oder Genehmigung der Regeln zur Konkretisierung des DSG von einem der drei Mitglieder des Direktoriums sichergestellt.

c) Beibehaltung einer/eines Beauftragten mit Komitee

Die Beibehaltung des geltenden Systems bietet den Vorteil, dass das Modell einfach sowie unbürokratisch ist und rasche Reaktionen der Aufsichtsbehörde gewährleistet. Das System ist bekannt und funktioniert. Die Organisationsform der Beauftragten bzw. des Beauftragten ist überdies keineswegs selten. Die meisten Schweizer Kantone haben sich für dieses System entschieden, ebenso wie zahlreiche europäische Länder wie Deutschland, Grossbritannien, Ungarn, Slowenien (unter der Bezeichnung «Beauftragter»), Spanien und Polen (unter der Bezeichnung «Direktor»).

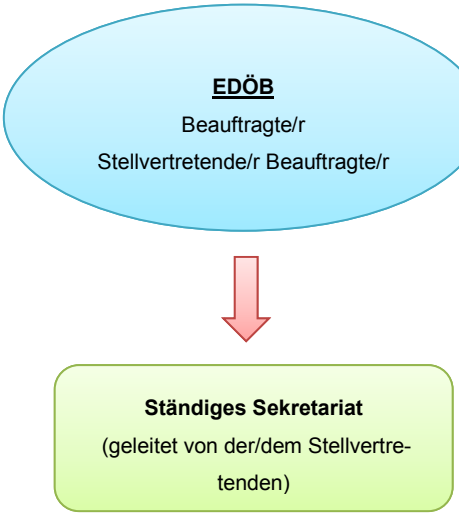
Um die Unabhängigkeit der Aufsichtsbehörde zu stärken, wird vorgeschlagen, dass die/der stellvertretende Beauftragte ebenso wie die/der Beauftragte vom Bundesrat gewählt wird, wobei die Wahl durch die Bundesversammlung zu genehmigen ist.

[104] Siehe für ein Organigramm: <http://www.fr.ch/atprd/de/pub/ueber_uns/organisation.htm>.



d) Beibehaltung einer/eines Beauftragten ohne Komitee

Wie bereits erwähnt, lehnt es eine *Minderheit der Begleitgruppe* ab, ein spezialisiertes Komitee einzusetzen, welches Regeln der Guten Praxis bzw. verbindliche Detailregeln zuhanden der Datenbearbeitenden erlässt oder genehmigt (siehe Ziff. 4.10.3 lit. b oben). Im Modell der/des Beauftragten ohne Komitee würde die Erarbeitung und/oder Genehmigung der Regeln zur Konkretisierung des DSG von der Aufsichtsbehörde selbst sichergestellt.



4.10.4 Wiederwahl und Amtsdauer

Die Begleitgruppe schlägt vor, die Anzahl der Amtszeiten der Mitglieder der Datenschutzaufsichtsbehörde – unabhängig vom Organisationsmodell – auf drei zu beschränken. Ihres Erachtens könnte dies zur Unabhängigkeit der Mitglieder der Aufsichtsbehörde beitragen. Zugleich würde dies Karrieremöglichkeiten eröffnen, was qualifizierte Personen zu einer Bewerbung veranlassen könnte.

4.10.5 Zusammenarbeit zwischen Aufsichtsbehörden auf nationaler und internationaler Ebene

Im Falle einer Ausdehnung des Geltungsbereichs des DSG auf Datenbearbeitungen durch kantonale Organe wäre es zweckmässig gewesen, die Zusammenarbeit zwischen der eidgenössischen Datenschutzaufsichtsbehörde und den kantonalen Aufsichtsstellen zu institutionalisieren und auszubauen. Da aber auf eine solche Ausdehnung verzichtet werden soll (vgl.

Ziff. 4.2.1 lit. a), scheint die derzeitige Situation, welche hauptsächlich auf einem freiwilligen, punktuellen und informellen Austausch beruht, beibehalten werden zu können.

Hingegen sollte die Einführung von Koordinationsregeln zwischen der eidgenössischen Datenschutzaufsichtsbehörde und den kantonalen Behörden geprüft werden, zum Beispiel im Fall von positiven Kompetenzkonflikten. Abzuklären ist ausserdem, ob Regeln für die Zusammenarbeit zwischen der eidgenössischen Datenschutzaufsichtsbehörde und den entsprechenden ausländischen Aufsichtsorganen angebracht wären.

4.10.6 Finanzierung

Für die Begleitgruppe stellt sich die Frage, wie die Aufgaben der Datenschutzaufsichtsbehörde inskünftig finanziert werden sollen, insbesondere da die Datenschutzaufsichtsbehörde mit der Stärkung und Erweiterung ihrer Kompetenzen (vgl. Ziff. 4.10.2) beträchtlich mehr Ressourcen als heute benötigen würde.

Eine *Mehrheit der Begleitgruppe* vertritt die Ansicht, dass der Datenschutzaufsichtsbehörde zwar mehr finanzielle Mittel zur Verfügung gestellt werden sollen. Allerdings soll die Finanzierung wie bisher über das ordentliche Budget bzw. die allgemeinen Steuereinnahmen des Bundes erfolgen.

Eine *Minderheit der Begleitgruppe* schlägt dagegen vor, als zusätzliches Finanzierungsmittel eine öffentliche Abgabe einzuführen. Dabei könnte für die Abgabepflicht eine ähnliche Regelung wie in Grossbritannien[105] vorgesehen werden, wonach die kommerzielle, elektronische Datenbearbeitung registrierungspflichtig gemacht und dafür (beispielsweise abhängig von der Unternehmensgrösse) eine Abgabe erhoben wird. Als Nachteile einer solchen Abgabepflicht werden von verschiedenen Mitgliedern der Begleitgruppe der hohe Verwaltungsaufwand, die schwierige Umsetzung im internationalen Kontext sowie die Möglichkeit der Abwälzung der Abgabe auf die Konsumenten angeführt. Ausserdem ist noch vertieft zu prüfen, ob für die Einführung einer solchen öffentlichen Abgabe eine verfassungsrechtliche Grundlage erforderlich ist. Dies hängt davon ab, ob die Abgabe als Steuer oder Kausalabgabe ausgestaltet wird. Für die Erhebung von Steuern bedarf der Bund grundsätzlich einer ausdrücklichen und spezifischen verfassungsrechtlichen Grundlage. Ohne ausdrückliche, spezifische Erhebungskompetenz in der Bundesverfassung, d.h. bloss gestützt auf eine Sachkompetenz, kann der Bund in der Regel nur Gebühren und Vorzugslasten (klassische Kausalabgaben), echte Lenkungsabgaben und Abgaben, die diesen nahekommen, erheben. Zentral für die Unterscheidung zwischen Steuern und Kausalabgaben ist das Kriterium der Zurechenbarkeit, d.h. es wird gefragt, ob bzw. inwiefern dem Abgabepflichtigen eine staatliche Gegenleistung zurechenbar ist. Eine Steuer liegt vor, wenn vom Abgabepflichtigen Abgaben erhoben werden, ohne dass ihm eine individuell zurechenbare staatliche Gegenleistung erbracht

---

[105] Das britische Modell basiert auf einer Registrationspflicht der Unternehmen. Der «Data Protection Act 1998» verpflichtet jeden «Data Controller» (insbesondere Unternehmen und Einzelunternehmen), sich bei der britischen Datenschutzaufsichtsbehörde ICO zu registrieren. Allerdings sind Ausnahmen von der Registrierungspflicht vorgesehen. Die Kosten der «Data Protection Registration» bemessen sich nach Grösse und Umsatz des Unternehmens. Für die meisten Unternehmen betragen die Kosten £ 35. Erst wenn gewisse Schwellenwerte (Umsatz höher als £ 25.9M und mehr als 249 Angestellte) überschritten werden, steigen die Kosten auf £ 500. Für staatliche Behörden mit mehr als 249 Angestellten betragen die Kosten ebenfalls £ 500. Vgl. dazu <http://ico.org.uk/for_organisations/data_protection/registration>.

wird (Voraussetzungslosigkeit der Abgabe).[106] Bei der Ausgestaltung einer öffentlichen Abgabe zur Finanzierung der Aufgaben der Datenschutzaufsicht stellen sich insbesondere die Fragen, für welche Tätigkeiten der Aufsichtsbehörde bzw. zu welchem Verwendungszweck die Abgabe erhoben werden und wie sich der Kreis der Abgabepflichtigen zusammensetzen soll.

Eine Abgaberegelung wie in Grossbritannien wäre vermutlich als Verwaltungsgebühr zu qualifizieren, die keine Grundlage in der Verfassung voraussetzt. Allerdings wäre die Verwaltungsgebühr durch das Kostendeckungs- und Äquivalenzprinzip begrenzt, d.h. sie dürfte insbesondere die Kosten des betreffenden Verwaltungszweigs für die Registrierung nicht überschreiten und könnte damit nicht zur Finanzierung der weiteren Aufgaben der Datenschutzaufsichtsbehörde beitragen. Von einer neuen verfassungsrechtlichen Grundlage könnte unter Umständen – analog zur Banken- und Privatversicherungsaufsicht – auch bei einer Aufsichtsgebühr abgesehen werden, wenn der Kreis der Abgabepflichtigen (z.B. kommerzielle, elektronische Datenbearbeitende) mit dem Kreis der Abgabebegünstigten übereinstimmt. Die Aufsichtsabgabe wäre dabei so zu bemessen, dass sie die Kosten der Aufsicht über die Abgabepflichtigen (z.B. kommerzielle, elektronische Datenbearbeitende) deckt. Die Kosten für die Aufsicht über die übrigen Datenbearbeitenden (z.B. nicht kommerzielle private Datenbearbeitende, Bundesorgane) könnten dagegen (ohne entsprechende verfassungsrechtliche Grundlage) nicht über eine solche Abgabe gedeckt werden. Ein solches System wäre in der praktischen Umsetzung sehr komplex und würde neuen personellen und finanziellen Aufwand generieren.

Ein Modell (wie z.B. in Spanien), wonach die Einkünfte aus den von der Datenschutzaufsichtsbehörde verhängten Bussen zur Finanzierung des Budgets herbeigezogen werden können, ist von der Begleitgruppe geprüft, aber abgelehnt worden. Zum einen steht noch nicht fest, inwieweit der Datenschutzaufsichtsbehörde Sanktionskompetenzen eingeräumt werden und ob damit überhaupt ausreichend finanzielle Mittel beschafft werden könnten (vgl. Ziff. 4.10.2). Zum anderen sind die Mitglieder der Begleitgruppe überwiegend der Ansicht, dass ein solches Vorgehen finanzpolitischen Grundsätzen widersprechen würde. Ausserdem soll nicht der Anschein erweckt werden, dass Sanktionen zum Zweck der Selbstfinanzierung ausgesprochen werden.

Um die Unabhängigkeit der Datenschutzaufsichtsbehörde zu stärken, schlägt die Begleitgruppe vor, der Datenschutzaufsichtsbehörde eine vergleichbare Budgetkompetenz wie der Eidgenössischen Finanzkontrolle einzuräumen.[107] Dies hätte zur Folge, dass das Budget der Datenschutzaufsichtsbehörde direkt dem Parlament (ohne Änderung durch den Bundesrat)

---

[106] Vgl. dazu ausführlich das Gutachten des Bundesamtes für Justiz vom 15. Juli 1999, in: VPB 2000, Nr. 25. In diesem Gutachten hat das BJ die Auffassung vertreten, dass «eine explizite und spezifische Verfassungsgrundlage für die Erhebung solcher Abgaben erforderlich ist, bei denen kein oder bloss ein zu schwacher Zurechnungszusammenhang zwischen dem Kreis der Abgabepflichtigen und dem Verwendungszweck der Abgabe vorhanden ist» (Ziff. A./III./1./b). Für die Erhebung von jährlichen, pauschal bemessenen Abgaben im Bereich der Banken- und Privatversicherungsaufsicht sowie der Unfallverhütung im Strassenverkehr ist das BJ zum Schluss gekommen, dass bei diesen Abgaben Kongruenz zwischen dem Kreis der Abgabepflichtigen und dem Kreis der Personen, denen die Abgabeverwendung als Gruppe zugute kommt, bestehe. Es erscheine deshalb als vertretbar, die Aufsichtsabgaben und den Unfallverhütungsbeitrag auf die materielle Sachkompetenz des Bundes in den betreffenden Aufgabenbereichen zu stützen und auf eine explizite und spezifische Verfassungsgrundlage für diese Abgaben zu verzichten.

[107] Vgl. Art. 2 Abs. 3 des Finanzkontrollgesetzes (FKG; SR 614.0).

unterbreitet würde.

4.11 Strafbestimmungen

Das DSG enthält mit den Art. 34 und 35 gegenwärtig zwei Strafbestimmungen. Des Weitern werden im Strafgesetzbuch in den Art. 179 ff. StGB strafbare Handlungen gegen den Geheim- oder Privatbereich festgelegt. Angesichts der technologischen Entwicklung (Drohnen, Google Glass, Dashcams usw.) ist zu prüfen, ob diese Vorschriften unverändert beibehalten oder verschärft werden sollen (z.B. indem die Tatbestände als Offizialdelikte gestaltet würden) oder ob neue Straftatbestände geschaffen werden sollen.

Ein *Teil der Mitglieder der Begleitgruppe* ist der Ansicht, im Strafgesetzbuch solle eine Bestimmung zum Identitätsmissbrauch eingeführt werden. Es wird vorgeschlagen, zunächst abzuwarten, ob der Nationalrat der Motion Comte 14.3288 «Identitätsmissbrauch. Eine strafbare Handlung für sich» Folge leisten wird. Der Bundesrat hatte die Ablehnung der Motion beantragt. Vom Ständerat ist die Motion jedoch am 12. Juni 2014 angenommen worden.[108]

4.12 Schlussbestimmungen

Die Bestimmungen zu den Regelungskompetenzen des Bundesrates (Art. 36 DSG) sowie zum Vollzug durch die Kantone (Art. 37 DSG) sind den Änderungen gemäss Ziff. 4.1 bis 4.11 anzupassen. Schliesslich sind für die vorgeschlagenen Neuerungen zum DSG Übergangsbestimmungen vorzusehen (vgl. Art. 38 DSG).

5. Erlassform und normatives Umfeld

Verfassungsrechtliche Grundlagen: Die Bundesverfassung enthält keine Bestimmung, die dem Bund ausdrücklich eine Kompetenz im Datenschutzbereich zuweist.[109] Hingegen schliessen verschiedene Bundeskompetenzen auch die Befugnis zum Erlass von Datenschutzregelungen ein. Im Privatrechtsbereich kann der Gesetzgeber sich insbesondere auf seine Gesetzgebungskompetenz auf dem Gebiet des Zivilrechts abstützen (Art. 122 BV).[110] Auf dem Gebiet des öffentlichen Rechts liegt die Regelungskompetenz des Bundes zum Erlass von Datenschutzbestimmungen, die auf Verwaltungsbehörden anwendbar sind, in der ihm gemäss Art. 173 Abs. 2 BV eingeräumten Organisationsgewalt. Für die kantonalen und

---

[108] Die Kommission für Rechtsfragen des Nationalrates (RK-NR) hat ihrem Rat am 17. Oktober 2014 mit 19 zu 1 Stimmen bei 3 Enthaltungen beantragt, die Motion Comte 14.3288 anzunehmen.

[109] Art. 13 Abs. 2 BV sieht zwar den Anspruch jeder Person auf Schutz vor Missbrauch ihrer persönlichen Daten vor. Es handelt sich hier aber um ein Grundrecht, das dem Bund keine Zuständigkeiten überträgt. Eine Revision dieser Verfassungsbestimmung ist im Übrigen Gegenstand der parlamentarischen Initiative Vischer 14.413 «Grundrecht auf informationelle Selbstbestimmung», welche Art. 13 Abs. 2 BV dahingehend ändern will, «dass der Datenschutz statt eines Missbrauchsschutzes zu einem Grundrecht auf informationelle Selbstbestimmung wird». Die Staatspolitische Kommission des Nationalrates (SPK-NR) hat der parlamentarischen Initiative am 29. August 2014 Folge gegeben.

[110] Weitere relevante Verfassungsnormen sind z.B. Art. 95 BV (Gesetzgebungskompetenz des Bundes bezüglich der Ausübung privatwirtschaftlicher Erwerbstätigkeit) sowie Art. 97 BV (Gesetzgebungskompetenz des Bundes zum Schutz der Konsumentinnen und Konsumenten).

kommunalen Verwaltungen kann der Bund dagegen grundsätzlich keine Datenschutzbestimmungen erlassen[111].[112] Die in Ziff. 4 des vorliegenden Normkonzepts enthaltenen Massnahmen können auf die bestehenden verfassungsrechtlichen Grundlagen abgestützt werden. Eine Teilrevision der Verfassung wäre allerdings notwendig,

- falls die Kompetenzverteilung zwischen Bund und Kantonen im Bereich des Datenschutzes angepasst und der Anwendungsbereich des DSG auf die kantonalen Organe ausgeweitet werden sollte (vgl. Ziff. 4.2.1 lit. a, wo jedoch vorgeschlagen wird, auf eine solche Massnahme zu verzichten); sowie
- falls eine öffentliche Abgabe zur Finanzierung der Aufgaben der Datenschutzaufsichtsbehörde eingeführt und als Steuer ausgestaltet werden sollte (vgl. Ziff. 4.10.6).

Regelung auf Gesetzes- und Verordnungsstufe: Mit den in Ziff. 4 vorgeschlagenen Anpassungen des Datenschutzrechts an die technologischen und gesellschaftlichen Entwicklungen soll hauptsächlich das DSG revidiert werden. Da die Änderungen voraussichtlich mehr als die Hälfte der bestehenden Artikel des DSG betreffen, erscheint eine Totalrevision des Erlasses sinnvoll.

Eine Revision des DSG wird entsprechende Anpassungen des dazugehörigen Verordnungsrechts (VDSG, VDSZ) erforderlich machen. Möglicherweise sind auch in den allgemeinen Verfahrensgesetzen (ZPO, VwVG, VGG, BGG) einzelne Änderungen notwendig. Ausserdem hat eine Revision des DSG zur Konsequenz, dass überprüft werden muss, ob die zahlreichen bereichsspezifischen Datenbestimmungen des öffentlichen Rechts (vgl. Ziff. 4.1 und Ziff. 4.9.1) die neuen Vorgaben des DSG erfüllen. Schliesslich soll untersucht werden, inwiefern bezüglich der strafrechtlichen Bestimmungen zum Schutz der Geheim- und Privatsphäre (insbesondere Art. 179 ff. StGB) gesetzgeberischer Handlungsbedarf besteht (vgl. Ziff. 4.11)

Internationales Recht: Die Revisionsarbeiten zum DSG sollen die Reformentwicklungen beim Europarat und in der EU im Bereich des Datenschutzes berücksichtigen und insbesondere die notwendigen Voraussetzungen für eine allfällige Ratifizierung der modernisierten Datenschutzkonvention SEV 108 schaffen (vgl. dazu Ziff. 2).

6. Grobstruktur der Regelung

Es wird vorgeschlagen, die Struktur des DSG grundsätzlich beizubehalten und soweit nötig zu ergänzen (vgl. Ziff. 4). Dabei würde das neue Gesetz wahrscheinlich mehr Artikel als bisher umfassen:

- Bestimmungen betreffend Zweck, Geltungsbereich und Begriffe
- Allgemeine Datenschutzbestimmungen, die sowohl für die Organe des Bundes als auch für private Datenbearbeitende gelten (Datenbearbeitungsgrundsätze, Rechte der betroffenen Personen, grenzüberschreitende Datenbekanntgabe, Zertifizierungsverfahren)
- Besondere Bestimmungen für die Datenbearbeitung durch Privatpersonen (persönlichkeitsverletzende Tatbestände, Rechtfertigungsgründe, Verfahrensbestimmungen)
- Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane (insbesondere

---

[111] Eine Ausnahme bilden die Bereiche, in welchen den Kantonen die Umsetzung des Bundesrechts übertragen ist (vgl. Art. 37 DSG).

[112] Vgl. zum Ganzen die Botschaft des Bundesrates vom 19. Februar 2003 zur Änderung des Bundesgesetzes über den Datenschutz (DSG), BBl 2003 2101, 2151 f.

Erfordernis einer genügenden Rechtsgrundlage für die Datenbearbeitung, spezifische Bearbeitungsvorschriften, Verfahrensbestimmungen)

- Bestimmungen zu Organisation und Aufgaben der Datenschutzaufsichtsbehörde
- Bestimmungen zum Aufsichtsverfahren
- Bestimmungen zum alternativen Streitbeilegungsverfahren sowie zur Einrichtung einer Mediationsstelle
- Bestimmungen zum Komitee, welches für den Erlass bzw. die Genehmigung von detaillierten Regeln zur Anwendung des DSG bzw. Regeln der Guten Praxis zuständig ist
- Strafbestimmungen
- Schlussbestimmungen (Vollzug, Übergangsbestimmungen)

7. Normative Dichte (Detaillierungsgrad)

Das Datenschutzgesetz ist als Querschnittsgesetz weitgehend technologieneutral ausgestaltet. Es enthält vorwiegend Grundsatzregelungen, die für jeden Umgang mit Personendaten gelten. Es soll daher keinen zu hohen Detaillierungs- und Spezialisierungsgrad aufweisen. Insbesondere die allgemeinen Datenbearbeitungsgrundsätze sind hinreichend abstrakt zu halten, um den rechtsanwendenden Behörden ausreichend Spielraum für die sachgerechte Beurteilung von Einzelfällen aus den unterschiedlichsten Sachbereichen einzuräumen. Daher wird vorgeschlagen, die bisherige normative Dichte des DSG beizubehalten.

Um die Durchsetzung des Datenschutzrechts zu verbessern und die Rechtssicherheit im Umgang mit Personendaten zu erhöhen, wird eine weitere Konkretisierung des Datenschutzrechts auf einer anderen Regelungsstufe indessen als notwendig erachtet. Zu diesem Zweck wird in Ziff. 4.1.2 lit. b ein möglichst flexibler und praxisnaher Ansatz gewählt: Es wird vorgesehen, das DSG durch detaillierte Handlungsanweisungen bzw. Anwendungsvorgaben zu präzisieren. Dabei ist eine Mehrheit der Begleitgruppe der Ansicht, dass dies durch nicht verbindliche Regeln der Guten Praxis erfolgen soll. Diese Regeln sollen durch ein spezialisiertes Expertenkomitee erlassen bzw. genehmigt werden (vgl. Ziff. 4.1.2 lit. b, 4.10.2 lit. c sowie 4.10.3).

8. Zeitplan

Der Bundesrat hat das EJPD beauftragt, bis Ende 2014 Vorschläge zum weiteren Vorgehen für eine allfällige Revision des DSG zu unterbreiten. Zu diesem Zweck wird das BJ – unter Berücksichtigung des vorliegenden Normkonzepts – ein Aussprachepapier an den Bundesrat ausarbeiten. Da die CAHDATA ihre Arbeiten zum Modernisierungsentwurf der Datenschutzkonvention SEV 108 voraussichtlich im Dezember 2014 abschliessen wird (vgl. Ziff. 2), könnte es sinnvoll sein, dem Bundesrat das Aussprachepapier erst anfangs 2015 zu unterbreiten, so dass die Resultate der CAHDATA in die Entscheidfindung miteinbezogen werden können.

Im Aussprachepapier sollen inhaltliche Grundsatzfragen sowie der Kalender für das weitere Vorgehen thematisiert werden. Zu Letzterem kommen grundsätzlich drei unterschiedliche Varianten in Betracht:

- Mit den Revisionsarbeiten zum DSG wird zugewartet, bis die europäischen Reformen zum Datenschutzrecht abgeschlossen sind.
- Das EJPD wird mit der Ausarbeitung eines Vorentwurfs zur Revision des DSG beauftragt, ohne den Abschluss der europäischen Datenschutzrechtsreformen abzuwarten.

- Das EJPD wird mit dem Vorentwurf einer Revision des DSG beauftragt, wobei für dessen Ausarbeitung eine genügend lange Frist (z.B. zwei Jahre) eingeräumt wird, so dass die notwendigen Anpassungen des schweizerischen Datenschutzrechts für eine Ratifizierung der modernisierten Datenschutzkonvention SEV 108 möglichst bekannt sind und berücksichtigt werden können.

Anhang: Stellungnahmen einzelner Mitglieder der Begleitgruppe

economiesuisse

per Mail
Frau Monique Cossali Sauvain
Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz (BJ)
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik
Bundesrain 20
3003 Bern

23. September 2014

Stellungnahme economomiesuisse zum Normkonzept Revision Datenschutzgesetz (DSG)

Sehr geehrte Frau Cossali

Sie haben uns eingeladen, zum Normkonzept zur Revision Datenschutzgesetz (DSG) (Fassung vom 10. September 2014) Stellung zu nehmen, falls wir dies wünschen. Für die gebotene Gelegenheit zur Meinungsäusserung danken wir Ihnen bestens und machen nachfolgend gerne davon Gebrauch. Zu diesem Zeitpunkt beschränken wir uns dabei auf die wichtigsten Punkte mit grundlegendem Charakter und ohne einen Anspruch auf Vollständigkeit zu erheben.

Ein funktionierender Datenschutz ist aus Sicht der Wirtschaft wichtig

Die Diskussion über den Datenschutz ist vor dem Hintergrund des technologischen Wandels angebracht und muss geführt werden. **Für die Wirtschaft ist ein angemessenes und wirksames Datenschutzgesetz wichtig. Massvolle und klare Bestimmungen lassen Raum für die wirtschaftliche Entfaltung und dienen der Rechts- und Investitionssicherheit. Sie ermöglichen die Entwicklung und den Einsatz von innovativen digitalen Produkten und industriellen Anwendungen.**

Darüber hinaus sind Akzeptanz und Vertrauen der Nutzer in den Datenschutz eine zentrale Voraussetzung für die Fortentwicklung der immer wichtiger werdenden digitalen Wirtschaft und die Nutzung des damit verbundenen wirtschaftlichen Potenzials. Der überwältigende Teil der Unternehmen hat denn auch ein grosses Interesse daran, dass datenschutzrechtliche Vorschriften eingehalten werden – nicht nur im eigenen Haus, sondern auch durch die anderen Wettbewerber. Andernfalls drohen massive Reputationsschäden, die nicht nur die unmittelbar betroffenen Unternehmen belasten, sondern gleich ganze Branchen in Mitleidenschaft ziehen können. Ausserdem besteht das Risiko, dass nicht datenschutzkonforme Produkte, Dienstleistungen und ganze Geschäftsmodelle nachträglich verboten werden und damit bereits getätigte Investitionen verloren gehen.

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

Intelligente Datenschutzvorschriften, die ein gutes Datenschutzniveau bieten, sind für die Unternehmen und für den Wirtschaftsstandort Schweiz ein Vorteil. Überschiessende und im Geschäftsalltag nicht praktikable Regulierungen wirken sich hingegen innovationshemmend aus und können der Wettbewerbsfähigkeit von Unternehmen im internationalen Umfeld schaden. Sie treffen ebenso die Nutzer, die nicht von neuen Produkten und Dienstleistungen profitieren können. Nicht umsonst heisst es denn auch in der Botschaft zum geltenden DSG, dass die durch die immer besseren Technologien ermöglichte Entwicklung nicht verhindert oder eingeschränkt werden soll (Bundesrat / BBl 1988 II 417). Diese Feststellung gilt uneingeschränkt auch für die Gegenwart.

Bei einer geplanten DSG-Revision ist auch zu beachten, dass beim Datenschutzrecht, das eine Konkretisierung des Grundrechts zum Schutz auf Privatsphäre (Art. 13 BV) darstellt, der Schutzaspekt im Verhältnis *zwischen Staat und Bürger* die höchste Bedeutung ist. Demgegenüber ist das Verhältnis *zwischen Privaten* vom Grundsatz der Privatautonomie geprägt, weshalb in diesem Bereich übermässige Datenschutzregulierungen besonders problematisch und rechtfertigungsbedürftig sind und nur mit Zurückhaltung erlassen werden dürfen. Der Nutzen, den die sich verbessernden Informationstechnologien bieten, soll nicht leichtfertigt geopfert werden. Jeder Einzelne soll im Privatbereich grundsätzlich selbst entscheiden können, ob er ein bestimmtes (allenfalls mit einer Bekanntgabe gewisser Daten verbundenes) Angebot nutzen möchte oder nicht. Als mündiger Bürger ist er dazu auch ohne weiteres in der Lage.

Weiter gilt es auch im Blick zu behalten, dass Datenschutzrecht nicht Konsumentenrecht ist. Die beiden Bereiche verfolgen unterschiedliche Schutzzwecke und sollen folglich nicht vermischt werden: Während das erste nämlich auf den Grundrechtschutz ausgerichtet ist; bezieht sich das zweite auf kommerzielle Beziehungen zwischen Anbietern und Abnehmern. Daher haben etwa Instrumente wie Sammelklagen oder vom allgemeinen haftpflichtrechtlichen Regime abweichende Schadenersatzklagen etc. keinen Platz im DSG.

<u>Grundsätzliche Bemerkungen zum gesellschaftspolitischen Umfeld und zum Revisionsprojekt DSG</u>

In den letzten Jahren ist die Präsenz des Themas Datenschutz in den Medien und der öffentlichen Wahrnehmung gestiegen, und es hat in der politischen Agenda an Bedeutung gewonnen. Das hat verschiedene Gründe: Zum einen haben spektakuläre Überwachungs- und Spionageaffairen und das Bekanntwerden schwerwiegender Eingriffe in die Privatsphäre der Bürger durch geheimdienstliche Behörden die Sensibilität für den Datenschutz erhöht (obschon es hier eigentlich nicht um Probleme des Datenschutzes sondern vielmehr der Datensicherheit geht). Sie haben teilweise auch ein diffuses Unbehagen gegenüber den Möglichkeiten, die mit den neuen Informations- und Kommunikationstechnologien einhergehen, hervorgerufen. Dieser Eindruck wird zusätzlich verstärkt durch Meldungen über Hackerattacken und Datendiebstahl bzw. -verluste bei einzelnen grossen in- und ausländischen Unternehmen. Weiter hat mit den verbesserten Bearbeitungsmöglichkeiten und höheren Speicherkapazitäten die Menge der verarbeiteten Daten zugenommen. Gleichzeitig entstehen zahlreiche neue internetbasierte Geschäftsmodelle und Anwendungen, und die Sozialen Medien erleben einen regelrechten Boom. Mit diesen Entwicklungen gehen auch Fragen betreffend den (zu leichtfertigen) Umgang mit persönlichen Daten einher. Zudem ergingen einige vielbeachtete letztinstanzliche Grundsatzentscheide zu relevanten datenschutzrechtlichen Fragen, die eine Handvoll besonders technologienaher Unternehmen betrafen (vgl. die Bundesgerichtsentscheide betreffend Logistep und Google Street View oder das EuGH-Google-Urteil betreffend Löschungsrecht).

So notwendig die Diskussion um den Datenschutz in diesem sich verändernden gesellschaftlich-technologischen Umfeld ist, so essentiell ist es mit Blick auf eine mögliche Revision des DSG, dass

das bewährte heutige Datenschutzregime nicht ohne Notwendigkeit und zeitliche Dringlichkeit über den Haufen geworfen wird; vor allem Im Privatbereich. **Bevor eine Revision an die Hand genommen wird, müssen zwingend der tatsächliche Handlungsbedarf anhand von Fakten und empirischen Untersuchungen konkret ausgewiesen sowie das angestrebte Ziel klar definiert sein. Es ist transparent und detailliert aufzuzeigen, inwiefern genau die geltenden Regelungen ihre Wirkung verfehlen und ob bzw. mit welchen Mitteln ein allfälliger Missstand effektiv behoben werden kann.** Nur so lassen sich die verschiedenen Alternativen (inklusive eines „Nichtstuns“) abschätzen. Und nur so lassen sich die Interessen gegeneinander abwägen und ausgleichen, und lässt sich die Verhältnismässigkeit von neu vorgeschlagenen Vorschriften überprüfen. Diese Kriterien sind beim laufenden Revisionsprojekt jedoch nicht erfüllt.

Darüber hinaus darf eine Revision auch nicht nur auf einige wenige vielbeachtete Einzelfälle bzw. auf eine Branche oder gar ein paar wenige internationale Konzerne gemünzt sein. Denn **das DSG gilt für die gesamte Wirtschaft – für alle Industriezweige, grosse und kleine, national wie international tätige Unternehmen. Durch unpassende Regulierungen, die ihr eigentliches Ziel verfehlen oder darüber hinausschiessen, werden alle Unternehmen getroffen. Deshalb muss sich eine Revision auf die wesentlichen Punkte beschränken auf einer konkreten und detaillierten Risikoanalyse aufbauen. Dabei sind die angeblichen Lücken genau aufzuzeigen, und es ist zu benennen, was die Folge einer Nichtregelung im Privatbereich wäre.**

Fehlender Handlungsbedarf für eine umfassende DSG-Revision

Der Bedarf für eine umfassende DSG-Revision ist nach wie vor nicht konkret bzw. unzureichend ausgewiesen. Nur sechs Jahre nach der letzten Revision braucht es für den Privatbereich keine neuerliche Überarbeitung des Gesetzes, die über formelle Anpassungen wie z.B. eine übersichtlichere Darstellung oder allenfalls einzelne punktuelle Verbesserungen hinausgeht. Allein der Umstand, dass sich das technologische und gesellschaftliche Umfeld weiterentwickelt, ist jedenfalls kein Anlass, von einem funktionierenden System abzuweichen. Das DSG wurde bewusst technologieneutral ausgestaltet, und es hat sich seither bestens bewährt. economiesuisse lehnt daher eine Revision in der vorgesehenen Form ab. Insbesondere sehen wir nicht, wo und inwiefern beim geltenden Recht Mängel bestehen sollten, die einen so weitgehenden gesetzgeberischen Eingriff erforderlich machen würden.

Ziel der 2010 im Auftrag des Bundsamts für Justiz (BJ) durchgeführten Evaluation des DSG war es, das DSG auf seine Wirksamkeit hin zu überprüfen. Im Vordergrund standen erstens die Bekanntheit und die Durchsetzungsmechanismen des Gesetzes einerseits sowie die Stellung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) andererseits. Der Schlussbericht zur Evaluation vom 9. Dezember 2011 weist zusammenfassend auf die technologische Entwicklung als Herausforderung hin (S. I), er stellt aber keine schweren Mängel fest. Vielmehr hält als Gesamtbilanz fest, dass der EDÖB seinen gesetzlichen Auftrag erfülle und dabei eine hohe Wirksamkeit erziele und seine Aufsichtstätigkeit im Einzelfall wirksam sei: In der Mehrheit der Sachverhaltsabklärungen stelle er nur geringfügige Probleme fest, welche die Datenbearbeiter anschliessend freiwillig behöben. Spreche er bei grösseren Mängeln Empfehlungen aus, würden diese grossmehrheitlich umgesetzt, entweder direkt oder nach einem Gerichtsurteil. Bei Bearbeitungen, die intransparent sind oder im Ausland erfolgen, stosse die Aufsicht an Grenzen. Zudem mache der EDÖB heute aus Ressourcengründen keine stichprobenartigen Kontrollen, was der Breitenwirkung der Aufsicht abträglich sei. Mit einer präventiven Wirkung auf andere Datenbearbeiter sei aber insofern zu rechnen, als bekannt werdende Missstände öffentliches Interesse erregen (S. III f.). Es gebe auch deutliche Hinweise, dass das Risiko eines Imageschadens das Verhalten zugunsten des Datenschutzes beeinflusst (S. II). Auch die Beratungs- und Informationstätigkeit würden von den

Bearbeitern insgesamt als nützlich, praxisnah und konstruktiv bewertet (S. III f.). Bezüglich des Verhaltens der Nutzer hält der Bericht fest, dass die Betroffenen die neuen Möglichkeiten der Informationsgesellschaft mehrheitlich begrüssten (S. 66). Sie erachteten Datenschutz zwar als wichtig, schützten sich aber nicht immer konsequent selbst und gäben persönliche Daten bisweilen grosszügig preis. Betreffend die Schutzrechte gelangt der Bericht zum Schluss, dass die im DSG verankerten Durchsetzungsrechte der Betroffenen im internationalen Rechtsvergleich gut ausgebaut seien sowie dass Betroffene den Rechtsweg selten beschritten (S. II). Das Fazit des Berichts lautet: Vom DSG gehen klare Wirkungen zugunsten des Datenschutzes aus. Gleichzeitig sind die Wirkungen des EDÖB in verschiedener Hinsicht begrenzt und die Betroffenen machen wenig Gebrauch von den vorhandenen Durchsetzungsrechten (S. IV). Über die Gründe hierfür kann im Bericht nur spekuliert werden: Als mögliche Erklärung wird „erstens die vermutlich geringe Bekanntheit der Durchsetzungsrechte und des Rechtswegs sowie das geringe Wissen über die Anwendung dieser Rechte" genannt. Und zweitens „dürfte aus Sicht der Betroffenen ein vergleichsweise beträchtlicher Aufwand einer Klage einem diffusen und nicht gesicherten Nutzen gegenüberstehen" (S. II f.).

Aus dem Bericht des Bundesrates vom 9. Dezember 2011 zur Evaluation des DSG drängt sich kein dringender Handlungsbedarf auf, weder in inhaltlicher noch zeitlicher Hinsicht. Insbesondere lässt sich aus dem Papier nicht herleiten, dass das DSG seine bzw. die gewünschte Schutzwirkung nicht entfalte. Ebenso wenig legt es nahe, dass etwa die Durchsetzungsrechte oder die Kompetenzen der Aufsichtsbehörde zu schwach wären und daher ausgebaut werden sollten oder gar müssten. Vielmehr hält der Bericht fest, dass es in einem weiteren Schritt Aufgabe der Politik sei zu entscheiden, ob eine umfassende Diskussion über den Datenschutz geführt werden soll und welches das gewünschte Schutzniveau des DSG sein solle (S. IV, S. 215). So werden im Bericht denn auch ausdrücklich nicht Empfehlungen ausgesprochen, sondern mögliche Handlungsoptionen angedacht. Diese (teilweise sehr einschneidenden) Optionen haben „eher der Charakter von Gedankenanstössen als derjenige eines Arbeitspapiers im Hinblick auf die Formulierung im Einzelnen analysierter Vorschläge" (S. 215, 217).

economiesuisse fordert, dass keine umfassende DSG-Revision wie die geplante in Angriff genommen wird, ohne dass angebliche Missstände unter dem geltenden DSG klar belegt sind. Hierbei muss auf Fakten abgestellt werden. Gesetzgeberischer Aktivismus, getrieben von einem unbestimmten Misstrauen gegenüber dem veränderten technologischen Umfeld und ausgehend von Stimmungen oder blosse Vermutungen, ist verfehlt. So kann etwa aus der Tatsache, dass die Nutzer selten den Rechtsweg beanspruchen, keineswegs automatisch auf Defizite des DSG geschlossen werden. Die geringe Beanspruchung der Gerichte sehen wir im Gegenteil als Hinweis darauf, dass das heutige Datenschutzsystem seinen Zweck erfüllt. So lieferten denn auch etwa die Fälle Logistep, Google Streetview oder Moneyhouse – die gerne als Beispiele für die mit den neuen Technologien verbundenen Problematiken angeführt werden – keinerlei Hinweise darauf, dass im geltenden Recht etwa die Klagerechte zu schwach ausgestaltet wären, Beweisschwierigkeiten bestünden, die Kompetenzen des EDÖB zu wenig weit reichten oder Sanktionsmöglichkeiten fehlten. Vielmehr ging es in diesen Fällen jeweils um Auslegungsfragen des DSG, in denen die angerufenen Gerichte Klarheit schafften.

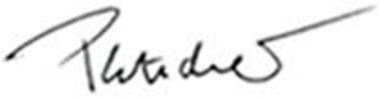
<u>Anpassung an internationale Bestrebungen (EU/Europarat) nur sofern für Marktzugang zwingend</u>

Das durch das geltende DSG garantierte Schutzniveau ist im internationalen Vergleich bereits hoch; eine Verschärfung insbesondere im Privatbereich ist unnötig. Ein überzogenes, „veradministriertes" Datenschutzrecht würde die Schweiz global gesehen ins Hintertreffen bringen. Dabei darf sich der Vergleich nicht allein an Europa orientieren, sondern der Blick ist darüber hinaus insbesondere auch auf die USA und Asien zu richten. Ein im Verhältnis zur EU schlank

ausgestaltetes, „smartes“ Datenschutzrecht ist ein willkommener Wettbewerbsvorteil für die Schweizer Wirtschaft.

Wenn überhaupt, besteht Handlungsbedarf aus Sicht von economiesuisse nur für den Fall und insoweit, als durch die Revisionen auf europäischer Ebene der Marktzugang zur EU betroffen ist. Bevor das Schweizer Recht erneut revidiert wird, sollten unbedingt zuerst die Resultate der laufenden Entwicklungen in der EU und im Europarat abgewartet werden. Eine allfällige Anpassung an das europäische Recht bzw. Umsetzung ins nationale Recht soll schliesslich nur dort erfolgen, wo dies unter dem Gesichtspunkt des Marktzugangs zwingend notwendig ist. Dazu muss bei jeder vorgeschlagenen Änderung nachvollziehbar sein, welches das unbedingte gesetzgeberische Minimum ist, um die Gleichwertigkeit mit dem europäischen Datenschutzstandard zu erfüllen. Hierbei ist zu bedenken, dass es keiner absoluten Gleichwertigkeit bedarf (vgl. die Safe-Harbor-Lösungen im Verhältnis CH/EU-USA). Der Schweizer Gesetzgeber darf auf keinen Fall überhastet und ohne ausgewiesene Notwendigkeit übertriebene Regelungen ungeprüft aus dem europäischen Umfeld übernehmen. Der vorhandene Spielraum ist weitestmöglich auszunützen.

Freundliche Grüsse
economiesuisse



Thomas Pletscher
Mitglied der Geschäftsleitung

Dr. Marlis Henze
Wissenschaftliche Mitarbeiterin

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

Aktennotiz

Geht an Bundesam für Justiz, Frau Monique Cossali, Leiterin der Belgeitgruppe DSG

Bern, 6. Oktober 2014 sgv-Kl

Stellungnahme des sgv zum Normkonzept zur Revision des Datenschutzgesetzes (DSG) (Version vom 10.9.2014)

Die vorliegende Stellungnahme bezieht sich auf das Normkonzept vom 10. September 2014 und erhebt keinen Anspruch auf Vollständigkeit. Sie gibt lediglich die Position des sgv in den wichtigsten Punkten wieder.

Grundsätzliche Bemerkungen

Die letzte grössere Revision des DSG liegt 6 Jahre zurück. Nach Ansicht des sgv ist es verfrüht, an den eben erst geschaffenen Grundlagen zu rütteln. Eine Revision des DSG rechtfertigt sich derzeit nicht. Zuerst sollen die Ergebnisse der Diskussionen in der EU und im Europarat abgewartet und dann allenfalls notwendige Anpassungen des DSG vorgenommen werden.

Aus dem Bericht des Bundesrates vom 9. Dezember 2011 wird nicht klar ersichtlich, wo genau eine Revision des DSG ansetzen soll. Ziel des Berichts war es gemäss Bundesrat, „das Datenschutzgesetz auf seine Wirksamkeit hin zu überprüfen. Im Vordergrund der Untersuchung standen die Bekanntheit des Gesetzes und seine Durchsetzungsmechanismen einerseits sowie die Stellung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) andererseits“. Im Bericht wird festgehalten, dass die technologischen Entwicklungen das DSG herausfordern. Zudem würde es immer schwieriger, die Kontrolle über einmal bekannt gegebene Daten zu behalten. Aufgrund der Ergebnisse der Evaluation ist der Bundesrat der Auffassung, dass zu prüfen ist, inwieweit und in welcher Weise die Datenschutzgesetzgebung anzupassen ist, um den rasanten technologischen und gesellschaftlichen Entwicklungen Rechnung zu tragen. Aus dem Bericht wird klar, dass der EDÖB zusätzliche Ressourcen geltend macht.

Der Schweizerische Gewerbeverband sgv ist der Auffassung, dass die Öffentlichkeit gut informiert ist. Dafür sorgen nicht nur zahlreiche Publikationen von Konsumentenorganisationen, sondern z.B. auch die Webseite des EDÖB, von der sich jedermann nützliche Informationen zur Rechtslage herunterladen kann. Die Diskussion um social media und den Schutz der Persönlichkeit gegen den Missbrauch von grundsätzlich frei zugänglichen Daten ist berechtigt und notwendig. Sie darf aber nicht zum Aufbau einer weiteren Bürokratie führen.

Stellungnahme zu den Eckwerten des Normkonzepts (contenu essentiel de la révision)

4.1 Concept et mise en oeuvre

Der sgv unterstützt die Stossrichtung, dass das Datenschutzgesetz technologieneutral ist und sich auf die grundlegenden Prinzipien fokussiert. Da der Datenschutz sehr unterschiedliche Anforderungen haben kann, macht es Sinn, weiterhin sowohl ein allgemeines DSG als auch die spezialgesetzlichen Regelungen zu haben.

Allein aus der Tatsache, dass heute betroffene Personen ihre Rechte gegenüber Datenbearbeitern nur selten beanspruchen, nur wenige Betroffene Klage einreichen und Prozesse über datenschutzrechtliche Fragen führen, ist kein hinreichender Grund zur Stärkung der Kontrollbehörde. Die relativ geringe Zahl gerichtlicher Verfahren kann ebenso gut mit einem von der Öffentlichkeit insgesamt als

befriedigend empfundenen System erklärt werden. Dass heute die Nachfrage danach so klein ist, ist ein deutliches Zeichen dafür, dass kein Handlungsbedarf besteht. Eine Stärkung des Datenschutzbeauftragten drängt sich aus Sicht des sgv im heutigen Zeitpunkt nicht auf. Neue gesetzliche Vorschriften sind nicht notwendig. Ein wichtiger Grundstein für den wirtschaftlichen Erfolg in der Schweiz ist die Wirtschaftsfreiheit. Unnötige, neue Einschränkungen - in welchem Bereich auch immer - sind zu vermeiden. Der bestehende Datenschutz hat sich bewährt. Die Wirtschaft sieht sich einer starken, mündigen Abnehmer- und Konsumentenschaft gegenüber, die ihren Ansprüchen schon jetzt durchaus Gehör zu verschaffen weiss. Zusätzliche Kontrollgremien sind nach Ansicht des sgv nicht nötig.

4.2 Champ d'application et définitions

Der sgv ist der Auffassung, dass sich die heute dualistische Verantwortung von Bund und Kantonen in der Datenschutzgesetzgebung bewährt hat. Eine Mehrheit der Begleitgruppe schlägt das Auswirkungsprinzip vor. Das Datenschutzrecht würde damit auch Anwendung auf Sachverhalte finden, die sich im Ausland zutragen, aber die in einem wesentlichen Rahmen Auswirkungen auf die Schweiz haben. Der sgv lehnt diese Position ab und unterstützt das Territorialitätsprinzip, da sich doch zu einem wesentlichen Zusatzaufwand bei international tätigen Firmen führen könnten. Zudem ist die Durchsetzbarkeit in der Praxis fraglich.

4.3 Principes généraux de protection des données personelles

Im Normkonzept wird die Stärkung der Informationspflicht des Datenbearbeiters gefordert. Bereits heute gibt es das Auskunftsrecht. Dieses wird – wie im Bericht festgestellt – eher zurückhaltend genutzt. Eine generelle Informationspflicht für jegliches Bearbeiten von Daten ist unverhältnismässig.

Das dem Obligationenrecht zugrundeliegende Zug-um-Zug Geschäft (Ware gegen Barzahlung) wird tendenziell an Bedeutung verlieren. Kann die Bezahlung nicht mehr Zug um Zug abgewickelt werden, so übernimmt notwendigerweise eine der involvierten Parteien das Risiko der Vorleistung und damit das Risiko eines Zahlungsausfalls. Zu den involvierten Parteien können nicht nur der Lieferant gehören, sondern auch aussenstehende Finanzierer (Leasinggeber, Kreditkartenunternehmen). Für den gewerblichen Alltag ist der einfache Zugang zu gesicherten Daten (z.B. zu Bonitätsprüfungen) deshalb von zentraler Bedeutung. Zahlreiche Lieferanten, welche täglich Waren gegen Rechnung liefern, erleiden in der Schweiz Jahr für Jahr hohe Verluste. Schon allein die amtlich erfassten, jährlichen Forderungsausfälle belaufen sich auf Milliarden. Die Betreibungs- und Konkursstatistik des BFS weist für die Zeit zwischen 2008 und 2013 Konkursverluste von mehr als 2 Mia pro Jahr aus. Zahlenmässig werden nur Ausfälle aus den durchgeführten Konkursverfahren erfasst. Weitaus grössere Verluste resultieren aus den mangels Aktiven eingestellten Konkursen (ca. 50 % aller Verfahren) sowie aus zehntausenden von Pfändungsverlustscheinen, die gegen Private und nicht im Handelsregister eingetragene Kleinunternehmen oder wegen unbeglichener Steuerforderungen ausgestellt werden. Laut der offiziellen Statistik mussten 2013 knapp 2.8 Mio. Zahlungsbefehle ausgestellt und mehr als 1,45 Mio. Pfändungen vollzogen werden. Nach Branchenschätzung bescheren Insolvenzen und fruchtlose Pfändungen Wirtschaft und Fiskus Jahr für Jahr Verluste von gegen CHF 11 Mia.

Informationspflichten, die grundsätzlich jedes Personendatum bis hin zur Adresse umfassen, haben übermässig aufwändige Rapport- und Dokumentationspflichten zur Folge und sind im gewerblichen Alltag nicht praktizierbar. Neue Rechtsunsicherheiten und Regulierungen mit hohen Folgekosten werden geschaffen. Unabhängig, ob es sich um eine gesetzliche Vorgabe oder um „good practice" handelt, die aktive Informationspflicht über jegliches bearbeitetes Personendatum wäre mit einem enormen administrativen Aufwand für jeden Inhaber einer Datei verbunden. Oftmals wird sich zudem kaum abschätzen lassen, ob die betroffene Person davon nun Kenntnis hat oder es zumindest wissen müsste, oder eben nicht. Die Rechtsunsicherheit wäre gewaltig. Informationspflicht kann aus Sicht des sgv aus den dargelegten Gründen nicht Bearbeitungsgrundsatz sein.

Dass die Bonitätsauskunft nicht allein auf das Betreibungsregister abstützten kann, zeigt das Beispiel eines Bauherren, der den Generalunternehmer oder die anderen am Bau beteiligten Personen prüfen

will, um sicherzustellen, dass Garantieleistungen auch in der Zukunft erbracht werden können. Eine Garantieverpflichtung nützt nichts, wenn ein Anbieter bereits vor dem Konkurs steht und nur darum ein günstiges Angebot abgegeben hat. In einem solchen Fall reicht die Betreibungsauskunft schon deswegen nicht, weil viele Forderungen aus Kostengründen schon vor der Betreibung abgeschrieben werden. Diese Ausfälle müssen dann von den ehrlichen und pflichtbewussten Konsumenten übernommen werden. Dies widerspricht der geltenden Auffassung, dass derjenige, der einen Schaden verursacht, diesen auch tragen soll. Betreibungsinformationen fallen erst zu einem späten Zeitpunkt an. Es ist für jede Vertragspartei wichtig, frühzeitig zu erfahren, ob die Gegenpartei Zahlungsprobleme hat oder nicht. In Anbetracht der sich gegenüberstehenden Interessen ist es fehl am Platz, Zahlungsinformationen und damit verbundene Angaben der Bearbeitung durch die willkürliche Unterstellung unter den Begriff des Persönlichkeitsprofils der Bearbeitung ganz oder teilweise entziehen zu wollen. Überdies hat ein Anbieter sicherzustellen, dass sich eine Person nicht unnötig überschuldet. Dies kann er nur sicherstellen, wenn er Zugang zu entsprechenden Bonitätsinformationen hat.

Pflicht zur Ernennung eines Datenschutzbeauftragten

Der Verwaltungsrat trägt die oberste Verantwortung und muss die Organisation der Unternehmung nach den Risiken des Unternehmens ausrichten. Im Übrigen auferlegt OR 716a dem Verwaltungsrat die unübertragbaren und unentziehbaren Verpflichtungen. Er hat die Pflicht zur Oberleitung der AG und haftet, wenn er diese Pflicht missachtet. Hierfür führt er eine Risikobeurteilung bzw. ein IKS. Die Pflicht zur Einsetzung eines Datenschutzbeauftragten macht in diesem Zusammenhang keinen Sinn und schiesst über das Ziel hinaus. Mit dem gleichen Recht könnte von jedem Unternehmen ein Produktionsverantwortlicher gefordert werden.

Das heutige DSG ermöglicht Zertifizierungsverfahren und die freiwillige Ernennung eines Datenschutzbeauftragten oder einer Datenschutzbeauftragen in einer Firma. Jede Firma, die überdies mit sensiblen Personendaten operiert, hat ein ureigenes Interesse daran, keine Reputationsschäden zu riskieren.

Der sgv lehnt eine generelle gesetzliche Pflicht zur Ernennung eines Datenschutzbeauftragten für Unternehmen ab, nicht aber für die öffentliche Hand.

Von einer aktiven Meldepflicht von Datenschutzverletzungen ist mindestens im Einzelfall abzusehen. Eine Meldepflicht macht dann allenfalls Sinn, wenn eine sehr grosse Öffentlichkeit, z.B. Tausende von Personen betroffen sind und die Umstände eine Meldung erst rechtfertigen (z.B. verschickt eine Bank an Tausende von Kundinnen und Kunden falsche Kontoauszüge).

4.4 Rechte der betroffenen Personen – Katalog der Rechtsansprüche

Auskunftsrecht: Der wichtigste Grundsatz für eine funktionierende Wirtschaft und ein vertrauensvolles Zusammenarbeiten ist eine objektive Abwägung der sich gegenüberstehenden Interessen. Nicht nur Lieferanten sind an der Möglichkeit von Bonitätsprüfungen interessiert. Auch Konsumentinnen und Konsumenten möchten prüfen, ob sie eine Vorauszahlung an einen Lieferanten leisten sollen oder nicht.

Recht auf Berichtigung: Die Möglichkeit, die Empfänger von Personendaten in Erfahrung zu bringen, widerspricht dem Recht des Datenbearbeiters auf Schutz seiner Kunden. Die Korrekturen haben ohne weitere Angaben über die Informationsempfänger zu erfolgen.

Recht auf Löschung: Zu unterscheiden ist zwischen dem Recht auf „Löschung“ und dem Recht auf „Sperrung“. Für die Sperrung braucht es eine Personenidentifikationsnummer die referenziert werden kann. Bei der Löschung sind in jedem Fall die Daten weg und es kann nicht sichergestellt werden, dass diese in der Zukunft nicht wieder aufgenommen werden. Der Kunde muss sich aber der Folgen bewusst sein. Zudem dürfen nur in begründeten Fällen Daten gelöscht werden, die nicht aus hoheitlichen Quellen stammen. Daten, die von der öffentlichen Hand publiziert werden, sollten nicht gelöscht

werden können. Das Recht auf Löschung darf nicht missbraucht werden um Gutgläubige zu täuschen.

Automatisierte Entscheidungsfindung: Es gibt keinen Anspruch auf Kredit. Insofern muss auch kein „erhöhtes Schutzbedürfnis“ bestehen. Es gibt auch keine Regeln oder Bestimmungen, welche Grundlagen in die Entscheidungsfindung für einen Lieferantenkredit oder Kredit miteinfliessen. Jede Person ist frei in der Auswahl ihrer Kriterien. Die Bonität ist auch nur eines davon. So zählt am Schluss oftmals das Bauchgefühl. Bei der Bearbeitung von einer kleinen Anzahl von Geschäften kann dies individuell gemacht werden und wird von den Unternehmen vielfach in einer „Creditpolicy“ zusammengefasst. Dies ist nötig, damit die Mitarbeitenden wissen wie sie vorzugehen haben. In diesem Fall gibt es für den Betroffenen kein Recht zu erfahren, warum ihm kein Lieferantenkredit gewährt wird. Er kann die Ware ja in jedem Fall kaufen, nur eben nicht auf Kredit sondern gegen Vorauskasse.

Der Vorschlag einer Mehrheit der Begleitgruppe zielt darauf ab, „jeder Person das Recht einzuräumen, keiner auf einer rein automatisierten Bearbeitung von Daten basierenden Entscheidung unterworfen zu werden. Bei einer automatisierten Kreditentscheidung ist das Vorgehen gleich wie im Einzelfall, mit dem Unterschied, dass die Kriterien aufgrund der grossen Anzahl von Transaktionen systemgestützt aufbereitet werden. Subjektive gestützte Beurteilungen werden hingegen eliminiert, was ein Vorteil ist. Das Nichtzulassen automatisierter Einzelentscheidungen ist allerdings ein Eingriff in die Wirtschaftsfreiheit.

Die Abbildung von zahlungsrelevanten Informationen stellt kein Persönlichkeitsprofil dar. Bezahlt jemand eine Rechnungen nicht, oder ist er im Konkursverfahren, so hat der zukünftige Gläubiger das Recht, vor der Gewährung eines Lieferantenkredits zu prüfen, ob bereits Anzeichen auf Zahlungsschwierigkeiten bestehen.

4.8 Besondere Bestimmungen betreffend das Bearbeiten von Personendaten durch private Personen

Beweislastumkehr: Nach den allgemein geltenden Regeln der Beweislastverteilung muss heute die betroffene Person den Nachweis einer Persönlichkeitsverletzung erbringen. Eine Mehrheit der Begleitgruppe möchte die Beweislast umkehren und das Gericht ermächtigen, vom Datenbearbeiter im Einzelfall den Nachweis einer datenschutzkonformen Bearbeitung verlangen zu können. Der sgv lehnt eine solche Beweislastumkehrung ab. Die vorgeschlagene Beweislastumkehr wird im Ergebnis dazu führen, dass Datenbearbeiter alle möglichen Interna offenlegen müssen, um sich gegen die unsubstanzierte Behauptungen zu verteidigen, sie hätten sich nicht datenschutzkonform verhalten. Die Beweislastumkehr läuft auf eine Verschuldensvermutung hinaus und wird vom sgv abgelehnt. Ebenso unterstützt der sgv eine Kausalhaftung zu Lasten des privaten Datenverarbeiters nicht.

Der Vorschlag, die Bearbeitung von Daten juristischer Personen im Rahmen ihres Geschäftszwecks als Rechtfertigungsgrund aufzunehmen, ist zu unterstützen. Nur müsste dieser Rechtfertigungsgrund auf alle Unternehmen ausgedehnt werden, also auch auf Einzelfirmen und Personengesellschaften. Damit ist auch die haftende Person miteinbezogen. Die Anbieterseite ist als Ganzes gleich zu behandeln, zumal sie selbst wählen kann in welcher Rechtsform sie am Markt auftreten will.

Massnahmen zur verbesserten Durchsetzung individueller Ansprüche

Kostenerleichterungen: Mit der Einführung der neuen Prozessordnungen auf 1.1.2011 sind in den Kantonen Kostenvorschüsse für Kläger vor Gerichten eingeführt bzw. massiv erhöht worden. Damit ist die Hürde vor allem auch für gewerbliche Kreise, vor Gericht Recht zu erhalten, erhöht worden. In gewissen Kantonen und Gerichten bewirken hohe Gebühren faktisch eine Zugangsbarriere. Vor diesem Hintergrund ist es schwer vorstellbar, für den partikulären Fall von Datenschutzverletzungen „erheblich reduzierte“ Gerichtskosten festzulegen. Dass die reduzierten Kosten nur für natürliche, nicht aber für juristische Personen gelten sollen, ist ebenfalls schwer nachvollziehbar. Auch juristi-

sche Personen im kleingewerblichen Bereich verfügen nicht über finanzielle Mittel auf Vorrat.

Sammelklagen: Der sgv hat gegenüber Sammelklagen im Bereich des Datenschutzes grosse Vorbehalte.

4.10 Autorités de contrôle

Vorgeschlagen wird, der eidgenössischen Datenschutzbehörde ein Untersuchungsrecht, vergleichbar mit demjenigen der Wettbewerbsbehörde nach Art. 26 KartG zu geben. Nach einer informellen Voruntersuchung hätte die Datenschutzbehörde die Möglichkeit, eine formelle Untersuchung zu eröffnen und auch Bussen zu verteilen. Sie würde damit eine Verfügungsbefugnis erhalten.

Der sgv vertritt die Auffassung, dass die heutigen Möglichkeiten gemäss Art. 29 DSG genügen, wonach der Datenschutzbeauftragte von sich aus oder auf Meldung Dritter einen Sachverhalt im Privatrechtsbereich abklärt, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler); Datensammlungen registriert werden müssen (Art. 11*a*) oder eine Informationspflicht nach Artikel 6 Absatz 3 DSG besteht. Der Datenschutzbeauftragte kann entsprechende Empfehlungen erlassen. Aus Sicht des sgv sind zusätzliche Gremien nicht nötig.

Finanzierung des Datenschutzes: Der Schweizerische Gewerbeverband sgv unterstützt die bisherige Alimentierung des Datenschutzbeauftragten und seiner Mitarbeitenden aus dem Bundeshaushalt. Zusätzliche Finanzierungsmittel wie z.B. eine Abgabepflicht für Betriebe lehnt der sgv ab. Auch eine Finanzierung aus Bussen ist für den sgv nicht zielführend.

Schlussbemerkungen

Die Diskussion um den Datenschutz vor dem Hintergrund neuer Technologien und Entwicklungen ist wichtig. Datenschutz darf nicht nur aus der Optik von „Social media“, „Google“, usw. betrachtet werden. Aufgrund der hohen Nutzerzahl der sozialen Medien haben sich die Datenschutzbedürfnisse stark verändert. Das „Recht auf Vergessen“ wird stipuliert und ohne weiteres auf alle Datenverarbeiter und jede Form der Datenbearbeitung ausgedehnt. Den Auswirkungen auf Gewerbe und Wirtschaft muss dabei viel mehr Beachtung geschenkt werden. Datenschutz darf nicht dazu führen, dass Schuldner ein Recht auf die Löschung ihres negativen Zahlungsverhaltens erhalten. Die kürzlich erschienene Studie von Deloitte „Economic impact assessment of the proposed European General Data Protection Regulation“ zeigt unter anderem auf, was die wirtschaftlichen Auswirkungen sind und was für Bereiche von der Novellierung der Datenschutzgrundverordnung betroffen sind.[1]

Ebenfalls mit in die Überlegungen einzubeziehen sind:

- **Direct Marketing** als grundlegende Quelle der Kommunikation zwischen den Anbietern und deren Kunden. Die Möglichkeit, bestimmte Gruppen von Kunden zielgerichtet anzusprechen, ist das Schlüsselkriterium für die Abgrenzung von anderen Formen des Marketings.
- **Online Behavioural Advertising** bezieht sich auf die Verwendung von Online-Daten um die Interessen von Usern mit den spezifischen Angeboten abzustimmen.
- **Web Analytics** hilft Anbietern dem Konsumenten mit einer besseren Qualität und relevanteren Inhalten zu versorgen.
- **Credit Information**: Bonitätsinformationen sind wichtige „Enabler“ der Wirtschaft und versorgen die sie mit den notwendigen Tools, um das Ausfallrisiko zu bestimmen. Dies hilft die Kosten für die Güter zu verringern und vereinfacht den Onlinebezug von Gütern.

---

[1] Deloitte, Economic impact assessment of the proposed European General Data Protection Regulation, 2013; Seite 6 ff.

Diese vier Bereiche sind von erheblicher wirtschaftlicher Bedeutung und müssen in die Erwägungen miteinbezogen werden. Insgesamt ist sicherzustellen, dass nicht auf Kosten der Wirtschaft vermeintlich konsumentenfreundliche Regulierungen erfolgen, die anschliessend auf die Konsumenten zurückfallen.

Dieter Kläy

Ressortleiter

Bemerkungen Normenkonzept Revision DSG

VUD | David Rosenthal, 30. September 2014

Die folgenden Kommentare beziehen sich auf das Normenkonzept und Kommentare anderer Mitglieder der Begleitgruppe. Sie stützen sich auf Inputs aus dem VUD und meine persönlichen Erfahrungen.

A. Einleitende Bemerkungen

Der Bundesrat hat dem BJ den Auftrag erteilt, eine Revision des DSG zu prüfen. Wir sind jedoch nach wie vor der Ansicht, dass in der Sache kein Bedarf an einer Revision steht. Zwar ist der Datenschutz in den Schlagzeilen wie nie zuvor, doch das hat nur damit zu tun, dass er heute verstärkt Beachtung findet und durchgesetzt wird, nicht, dass er nicht hinreichend ist.

Sämtliche Fälle, die in der Schweiz zu einer gerichtlichen Beurteilung führten oder in denen die Behörden aktiv geworden sind, haben bewiesen, dass die gesetzlichen Grundlagen genügen. Sie haben sogar aufgezeigt, dass der Datenschutz heute tendenziell zu weit geht.

Als Beispiel sei ein ganz aktueller Fall erwähnt, in welchem ein Schweizer Gericht unter dem Titel des Datenschutzes selbst die Bearbeitung von *anonymen* Daten verboten hat, und das DSG anwandte, obwohl unbestrittenermassen gar keine Personendaten vorlagen.

Das Beispiel zeigt – wie etliche andere Prozesse im Bereich des Datenschutzrechts auch – dass die betroffenen Personen keineswegs am kürzeren Hebel sind. DSG ist technologieneutral und die darin enthaltenen Grundsätze sind nach wie vor richtig. Dass der Datenschutz mit den aktuellen technologischen Entwicklungen nicht Schritt halten kann, ist zwar eine weitverbreitete, politisch attraktive Behauptung, aber letztlich durch nichts belegt.

Richtig ist, dass die Fälle, in denen die Regeln verletzt wurden oder in denen die zur Anwendung dieser Regeln nötigen Wertungen diskutiert werden, sehr viel medienträchtiger sind und mehr Personen betreffen und vor allem internationaler sind als in der Vergangenheit. Die Regeln deswegen als ineffektiv oder gar überholt zu bezeichnen, ist ein Trugschluss.

Auch die in den Arbeiten immer wieder gehörte Aussage, niemand ausser einigen Experten würden das DSG verstehen, ist aus unserer Sicht falsch. Abstrakte Regeln gehören zum Wesen des schweizerischen Rechts und sind gerade einer der Gründe, warum das DSG auch heute noch funktioniert. Wird kritisiert, dass der Normalbürger bei der Lektüre des DSG nicht wisse, was er zu tun habe, so gilt dasselbe für das ZGB und OR. Kein "Normalbürger" kennt sich heute noch z.B. mit den Regeln im Kündigungsschutz im Arbeitsbereich oder Mietrecht aus; der Blick ins Gesetz genügt schon lange nicht mehr. Man muss Experte im Arbeits- oder Mietrecht sein, um zu verstehen, was wirklich gilt.

Das ist aber kein Fehler des Rechts, sondern zeigt die Entwicklungsfähigkeit abstrakter Regeln und es belegt die Komplexität unserer Welt. Die Dinge sind eben nicht so simpel, und wer

glaubt, dies auf einfache Weise mit neuen Regeln zu lösen, schadet der Sache. Es wäre schade, wenn wir die Schweizer Rechtstradition durch die heute leider weit verbreiteten populistischen und sehr eingängigen, aber zu kurz gedachten Forderungen im Bereich des Datenschutzes über Bord zu werfen.

Übrigens ist auch das heutige Instrument von Art. 29 DSG, dass dem EDÖB ein umfassendes Klagerecht gibt, vollauf genügend und sehr effizient ist. Es ist klar, dass dies eine politisch nicht opportune Aussage ist, da alles nach "Stärkung" des Datenschutzes schreit und ein EDÖB, der lediglich "Empfehlungen" aussprechen statt verfügen kann, als zahnlos erscheinen mag (auch wenn dies in der Praxis seinem Klagerecht in keiner Weise gerecht wird; er kann heute faktisch genauso Druck ausüben wie wenn er selbst Anordnungen treffen könnte, wie zahlreiche Beispiele zeigen). Dass der EDÖB selbst Verfügungskompetenz möchte, ist vor diesem Hintergrund zwar nachvollziehbar, aber nicht zielführend und notwendig.

Aber bei Lichte betrachtet ist das einzige Problem, das der Durchsetzung des DSG durch den EDÖB im Wege steht, der Mangel an Ressourcen des EDÖB. Dieses Problem werden die vorgeschlagenen Anpassungen nicht lindern, sondern verschärfen. Sie mögen politisch unvermeidlich sein, aber die Schweiz wird dem Datenschutz (und der Wirtschaft, die die Kosten zu tragen hat) damit keinen Gefallen erweisen; die Anwälte und Berater werden sich hingegen freuen. Sie haben es schon im Bereich des Kartellrechts getan, aber die Kosten der Datenschutzaufsicht werden explodieren oder, falls die Ressourcen nicht zur Verfügung gestellt werden, in den eigenen Verfahrensbestimmungen stecken bleiben.

Es ist klar, dass die Schweiz im Falle einer Verabschiedung der revidierten Europaratskonvention 108 deren Regelungen irgendwie übernehmen muss. Sie sollte dabei jedoch nicht einfach etwas weltfremde Regelungen (wie z.B. bei den automatisierten Einzelfallentscheidungen oder der Transparenz, welche zu einer Inflation an "Hinweisen" führen wird, die am Ende nicht mehr Transparenz verschaffen werden, als es die kleingedruckten Geschäftsbedingungen von iTunes schon tun) mit dem Argument übernehmen, man müsse das eben tun. Die Schweiz hat in solchen Fällen einen erheblichen Spielraum bei der Umsetzung und sollte ihn mit Augenmass nutzen, auch wenn zu wünschen gewesen wäre, dass die Revision der Konvention von einem etwas ausgeglichenerem Gremium ausgearbeitet worden wäre.

B. Einige konkrete Bemerkungen

1. Best Practice

Die Best Practice-Regeln werden nur dann ihren Zweck erfüllen, wenn sie den Datenbearbeitern Rechtssicherheit geben. Der VUD regt an, ausdrücklich auf die Regelung in Österreich zu verweisen, wo es "genehmigte" Good-Practice-Regelungen schon gibt. Hier findet sich ein Beispiel:

https://www.wko.at/Content.Node/branchen/sbg/BankVersicherung/Banken-und-Bankiers/Verhaltensregeln-fuer-Gluecksspielbetreiber-1.html

2. Begriffsdefinitionen

Es ist nicht sinnvoll, Begriffe wie das "Territorialitätsprinzip", die durch die Rechtssprechung vor dem Hintergrund der laufenden gesellschaftlichen Entwicklung ständig weiterentwickelt werden, festzuschreiben und damit einer Weiterentwicklung zu entziehen. Damit wird genau jener Fehler begangen, von dem man glaubt, ihn mit der jetzigen Revision beheben zu müssen, nämlich dass das DSG von der technologischen und gesellschaftlichen Entwicklung überholt wird. Dies ist nicht der Fall, doch gewisse der ins Auge gefassten Anpassungen werden das DSG so sehr auf ganz bestimmte Praxisanwendungen konkretisieren, dass das DSG nicht mehr "passen" wird, wenn sich die Fragestellungen, Wertvorstellungen oder andere Aspekte auch schon nur leicht ändern. Das DSG ist zwar schon viele Jahre alt, aber der Umstand, dass es so allgemeingültig formuliert ist, macht es auch sehr flexibel. Der Fall Google Street View hat bewiesen, dass sich das DSG bestens auch im Zeitalter der internationalen Internetdienste anwenden lässt.

Beim Umgang mit Personendaten sind grundsätzlich folgende Funktionen zu unterscheiden: (A) die natürliche oder juristische Person, welche für die Bearbeitung von Daten in irgend einer Form zuständig und verantwortlich ist: “controller“ im Sinne von Art. 2.d RL 95/46/EG; (B) der “Inhaber einer Datensammlung“ im Sinne von Art. 3 Bst. i DSG; (C) der “Auftragsdatenbearbeiter“ (“processor“ im Sinne von Art. 2.e RL 95/46/EG), d.h. jener Dritte im Sinne von Art. 10a DSG, welcher Daten im Auftrag eines Auftraggebers bearbeitet. Bisher fehlt im schweizerischen Datenschutzrecht eine Definition welche in Abgrenzung zum “Inhaber der Datensammlung“ nach Art. 3 Bst. i DSG und Art. 2 d) der Europaratskonvention ETS Nr. 108 “controller of the file“ die für eine Bearbeitung von Personendaten verantwortliche Person oder Stelle definiert. Wir betrachten die beiden Begriffe “Inhaber der Datensammlung“ sowie “bearbeitende Stelle“ keineswegs als gleichwertig, wie u.E. zu Unrecht im Normkonzept angenommen wird, sondern als auf erheblich verschiedene Tatbestände bezogene Begriffe bzw. Funktionen. Auch wenn im europäischen Ausland die verschiedenen Begriffe zum Teil durchmischt werden, erachten wir es als sinnvoll, hier weiterhin klar zwischen den verschiedenen Funktionen zu trennen.

Nach geltendem schweizerischen Recht werden die “Persönlichkeitsprofile“ gemäss Art. 3 Bst. d DSG durchgehend den gleichen Anforderungen unterstellt wie die “besonders schützenswerten Personendaten“ nach Art. 3 Bst. c DSG. Nun soll die für das schweizerische Datenschutzrecht von 1992 originelle und weit in die Zukunft greifende Definition des “Persönlichkeitsprofils“ gestrichen und durch spezielle Regelungen zum “Profiling“ ersetzt werden. Es stellte sich bei uns bei nochmaliger Betrachtung die Frage, wieviel damit gewonnen würde. Denn auch bei den Bestimmungen über das “Profiling“ wird man um eine entsprechende, wegen der Tragweite der Bestimmung heikle Definition der “Persönlichkeitsprofile“ nicht herumkommen.

3. Informationspflicht

Es ist sinnvoll, die heute in Art. 14 und 18a/b DSG zusätzlich vorgesehene Informationspflicht zugunsten eines allgemeinen Grundsatzes der Transparenz aufzuheben. Es muss jedoch darauf geachtet werden, dass die selbständige Informationspflicht nicht zu einem übermässigen bürokratischen Aufwand führt wie bei den heute in der Praxis kaum sinnvoll umsetzbaren Art.

14 und 18-18b DSG. Eine Pflicht zur Information der betroffenen Personen über jede der heute allgegenwärtigen, aber auch alltäglichen Datenerfassungen und -bearbeitungen bei jeder Art elektronischer Kommunikation geht schlicht zu weit, Europarat hin oder her. Hier ist im Normenkonzept nochmals zu betonen, dass eine vernünftige, sachgerechte und zurückhaltende Umsetzung anzustreben ist, die nicht zu einer Inflation der Information führt, die gar nichts bringt, ja sogar kontraproduktiv ist.

4. Auskunftsrecht

Der Zugang externer Personen zu firmeninternen Unterlagen muss restriktiv gehandhabt werden, schon aus Gründen der Datensicherheit. Es besteht heute schon eine Tendenz der Gerichte, externen Personen durch ausufernde Auskunftsansprüche Zugang zu allen möglichen internen Unterlagen von Unternehmen zu geben, selbst wenn es überhaupt nicht um den Datenschutz geht; das Auskunftsrecht wird immer häufiger missbraucht, um Beweismittel für datenschutzfremde Zwecke zu sammeln, Unternehmen zu schikanieren und auszuforschen. Ein Ausbau der Zugangsrechte, wie teilweise auch hier gefordert, ist nicht angezeigt.

Bezüglich der heutigen Regelung ist es zwingend, dass im Falle eines strittigen Auskunftsgesuchs, die Interessenabwägung immer auch die Interessen des Inhabers der Datensammlung berücksichtigt werden. Es gibt keinen sachlogischen Grund, warum seine Interessen per se nicht beachtlich sind, wenn er die Daten, um die es geht, bereits an Dritte weitergegeben hat (wozu z.B. ein konzerninterner Datenverkehr schon genügen kann). Genau dies sieht Art. 9 Abs. 4 DSG heute aber vor. Der bestehende Zusatz "und er die Personendaten nicht Dritten bekannt gibt" ist in dieser Bestimmung daher ersatzlos zu streichen. Es gibt keinen Grund zur Befürchtung, dass die Gerichte, welche die Interessenabwägung letztendlich vornehmen müssen, dies nicht sachgerecht tun werden. Heute wird ihnen aber in den erwähnten Fällen die Vornahme einer Interessenabwägung untersagt.

Es wurde im Kreise des VUD noch angeregt, beim Auskunftsrecht vorzusehen, dass die betroffene Person dann, wenn sie Auskunft über Sicherungs- und Archivdaten sucht, ein rechtlich geschütztes Interesse glaubhaft zu machen hat; hier also höhere Anforderungen gelten sollen (vgl. dazu § 19(1) und (2) sowie §§ 33(2) Ziff. 2 und 34 (7) BDSG). Das rechtfertigt sich umso mehr, als Unternehmen immer stärker durch den Gesetzgeber zur Aufbewahrung von Daten verpflichtet werden. Als sinnvoll erachtet wird auch, eine Mitwirkungspflicht der betroffenen Person zum Auffinden der Daten zu statuieren.

5. Zustimmung

Die geltende Regelung betreffend Zustimmung soll beibehalten werden. Die im Europarat und in der EU teilweise diskutierten Anpassungen rühren von einem dort – anders als in der Schweiz – praktizierten Verständnis des Begriffs der Einwilligung her. In der Schweiz sind die Anforderungen an eine Einwilligung schon relativ hoch. Der Unterschied z.B. zwischen einer "klaren" und "nicht klaren" Einwilligung ist dem Schweizer Recht wesensfremd; entweder liegt eine Einwilligung vor oder aber eben nicht. Wir möchten zudem ausdrücklich davor warnen, von einer fehlenden Einwilligung auszugehen, wenn eine betroffenen Person sich über die Datenbearbeitung nicht erkundigt, welche die von der bearbeitenden Stellen zugänglich gemachten

Angaben über die Bearbeitung der Daten nicht gelesen oder diese nicht verstanden hat, und unüberlegt das “Gelesen und Verstanden-Häklein“ unter ein Angebot im Web gesetzt hat. Voraussetzung für eine gültige Einwilligung ist natürlich eine “angemessene vorangehende Information“ im Sinne von Art. 4 Abs. 5 DSG. Es kann diesbezüglich auf die Gerichtspraxis zu “ungelesenen oder nicht verstandenen AGB“ unter Vorbehalt der Ungültigkeit von ungewöhnlichen, einseitigen, irreführenden AGB verwiesen werden: Zusammengefasst in BGE 109 II 213. Es gibt auch hier keinen Grund, dies im Datenschutz anders als im ganzen Rest des Schweizer Rechts zu regeln.

6. Widerspruchsrecht

Das Widerspruchsrecht ist nicht auszubauen, weil es heute schon besteht und nicht erwiesen ist, warum es nicht genügen soll. Im Gegenteil: hat das Google-Urteil des EuGH jüngst gerade wieder belegt, wie streng das heutige Datenschutzrecht sein kann, wenn es tatsächlich genutzt wird. Das Urteil zeigt aber auch die Schattenseiten auf (Zensurdiskussion). Das Datenschutzrecht sollte zudem wertungsfrei bleiben und nicht dafür benutzt werden, die Weiterentwicklung unserer Wertordnung aufzuhalten, bloss weil man sie für heikel hält. Die Profilbildung wird in unserer Gesellschaft immer wichtiger, weil es je längers je mehr Möglichkeiten gibt, solche zu bilden; sie hat aber wie alles ihre guten und schlechten Seiten. Profile können etwa auch dazu dienen, Entscheide vorhersehbarer, transparenter zu machen. Und Unternehmen können durch Profile missbräuchliche Verhaltensweisen immer besser erkennen. Die Profilbildung zu verteufeln, ist nicht sachgerecht. Es kann daher nicht Sache des Datenschutzrechts sein, der Profilbildung durch ein spezifisches Widerspruchsrecht pauschal einen Riegel schieben zu wollen.

7. Datenportabilität

Das Recht auf Datenportabilität hat im Datenschutzrecht nichts zu suchen. Es geht dabei nur um die Regulierung der Marktzugangs zu sozialen Netzwerken. Das ist eine typische "Denkzettel"-Regel einiger EU-Politiker und Datenschützer, denen Facebook ein Dorn im Auge ist, deren Auswirkung aber niemand versteht und deren Kosten schon gar nicht. Wir sollten nicht den Fehler machen, solche Dinge in unser Recht zu übernehmen; dies ist überdies ein massiver Eingriff in die Wirtschaftsfreiheit. Falls sich die Datenportabilität auf EU-Ebene tatsächlich durchsetzen sollte, würden die Schweizer Kunden bei solchen Diensten ohnehin automatisch mitprofitieren.

8. Ausländische Gerichts- und Behördenverfahren als Rechtfertigungsgrund für Exporte

Die geforderte Ausdehnung des Rechtfertigungsgrunds bei Datenexporten von Gerichten auf Behörden ist sachgerecht. Ein Unternehmen darf heute Unterlagen liefern, wenn es im Ausland angeklagt worden ist oder selbst gegen jemanden klagt, und sei es wegen einer belanglosen Sache (Art. 6 Abs. 2 Bst. d DSG). Es darf aber keine Unterlagen liefern, wenn dies im Rahmen eines vorgerichtlichen, aber ebenso regulierten Behördenverfahrens erforderlich ist, zum Beispiel die eigene Unschuld zu beweisen. Diese Unterscheidung ist nicht nachvollziehbar. Ein Unternehmen wird heute dadurch gezwungen, entweder das DSG zu verletzen oder bei einer Behördenuntersuchung die Kooperation zu verweigern und es zu einer Anklage vor Gericht – mit potenziell katastrophalen Folgen für alle Beteiligten – kommen zu lassen, da erst dann nach

DSG geliefert werden darf. Das macht keinen Sinn. Die Regelung ist daher auf Behördenverfahren auszudehnen.

9. Zertifizierungspflicht

Die Zertifizierungspflicht im Bereich der Krankenversicherung ist letztlich ein Kompromiss im Streit um die Einführung der Fallpauschalen; sie kann und sollte keineswegs als Vorbild für weitere Zertifizierungspflichten für andere Bereiche dienen. Die Zertifizierungen und damit verbundenen Aufwände kosteten den Prämienzahler bereits Millionen, ohne, dass sie wirklich einen Zusatznutzen bringen. Eine Zertifizierung belegt einzig, dass ein Datenschutzmanagementsystem existiert, also entsprechende Prozesse und Dokumentationen vorhanden sind, es belegt aber in keiner Weise, ob der Datenschutz wirklich eingehalten wird. Datenschutzverstösse verhindert auch ein DSMS nicht. Es gibt einen guten Grund, warum sich Unternehmen nicht für Zertifizierungen nach Art. 11 DSG interessieren. Solange sie freiwillig sind, schaden sie nichts. Wird die Zertifizierungspflicht aber ausgedehnt, dient dies vor allem der Zertifizierungsbranche. Soll in gewissen Branchen der Datenschutz verstärkt werden, sind Kontrollen und Untersuchungen, wie sie bisher praktiziert wurden, wesentlich wirksamer und nachhaltiger.

10. Rechtfertigungsmöglichkeit auch bei Verletzung der Datenschutzgrundsätze

Es wurde angeregt, dass Art. 12 Abs. 2 Bst. a DSG entgegen dem Vorschlag im Normenkonzept so belassen wird, wie er heute im Gesetz ist. Dies ist abzulehnen. Der EDÖB hatte dies im Fall Logistep so vertreten, aber das Bundesgericht hat festgestellt, dass es sich um ein Versehen handelte (wie in der Lehre mit Verweis auf die Sitzungsprotokolle nachgewiesen wurde; das Parlament ging damals von einer falschen Annahme aus). Es hielt fest, dass auch Verletzungen der Bearbeitungsgrundsätze gerechtfertigt werden können. Dies entspricht auch einem Grundprinzip des Persönlichkeitsschutzrechts entspricht. Der Fall, in welchem der Entscheid zustande kam, war jedoch ein sehr schlechter Fall und das Bundesgericht wurde für seine Interessenabwägung zugunsten des Datenschutzes massiv kritisiert. Aus der Not gebar es die Formel, dass eine Rechtfertigung eben nur mit grosser Zurückhaltung zulässig sei. Diese Formel wird inzwischen vom EDÖB und auch den Gerichten gebetsmühlenmässig wiederholt wird. Das Bundesgericht hält sich selbst allerdings nicht (mehr) daran, sondern praktiziert die Interessenabwägung so, wie eine Interessenabwägung überall im Schweizer Recht vorzunehmen ist: Durch schlichtes Abwägen aller auf dem Spiel stehenden Interessen. So gilt es heute auch. Bereits im Fall Google Street View wurde die Interessenabwägung wieder wie vor der letzten Revision durchgeführt. Die Sache sollte im Normenkonzept korrekterweise ausdrücklich beim Namen genannt werden, nämlich dass es sich bei der heutigen Formulierung um ein Versehen handelte. Das gesetzgeberische Versehen sollte definitiv korrigiert werden.

11. Verfügungskompetenz des EDÖB, kollektive Klageinstrumente

Wie eingangs erwähnt ist es wenig sinnvoll, den EDÖB durch Verfügungskompetenzen verfahrensmässig unnötig zu belasten. Er wird mehr Ressourcen benötigen, und die wenigen zusätzlichen Ressourcen, die er erhalten wird, werden für die Wahrung der nötigen Verfahrensvorschriften und -garantien verbraucht werden. Damit ist dem Datenschutz nicht gedient, und inzwischen scheint diese Erkenntnis verschiedenenorts zu reifen.

Wenn nun stattdessen auf Instrumente wie Verbands- oder Sammelklagen ausgewichen werden soll, wird dies den Datenschutz zusätzlich schwächen. Die Datenschutzverbandsklage gibt es seit Jahren und sie ist toter Buchstabe. Die Sammelklage wird in Datenschutzbelangen ebenfalls toter Buchstabe (was die Stärkung des Datenschutzes betrifft) bleiben, birgt aber einiges an Missbrauchspotenzial. Der Datenschutz eignet sich schlicht nicht für Sammelklagen. Und dort, wo es darum geht, gegen eine bestimmte Art der Datenbearbeitung einer bestimmten Person an sich vorzugehen, haben wir bereits das Verfahren nach Art. 29 DSG, das ausgezeichnet funktioniert und erprobt ist. Es ist zugleich das volkswirtschaftlich günstigste Instrument.

Google Street View oder Moneyhouse sind Paradebeispiele, dass das Verfahren nach Art. 29 DSG, in welchem der EDÖB quasi stellvertretend für die betroffenen Personen gegen eine Datenbearbeitung in grundsätzlicher Art und Weise vorgeht, funktioniert und zielführend ist. Kein Verein hätte eine solche Klage gegen Google Street View oder Moneyhouse geführt, eine Sammelklage wäre nie in Frage gekommen. Soll der EDÖB allerdings Verfügungskompetenz erhalten, wird er zwangsläufig wesentlich weniger frei in der Wahl seiner Fälle sein. Auch das ist ein Grund, am bisherigen System festzuhalten.

12. Prozessuale Instrumente

Die Beweislastumkehr läuft, wie entsprechende Kommentatoren festgestellt haben, auf eine Vermutung der "Schuld" hinaus. Hier möchten wir nochmals zu bedenken geben, dass eine Beweislastumkehr in der Praxis unnötig ist. Der Schutz des Einzelnen scheitert in Datenschutzfällen nie am Problem der Beweislast, und es gibt auch keinerlei Belege für solche Fälle. In Tat und Wahrheit sieht das Schweizer Zivilprozessrecht schon heute weitgehende Mitwirkungspflichten seitens einer beklagten Person vor.

Es sei an dieser Stelle – wie schon in der Redaktionsgruppe – betont, dass es keinen Sinn macht, aus reiner Symbolik Dinge, die im Schweizer Zivilprozessrecht ausgiebig, gerecht und sachgerecht geregelt sind, für das Datenschutzrecht nochmals und zudem anders zu regeln. Es gibt keinen Grund, den Datenschutz anders zu behandeln. Auch für eine Kausalhaftung gibt es keinen Anlass. Sie belastet lediglich die Unternehmen, die solche Risiken in ihrer Kalkulation finanziell unterlegen und letztlich auf die Konsumenten überwälzen müssen, ohne, dass ihnen dies jedoch wirklich zu Gute kommt.

Die vorgeschlagenen Kostenerleichterungen braucht es in der Praxis nicht. Sie belasten nur die Staatskasse, werden aber den Rechtsschutz von Privatpersonen nicht stärken. Wenn überhaupt Kosten ein Hinderungsgrund für die Rechtsdurchsetzung sind, dann nicht die Gerichtskosten, sondern die Kosten für die anwaltliche Vertretung und die Pflicht, die gegnerischen Kosten im Falle eines Unterliegens tragen zu müssen.

Wenn aber aus politischen bzw. symbolischen Gründen eine Kostenerleichterung vorgesehen werden sollte, so hat sie für alle Verfahren von Konsumenten zu gelten, die dieselben Themenkomplexe betreffen, so namentlich UWG, DSG und ZGB 28. Andernfalls könnten die betreffenden Ansprüche aus prozessualen Gründen nicht mehr zusammen geltend gemacht werden, wie dies in der Praxis regelmässig geschieht; den betroffenen Personen wäre ein Bärendienst er-

wiesen. Im Grunde sollte es also gar keine Kostenerleichterung geben, und wenn doch, dann höchstens eine, die einer Klagehäufung nicht im Wege steht.

Der Hinweis, dass der Rechtfertigungsgrund von Daten juristischer Personen im Rahmen ihres Geschäftszwecks bzw. ihrer Geschäftstätigkeit auch auf Personengesellschaften und Einzelfirmen auszuweiten ist, erscheint an sich berechtigt; allerdings muss dies einhergehen mit der Definition des Begriffs der Personendaten (d.h. wenn im Rechtfertigungsgrund auch Einzelfirmen berücksichtigt werden, dann sollte auch der Begriff des Personendatums Daten von Einzelfirmen umfassen, was nicht der Fall ist, da sich sonst das Problem gar nicht stellt, weil deren Daten nicht vom DSG erfasst sind).

C. Abschliessende Bemerkung

Die Bemerkungen sind aufgrund sprachlicher Hindernisse (französische Teile des Normenkonzepts) nicht als abschliessende Stellungnahme bzw. Zustimmung zu allen anderen Teilen des Normenkonzepts zu verstehen.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police (DFJP)

Office fédéral de la justice (OFJ)
Domaine de direction Droit public
Unité Projets et méthode législatifs

Référence: COO.2180.109.7.150383 / 212.9/2012/00754

Date: 29 octobre 2014

Esquisse d'acte normatif relative à la révision de la loi sur la protection des données

Rapport du groupe d'accompagnement Révision LPD

Table des matières

1. Situation initiale ... 3
2. Contexte international ... 4
3. Position des membres du groupe d'accompagnement quant à l'existence d'un besoin de légiférer ... 6
4. Contenu essentiel de la révision ... 7
4.1 Concept et mise en œuvre ... 8
4.1.1 Concept ... 8
4.1.2 Mise en œuvre ... 8
4.2 Champ d'application et terminologie ... 11
4.2.1 Champ d'application ... 11
4.2.2 Définitions ... 15
4.3 Principes généraux de protection des données personnelles ... 16
4.3.1 Transparence des traitements ... 16
4.3.2 Mesures de diligence ... 17
4.3.3 Consentement ... 20
4.3.4 Autres principes ... 20
4.4 Droits des personnes concernées ... 21
4.4.1 Introduction ... 21
4.4.2 Catalogue des prétentions ... 21
4.4.3 Droit d'accès ... 22
4.4.4 Droit à la rectification ... 23
4.4.5 Droit à l'effacement ... 23
4.4.6 Décisions individuelles automatisées ... 24
4.4.7 Droit à la portabilité des données ... 25
4.5 Communication transfrontière de données ... 25

4.6 Procédure de certification 26
4.7 Registre des fichiers 26
4.8 Dispositions particulières relatives au traitement de données personnelles par des particuliers 26
4.8.1 Conception de la réglementation 26
4.8.2 Atteintes à la personnalité et motifs justificatifs 27
4.8.3 Prétentions et procédures 29
4.9 Dispositions particulières relatives au traitement de données personnelles par des organes fédéraux 34
4.9.1 Conception de la réglementation 34
4.9.2 Licéité du traitement de données (en particulier bases légales suffisantes) 34
4.9.3 Dispositions particulières pour certaines formes de traitement de données 35
4.9.4 Mesures organisationnelles 36
4.9.5 Prétentions et procédures 36
4.9.6 Relation entre les dispositions de la LPD et de la LTrans 37
4.10 Autorités de contrôle 37
4.10.1 Introduction 37
4.10.2 Tâches et pouvoirs de l'autorité de contrôle 38
4.10.3 Organisation de l'autorité de contrôle 43
4.10.4 Renouvellement des rapports de fonction 46
4.10.5 Collaboration entre autorités au plan national et international 46
4.10.6 Financement 46
4.11 Dispositions pénales 48
4.12 Dispositions finales 48
5. Forme de l'acte normatif et contexte normatif 48
6. Structure générale de la réglementation 50
7. Densité normative (degré de détail) 50
8. Calendrier 50

Annexe : Prises de position de certains membres du groupe d'accompagnement

1. Situation initiale

La loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1) est entrée en vigueur le 1er juillet 1993. Elle vise à protéger la personnalité des personnes qui font l'objet d'un traitement de données (art. 1 LPD) et ainsi à garantir le droit fondamental à la sphère privée (art. 13, al. 2, Constitution fédérale, Cst.; RS 101). Elle s'applique au traitement de données personnelles effectué par des personnes privées et par des organes fédéraux (art. 2, al. 1, LPD).

Quelque 20 ans après son entrée en vigueur, la LPD a fait l'objet d'une évaluation détaillée. Il ressort du rapport du Conseil fédéral sur cette évaluation[1] que la loi a permis d'atteindre un niveau de protection appréciable dans les domaines où les défis étaient déjà connus au moment de son entrée en vigueur. Les développements technologiques et sociétaux intervenus depuis lors engendrent cependant depuis quelques années de nouvelles menaces pour la protection des données.

Se fondant sur les conclusions de cette évaluation, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) d'examiner des mesures législatives permettant de renforcer la protection des données afin de prendre en compte les nouvelles menaces qui pèsent sur la sphère privée. Il souhaite plus précisément connaître des mesures permettant d'atteindre les objectifs suivants :

- Assurer la protection des données plus en amont ;
- Sensibiliser davantage les personnes concernées aux risques que représentent les nouvelles technologies pour la protection de la personnalité ;
- Améliorer la transparence des traitements de données ;
- Améliorer le contrôle et la maîtrise des données après leur communication ;
- Protéger les mineurs.

Le Conseil fédéral estime que d'autres possibilités d'intervention sont également dignes d'être examinées, à savoir le renforcement de l'indépendance du Préposé fédéral à la protection des données et à la transparence (PFPDT), l'extension de l'instrument de l'autoréglementation et la répartition des compétences entre Confédération et cantons.

Le DFJP est chargé de soumettre au Conseil fédéral, à la fin de 2014 au plus tard, des propositions sur la suite des travaux. Ce faisant, il doit tenir compte notamment des conclusions de l'évaluation ainsi que des développements en cours dans le domaine de la protection des données dans l'Union européenne et au Conseil de l'Europe. Au sein du DFJP, ce dossier est placé sous la responsabilité de l'Office fédéral de la justice (OFJ).

L'OFJ a institué un groupe de travail élargi afin de disposer des connaissances nécessaires et de tenir compte des intérêts des différents milieux qui pourraient être touchés par la révision de la loi sur la protection des données. Chargé d'accompagner les réflexions sur la réforme, ce groupe comprend des représentants de l'administration fédérale, des cantons, des milieux scientifiques ainsi que des organisations de l'économie et des consommateurs (ci-après : groupe d'accompagnement)[2]. L'OFJ a tenu plusieurs séances avec le groupe

[1] Rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données (FF 2012 255).

[2] Le groupe d'accompagnement est composé des personnes suivantes: Rolf Reinhard (préposé DFJP Protection des données, LTrans, protection de l'information), Jean-Philippe Walter (PFPDT suppléant), Stephan Brunner

d'accompagnement entre septembre 2012 et octobre 2014. Ils ont étudié la nécessité de modifier la LPD et résumé les résultats de leurs débats dans la présente esquisse d'acte normatif, en se fondant sur les travaux préliminaires d'un groupe de rédaction[3]. L'esquisse d'acte normatif pourrait servir de base à l'avant-projet de révision de la loi sur la protection des données, si le Conseil fédéral décidait de charger le DFJP d'un tel mandat (voir ch. 8). Au vu des nombreux intérêts représentés au sein du groupe d'accompagnement, différentes options sont souvent proposées pour les mesures législatives. Quelques membres du groupe ont en outre déposé une prise de position séparée sur l'esquisse d'acte normatif (cf. annexe).

Par ailleurs, plusieurs interventions parlementaires portant sur la protection des données, et ayant un rapport avec les travaux de révision en cours, sont pendantes devant les Chambres fédérales ou ont été transmises au Conseil fédéral. Elles sont traitées dans l'esquisse d'acte normatif, en rapport avec les thèmes spécifiques sur lesquelles elles portent.

2. Contexte international

Des réformes de la protection des données sont en cours au sein de l'Union européenne (UE) et au sein du Conseil de l'Europe. Le Conseil fédéral estime nécessaire de tenir compte de ces développements dans la réflexion menée au plan national (cf. ch. 1) :

– Modernisation de la Convention STE 108 du Conseil de l'Europe [4]: la Convention STE 108, que la Suisse a ratifiée, fait l'objet d'un profond remaniement. Cette Convention a vocation à devenir un standard universel minimal du fait qu'elle est ouverte à l'adhésion d'États non membres du Conseil de l'Europe et qu'elle constitue actuellement, avec son protocole additionnel[5], le seul texte international contraignant régissant la protection des données. Début 2011, le Conseil de l'Europe a entamé un processus de modernisation de la Convention STE 108. Cette révision poursuit deux objectifs majeurs : gérer les défis de la vie privée qui résultent de l'utilisation des nouvelles technologies de l'information et de la communication et renforcer le mécanisme de suivi et de mise en œuvre de la Convention STE 108. Le projet de modernisation de la Convention STE 108 pourrait être adopté

(Chancellerie fédérale), Thomas Pletscher/Marlis Henze (economiesuisse), Bruno Baeriswyl (préposé à la protection des données du canton de Zurich, président de « Privatim »), Bertil Cottier (Università della Svizzera italiana), Florence Bettschart (Fédération romande des consommateurs), Marc Langheinrich (Università della Svizzera italiana), Dieter Kläy (Union suisse des arts et métiers), David Rosenthal (Verein Unternehmens-Datenschutz), Jacques Vifian (Bureau fédéral de la consommation), Franz Zeller (Office fédéral de la communication), Philippe Künzler (Archives fédérales, à partir de juillet 2014) et Monique Cossali Sauvain (Office fédéral de la justice, présidence du groupe d'accompagnement).

[3] Entre janvier 2014 et juin 2014, une fraction du groupe d'accompagnement (groupe de rédaction) a élaboré un projet pour l'esquisse d'acte normatif. Il était composé des membres suivants: Jean-Philippe Walter (PFPDT suppléant), Stephan Brunner (Chancellerie fédérale), Bertil Cottier (Università della Svizzera italiana), David Rosenthal (Verein Unternehmens-Datenschutz) et Monique Cossali Sauvain (Office fédéral de la justice, présidence du groupe de rédaction). Cet avant-projet a ensuite été examiné et remanié par le groupe d'accompagnement, entre juillet et octobre 2014.

[4] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RS 0.235.1).

[5] Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (RS 0.235.11).

et ouvert à la signature dans le courant de 2015.[6] La non-ratification de la Convention modernisée par la Suisse paraît peu réaliste au groupe d'accompagnement. Une telle décision aurait un impact négatif considérable sur les flux transfrontières de données, ce qui aurait des conséquences négatives pour l'économie suisse.

– Paquet de réformes de l'UE : les réformes au plan européen comprennent un projet de *« règlement 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* (ci-après: «projet de règlement UE») »[7] d'une part, et un *projet de « directive relatif 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'exécutions de sanctions pénales, et à la libre circulation de ces données »* (ci-après: «projet de directive UE»)[8] d'autre part. Le projet de règlement UE remplacera la Directive 95/46/CE[9]. Le projet de directive UE remplacera la décision-cadre 2008/977/JAI[10]. Les réformes entreprises par l'UE poursuivent les buts suivants: moderniser le système juridique en matière de protection des données, renforcer les droits des individus, réduire les formalités administratives afin d'assurer une libre circulation des données personnelles dans l'UE et au-delà, améliorer la clarté et la cohérence des règles de l'UE pour la protection des données personnelles et réaliser une application et une mise en œuvre cohérentes et efficaces du droit à la protection des données personnelles dans tous les domaines d'activités de l'UE.

  La Suisse n'est liée par les deux projets susmentionnés que dans la mesure où ils constituent un développement des acquis de Schengen/Dublin. Tel est clairement le cas du *projet de directive UE*. La question est encore ouverte pour ce qui est du *projet de règlement UE*. Dans les domaines qui ne relèvent pas des accords de Schengen/Dublin, la Suisse est considérée comme un État tiers. L'échange de données avec l'UE est alors en principe soumis à la condition que cette dernière reconnaisse à la législation suisse en matière de protection des données un niveau de protection équivalent (décision d'adéquation), ce qui est actuellement le cas. La Suisse, si elle souhaite conserver ce statut, a donc tout intérêt à renforcer sa législation en se rapprochant de la législation européenne, même si elle n'est pas tenue de coller au projet de règlement UE.

  Le calendrier de la réforme de l'UE est encore flou. La phase de trilogue (réunion tripartite informelle à laquelle participent des représentants du Parlement européen, du Conseil et de la Commission) n'a pas encore débuté. La réforme ne devrait pas aboutir avant fin 2015.

---

[6] La dernière séance du comité ad hoc chargé d'examiner le projet de modernisation de la Convention STE 108 (Ad Hoc Committee On Data Protection [CAHDATA]) aura lieu début décembre 2014.

[7] Cf. <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52012PC0011&qid=1410779268743> (Proposition de la Commission du 25 janvier 2012).

[8] Cf. <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52012PC0010&qid=1410777949926> (Proposition de la Commission du 25 janvier 2012).

[9] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281. p. 31 – 50).

[10] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO L 350/60, p. 60 – 71).

Les réformes en cours entraînent les conséquences suivantes pour la révision de la LPD:

– Le projet de révision de la LPD faisant suite à l'évaluation de 2011 devrait permettre dans toute la mesure du possible la ratification du projet de modernisation de la *Convention STE 108* (pour autant que la révision de la Convention aboutisse dans un délai raisonnable): la présente esquisse d'acte normatif tient compte des exigences du projet de modernisation dans son état actuel provisoire[11].
– Le *projet de règlement UE*, s'il lie la Suisse, ne le fera que pour les domaines relevant des accords de Schengen/Dublin. La présente esquisse tient malgré tout compte de ses orientations et s'en inspire de manière générale pour tous les traitements de données. La révision de la loi ne saurait en aucun cas aller moins loin que le droit actuel, sous peine de compromettre la décision d'adéquation en vigueur dans les domaines «non Schengen/Dublin».
– Les modifications entraînées par la transposition du *projet de directive UE* se feront vraisemblablement à part, à la fois pour des raisons de calendrier et pour des raisons de clause référendaire (art. 141a al. 2 Cst.), bien qu'une jonction des deux projets ne soit pas exclue. Elles devront se limiter aux modifications liées à la transposition de la directive. Il s'agira d'assurer la cohérence et la coordination des différents travaux de révision ; une esquisse d'acte normatif pour la transposition du projet de directive UE sera soumise à part.

Indépendamment des réformes en cours au niveau européen, la Suisse devra tenir compte des recommandations reçues dans le cadre de la deuxième évaluation Schengen (application correcte des dispositions Schengen relatives à la protection des données) qui a eu lieu en 2014.

Ce contexte de réformes européennes a évidemment des incidences sur le calendrier (cf. ch. 8).

3. Position des membres du groupe d'accompagnement quant à l'existence d'un besoin de légiférer

Il y a fondamentalement deux tendances au sein du groupe d'accompagnement s'agissant du besoin de renforcer la législation en matière de protection des données.

Une *minorité du groupe d'accompagnement*, représentée par les milieux économiques, estime qu'une révision de la LPD ne se justifie pas et que le droit actuel est en l'état suffisant pour garantir les droits et obligations des personnes concernées. Cette partie du groupe d'accompagnement souhaite que le Conseil fédéral attende l'aboutissement des travaux au sein de l'UE et au sein du Conseil de l'Europe et qu'il ne propose que les modifications exigées pour pouvoir accéder au marché (libre circulation des données).

La *majorité du groupe d'accompagnement* estime que la loi actuelle mérite d'être révisée et qu'il convient d'aller de l'avant sans attendre l'entrée en vigueur des révisions au plan européen. Cette fraction préconise par ailleurs une révision plus ambitieuse de la loi, qui ne se limiterait pas aux adaptations exigées pour l'accès au marché. La législation sur la protection des données ne doit en effet pas simplement servir à régir les échanges de données entre particuliers dans une optique commerciale. Elle a une vocation bien plus large, et doit notamment mettre en œuvre le droit constitutionnel de tout un chacun de se déterminer libre-

[11] Version du 18 décembre 2012 (avec les propositions de modernisation adoptées par la 29e réunion plénière» ;cf. <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)04Rev4_F_Convention %20108%20modernisée%20version%20F.pdf>).

ment sur les données personnelles qu'il souhaite partager. L'État se doit donc de proposer des mesures efficaces pour concrétiser ce droit, et ce sans attendre qu'on l'y contraigne.

Les membres du groupe d'accompagnement qui sont opposés à la révision de la loi ont néanmoins formulé des remarques s'agissant du présent document, pour le cas où le Conseil fédéral décidait de poursuivre les travaux. Leur avis est ainsi pris en compte dans les opinions exprimées ci-après.

Plusieurs membres du groupe ont souhaité fournir une prise de position ad hoc sur l'esquisse d'acte normatif (cf. annexe).

4. Contenu essentiel de la révision

Les propositions ci-après relatives à l'adaptation de la LPD aux développements technologiques et sociétaux (ou aux menaces que ceux-ci font peser sur la sphère privée) [12] s'insèrent dans l'actuelle structure de la loi. Elles prévoient, outre une partie générale énonçant les principes du traitement des données applicables aussi bien aux organes de la Confédération qu'aux auteurs privés de traitements (voir plus bas, ch. 4.1 à 4.7), des dispositions spécifiques concernant le traitement de données par des particuliers (ch. 4.8) et par les organes fédéraux (ch. 4.9). D'autres propositions concernent l'organisation et les tâches des autorités de contrôle (ch. 4.10), les sanctions pénales (ch. **Erreur ! Source du renvoi introuvable.**) et les dispositions finales (ch. 4.12).

La présente esquisse d'acte normatif ne s'attache en revanche pas en détail au thème du Big Data (« mégadonnées ou données massives »). On parle de Big Data lorsqu'une grande quantité de données provenant de différentes sources sont saisies et enregistrées à l'aide de systèmes de traitement à très haut débit, en vue de permettre leur exploitation et leur analyse sans but prédéterminé et sans limite de temps[13]. Le Big Data implique de nouveaux enjeux pour le droit sur la protection des données (p. ex. eu égard aux principes de reconnaissabilité et de finalité ou à la ré-individualisation de données anonymes). Les conséquences du Big Data ne sont toutefois pas encore bien connues. Jusqu'ici, la doctrine juridique n'a traité en détail que quelques aspects de cette problématique[14]. En conséquence, la présente esquisse d'acte normatif ne propose pas de solutions globales, mais uniquement des mesures ponctuelles permettant de s'attaquer aux défis que le Big Data pose en matière de protection des données[15]. Un examen approfondi des implications du Big Data pour la protection des données pourrait avoir lieu dans le cadre des travaux de mise en œuvre de la

---

[12] Les mesures de protection des données peuvent entrer en conflit avec d'autres intérêts. Lors de l'examen de mesures législatives en la matière, il convient par conséquent de tenir compte non seulement de la protection de la personnalité, mais encore d'autres intérêts concernés (en particulier intérêts de l'économie, droit à la liberté d'opinion et d'information ainsi que d'autres intérêts spécifiques, tant privés que publics). Voir à ce propos le rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255, 267 et 269.

[13] Cf. la définition de ce terme sur le site du PFPDT http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=fr .

[14] Cf. BAERISWYL, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber/Thouvenin (édit.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zurich etc., 2014, pp. 46 ss.

[15] En font notamment partie les propositions de réglementation relatives au principe du « Privacy by Design » (cf. ch. 4.3.2), à l'analyse de l'impact potentiel du traitement de données (cf. ch. 4.3.2), au droit d'accès relatif à la structure logique du traitement des données (cf. ch. 4.4.3) ou aux décisions individuelles automatisées (cf. ch. 4.4.6).

motion Rechsteiner 13.3841 « Commission d'experts pour l'avenir du traitement et de la sécurité des données »[16].

4.1 Concept et mise en œuvre

4.1.1 Concept

Le groupe d'accompagnement propose de conserver une seule loi pour les secteurs privé et public. La garantie d'un développement coordonné et harmonieux de la protection des données en droit privé et en droit public passe en effet par une réglementation commune des problèmes inhérents aux deux domaines. Dans cette perspective, le groupe d'accompnement a, dans la mesure du possible, harmonisé les règles pour les deux secteurs afin de créer un cadre commun pour le traitement des données personnelles, et prévu des solutions différentes uniquement lorsque cela était indispensable.

Le but de la loi restera inchangé. La future loi devra conserver son caractère technologiquement neutre et se limiter comme maintenant à fixer des principes généraux, ceci afin de s'appliquer à une palette de situations la plus large possible.

L'idée de regrouper dans la loi tout ou partie des dispositions contenues dans les lois spéciales (sorte de codification du droit de la protection des données au niveau fédéral) a été abandonnée : de l'avis du groupe d'accompagnement, cela n'apporterait aucune plus-value. Un examen de la législation fédérale a révélé que la grande majorité des dispositions de protection des données contenues dans les lois spéciales visent à créer une base légale spécifique pour le domaine concerné ou à concrétiser les principes de la LPD pour le domaine concerné. Elles ne peuvent dès lors pas être remplacées par des dispositions générales dans la LPD, et les rassembler dans un code n'apporterait aucun avantage du point de vue légistique.

4.1.2 Mise en œuvre

a) Renforcement des pouvoirs de l'autorité de contrôle et facilitation de l'accès à la justice pour les particuliers

Une majorité du groupe d'accompagnement estime que le rapport d'évaluation du Conseil fédéral a montré des lacunes dans la mise en œuvre (« Durchsetzung ») de la LPD. Ces dernières sont principalement dues au fait que notre autorité de contrôle[17], en l'occurrence le PFPDT n'a aujourd'hui que peu de pouvoirs, et au fait que les personnes concernées font rarement valoir leurs droits en justice, vu la disproportion entre le bénéfice d'une éventuelle victoire judiciaire et les risques – principalement financiers – et les efforts liés à l'ouverture d'une procédure. Ces deux facteurs nuisent à une application effective de la loi, et condui-

[16] La motion Rechsteiner 13.3841 « Commission d'experts pour l'avenir du traitement et de la sécurité des données », que le Parlement a transmise le 4 juin 2014, charge le Conseil fédéral d'instituer une commission d'experts interdisciplinaire pour répondre à des questions relatives aux développements technologiques et politiques dans le domaine du traitement et de la sécurité des données, et d'en étudier l'importance pour l'économie, la société et l'État suisses. Ce groupe d'experts doit également formuler des recommandations pour la Suisse. La responsabilité de ce dossier incombe au Département fédéral des finances (DFF).

[17] Des propositions sont formulées au ch. 4.10 de la présente esquisse d'acte normatif pour adapter les tâches et les compétences / l'organisation de l'autorité de contrôle. La terminologie choisie pour la future surveillance de la protection des données s'aligne sur celle des réformes de l'UE et du Conseil de l'Europe, ce qui évite aussi de déterminer la forme de l'organisation par un choix linguistique. On parlera d' « autorité de contrôle ».

sent à une perte de contrôle et de maîtrise des données. Elles impliquent qu'une grande partie des cas de violation de la LPD ne sont pas constatés et perdurent. De plus, l'effet préventif de la loi est fortement diminué dans la mesure où les responsables de traitements, qui n'ont que peu de raison de craindre d'être remis à l'ordre, peuvent être tentés de ne pas tenir compte de cette éventualité dans leur comportement. Une meilleure mise en œuvre de la loi passe donc par un renforcement des pouvoirs de l'autorité de contrôle, soit l'octroi d'une compétence de rendre des décisions, voire de prononcer des sanctions et/ou par un renforcement des droits, principalement procéduraux, des personnes concernées.

La majorité du groupe est favorable à un renforcement des pouvoirs de l'autorité de contrôle. Elle estime en effet que le déséquilibre croissant et systématique dans les rapports entre les personnes concernées et les auteurs de traitements – souvent de grandes entreprises – qui se concrétise notamment par des politiques de traitement de données peu transparentes, voire par l'absence de possibilité de librement choisir l'utilisation qui sera faite de ces données, commande plus que de simples recommandations. Ce constat a déjà été fait dans de nombreux pays européens, tels la France, l'Italie, la Grande-Bretagne, la Suède ou l'Espagne, où les autorités de contrôle ont la faculté de rendre des décisions contraignantes, voire de prononcer des amendes.[18] Dans un monde globalisé où les échanges internationaux de données sont de plus en plus fréquents, il est primordial que notre autorité de contrôle dispose de moyens comparables à ceux de ses homologues étrangers. Notons aussi que le projet de modernisation de la Convention STE 108 prévoit que les autorités de contrôle disposent de pouvoirs de décision (un tel pouvoir est par ailleurs aussi prévu par le projet de directive UE [art. 46)] et le projet de règlement UE [art. 53]). Si le texte est adopté, et que la Suisse souhaite le ratifier, elle devra donc prévoir une telle compétence dans sa législation. Enfin, dans le cadre de la deuxième évaluation Schengen, l'UE a recommandé à la Suisse de doter le PFPDT du pouvoir de rendre des décisions contraignantes. Dans ses observations, l'UE a encore ajouté que le renforcement des pouvoirs de sanction du PFPDT serait le bienvenu.

Le groupe d'accompagnement est en revanche plus mitigé s'agissant de la question du renforcement des droits des personnes concernées. *Une partie* estime que les possibilités de faciliter l'accès à la justice pour les personnes concernées sont trop compliquées à mettre en œuvre et trop peu efficaces (voir les réflexions menées dans le cadre des prétentions des parties aux ch. 4.8.3 et 4.9.5) pour mériter que l'on entreprenne de gros chantiers. Par ailleurs, il ressort de l'évaluation de la LPD que les droits actuellement inscrits dans la loi sont, en comparaison internationale, déjà plutôt bien développés[19]. Cette fraction du groupe préconise donc de privilégier un renforcement significatif des pouvoirs de l'autorité de contrôle, et d'améliorer ponctuellement les droits des personnes concernées. *Une autre partie du groupe d'accompagnement* estime quant à elle qu'il existe des mesures efficaces pour renforcer l'accès des personnes concernées à la justice et qu'il convient aussi de les proposer. La protection des droits des individus est en effet un problème avéré selon le rapport d'évaluation. Pour cette partie du groupe, il s'agit également de parer à l'éventualité que les propositions relatives au renforcement du rôle de l'autorité de contrôle soient refusées au

[18] Cf. Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz du 10 mars 2011, pp. 172 et 213 s.; disponible en ligne (en allemand) <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

[19] Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz du 10 mars 2011, pp. 72 ss., 212 s.; disponible en ligne (en allemand) <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

cours du processus législatif en raison des ressources supplémentaires qu'elles nécessiteraient.

Une minorité du groupe d'accompagnement estime quant à elle qu'il n'est pas nécessaire de renforcer les pouvoirs de l'autorité de contrôle ni les moyens à disposition des personnes concernées pour faire valoir leurs droits. Des éventuelles modifications législatives ne doivent intervenir à ses yeux que dans la mesure de ce qui est nécessaire, en regard du droit UE et du projet de modernisation de la Convention STE 108, pour l'accès au marché (cf. ch. 3).

b) Règles plus détaillées

Le caractère général et technologiquement neutre des règles de la LPD entraîne, dans le secteur privé surtout, une certaine incertitude quant aux comportements à adopter, tant pour les auteurs de traitements que pour les personnes concernées, ce qui nuit à la mise en œuvre efficace de la loi. Afin de remédier à cette problématique et d'améliorer la prévisibilité du droit, le groupe d'accompagnement propose de compléter les principes généraux de la loi par des dispositions plus détaillées, applicables au secteur privé, voire au secteur public. On pourrait ainsi avoir des règles détaillées sur des thèmes qui suscitent aujourd'hui de nombreuses questions, comme la vidéosurveillance, le « Big Data », le commerce électronique ou le « Cloud Computing ». Ces règles permettraient également de préciser des notions figurant dans la loi (p. ex : « risque accru », cf. ch. 4.3.2) ou les modalités de certains droits (par ex: le droit à l'effacement, cf. ch. 4.4.5).

La question est de savoir si ces dispositions doivent êtres contraignantes ou non. Les deux tendances sont représentées dans le groupe d'accompagnement :

- Les règles contraignantes auraient l'avantage d'obliger directement leurs destinataires. Leur élaboration susciterait toutefois de nombreuses questions en lien avec le principe de la légalité (délégation de compétences, densité normative, légitimité de l'autorité qui les édicterait), et leur modification prendrait du temps, dans la mesure où il faudrait passer par le processus normal de modification des ordonnances interne à l'administration fédérale.
- Les règles non contraignantes (« bonnes pratiques », « bons usages ») seraient moins problématiques sous l'angle principe de la légalité. Elles sont modifiables très rapidement, et laissent une marge de manœuvre pour les responsables de traitements qui peuvent aussi appliquer d'autres règles. Pour inviter les auteurs de traitements à suivre ces règles, on pourrait instituer une présomption légale selon laquelle un traitement est licite pour autant que son auteur ait respecté les règles de bonnes pratiques. Cette présomption vaudrait pour les auteurs de traitements privés et publics. On pourrait par exemple s'inspirer de l'art. 52a de l'ordonnance sur la prévention des accidents professionnels (OPA; RS 832.30). Cette disposition prévoit que l'employeur est présumé se conformer aux prescriptions sur la sécurité au travail s'il observe les directives émises par la commission de coordination (al. 2). L'employeur peut cependant aussi se conformer aux prescriptions sur la sécurité au travail d'une autre manière que celle qui est prévue par les directives, s'il prouve que la sécurité des travailleurs est également garantie (al. 3). Non contraignantes, ces règles de bonnes pratiques reposeraient toutefois principalement sur la bonne volonté de leurs destinataires, ce qui pourrait réduire leur efficacité.

Une majorité du groupe d'accompagnement propose que l'élaboration de ces règles (contraignantes ou non contraignantes) soit confiée à un comité spécialisé (ci-après: « comité »),

distinct de l'autorité de contrôle au sens étroit (cf. aussi ch. 4.10.2, let. c, et ch. 4.10.3). Cet organe serait composé d'experts indépendants, et non de représentants des milieux concernés.[20] Les milieux intéressés seraient consultés pour l'élaboration des règles. Le comité pourrait aussi leur donner mandat d'élaborer eux-mêmes de telles règles. Les milieux concernés pourraient par ailleurs soumettre spontanément leurs règles pour approbation au comité.[21] Dans tous les cas, ces dernières seraient mises en consultation auprès des associations de protection des consommateurs.

- Variante: Le comité ne pourrait élaborer des règles de bonnes pratiques que si le mandat donné aux milieux concernés de le faire eux-mêmes n'est pas réalisé dans un certain délai.

Une *minorité du groupe* s'oppose à l'institution d'un comité spécialisé, qui engendrerait des charges administratives et financières supplémentaires et affaiblirait la protection des données. Elle propose que cette compétence soit conférée à l'autorité de contrôle elle-même (cf. ch. 4.10.3).

4.2 Champ d'application et terminologie

4.2.1 Champ d'application

a) Champ d'application personnel

La loi sur la protection des données régit le traitement de données personnelles, aussi bien par des personnes privées que par des organes fédéraux (cf. art. 2, al. 1, LPD). La LPD ne s'applique toutefois pas au traitement de données personnelles par des organes cantonaux, sous réserve de l'art. 37 LPD. La question de l'adéquation de cette répartition des compétences[22] entre Confédération et cantons a également été examinée ici. Le groupe d'accompagnement s'est demandé, dans une perspective d'harmonisation, s'il ne faudrait pas étendre le champ d'application de la LPD aux organes cantonaux. Une telle extension de la compétence législative de la Confédération en matière de protection des données requérrait une révision de la Constitution fédérale.

Une consultation effectuée par la Conférence des gouvernements cantonaux (CdC) auprès des cantons à la demande de la cheffe du DFJP a montré que la majorité des cantons ne sont pas favorables à l'extension du champ d'application de la loi aux traitements de données effectués par les organes cantonaux. Lors du Dialogue confédéral de l'automne 2013, la cheffe du DFJP a déjà fait savoir aux cantons qu'elle ne poursuivrait pas l'idée d'une unifi-

---

[20] La loi – respectivement l'ordonnance – devra encore prévoir notamment des règles sur l'élection, la période de fonction ou les conflits d'intérêts des membres du comité, ainsi que sur la position de ce dernier par rapport à l'autorité de contrôle elle-même.

[21] La loi fédérale autrichienne sur la protection des données se rapportant à des personnes (Datenschutzgesetz 2000) connaît une procédure allant dans ce sens. Le § 6, al. 4, stipule ainsi: « Pour définir plus précisément ce qui doit être considéré comme une utilisation de données de bonne foi dans les différents domaines, il est possible, pour le secteur privé, de confier à des organismes professionnels de représentation légale, à d'autres associations professionnelles ou à des institutions similaires le soin d'élaborer des règles de comportement. De telles règles ne peuvent être publiées qu'après avoir été soumises au chancelier fédéral, qui doit en examiner la conformité avec les dispositions de la présente loi fédérale et constater que tel est le cas. » (traduction non officielle).

[22] Cf. le rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255, 268.

cation du droit de la protection des données. Le champ d'application devrait donc à l'avenir se limiter, comme aujourd'hui, aux traitements de données effectués par des organes fédéraux et par des privés, de même que par des organes cantonaux en exécution du droit fédéral aux conditions de l'art. 37 LPD.

La LPD s'appliquera comme aujourd'hui aux médias. Une attention particulière sera cependant portée au besoin de prévoir des dispositions spéciales afin de protéger le secret de rédaction, en particulier dans le cadre du droit d'accès (cf. ch. 4.4.3). Il faudra aussi tenir compte de l'intérêt des médias dans le cadre du « droit à l'oubli » (cf. ch. 4.4.5).

b) Champ d'application à raison de la matière

La loi sur la protection des données d'applique au traitement de données concernant des personnes physiques et morales (art. 2, al. 1, LPD). Elle se distingue ainsi de la Convention STE 108 et de la législation de plusieurs États européens, qui ne protègent que les personnes physiques. Le groupe d'accompagnement a donc examiné s'il était justifié de maintenir cette protection pour les personnes morales.

Une majorité du groupe d'accompagnement a conclu que la LPD devait continuer de s'appliquer aux données de personnes morales. Elle estime que l'exclusion de ces dernières ne cadrerait pas avec le système juridique suisse, en vertu duquel les personnes morales bénéficient de la protection de la personnalité garantie par le code civil (art. 53 en relation avec les art. 28 ss CC [RS 210]). La majorité du groupe d'accompagnement considère au surplus que la non-application de la LPD aux données de personnes morales pourrait aboutir à des résultats problématiques. Elle souligne que les entreprises familiales et les petites entreprises surtout peuvent avoir besoin que leurs données soient protégées au même titre que les données de personnes physiques, notamment lorsque les informations relatives à la personne morale ont un rapport avec les personnes physiques la dirigeant.

La proposition de la majorité du groupe d'accompagnement prévoit toutefois que le traitement de données de personnes morales dans le cadre de leurs activités commerciales soit ajouté à la liste des intérêts privés prépondérants de l'art. 13, al. 2, LPD (cf. plus bas, ch. 4.8.2). Cette solution faciliterait les transactions commerciales dans la pratique, sans compromettre par trop la protection des données des personnes morales. Il ne s'agirait pas d'un motif justificatif absolu (pas plus que les autres intérêts énumérés à l'art. 13, al. 2, LPD) qui autoriserait en soi un traitement de données. Il faudrait ici également procéder à une pesée des intérêts, en tenant compte de toutes les circonstances du cas particulier. Lorsque le traitement porte sur des données ne concernant pas les activités commerciales, les personnes morales disposeraient d'ailleurs de tous les moyens de droit prévu par la LPD.

Enfin, pour faciliter les échanges de données transfrontières avec des pays dont l'ordre juridique ne protège pas les données personnelles de personnes morales, la majorité du groupe d'accompagnement propose d'arrêter dans la loi que l'adéquation de la protection des données selon l'art. 6 LPD n'implique pas que la législation étrangère protège les données personnelles de personnes morales (cf. plus bas, ch. 4.5).

Une minorité du groupe d'accompagnement souhaite que les données personnelles de personnes morales soient entièrement exclues du champ d'application de la LPD. Elle motive son choix par le fait que la législation de nombreux États européens, de même que le projet de modernisation de la Convention STE 108 protègent exclusivement les droits des personnes physiques. Elle estime en outre que la protection de la personnalité des personnes morales est déjà assurée à satisfaction par le CC (art. 28 ss), la loi fédérale contre la concurrence déloyale (LCD ; RS 241) et le secret d'affaires. Il serait dans tous les cas envisageable de soumettre les données personnelles des personnes morales à la LPD lorsqu'une personne physique est reconnaissable comme propriétaire d'une entreprise individuelle.

c) Champ d'application territorial

L'évaluation de la LPD a révélé que la dimension internationale du traitement des données ne cessait de gagner en importance en raison des développements technologiques. Les traitements transfrontières de données sont de plus en plus fréquents, ce qui débouche sur des situations complexes et peu transparentes pour les personnes concernées et pour les autorités de contrôle, ainsi que pour les auteurs de traitements[23]. Le groupe d'accompagnement s'est par conséquent demandé si ces nouveaux défis appellaient une adaptation du champ d'application territorial de la LPD (en particulier en ce qui concerne l'applicabilité de la loi à des faits de portée internationale).

L'actuelle LPD ne contient aucune disposition définissant explicitement son champ d'application territorial. Le droit international privé fournit des règles de conflits de loi spéciales pour les dispositions de droit privé de la LPD. La loi fédérale sur sur le droit international privé (LDIP; RS 291) définit notamment les compétences des tribunaux ou des autorités suisses en matière de protection des données, sous réserve de traités internationaux (art. 129, al. 1[24] et 130, al. 3, LDIP[25]) ainsi que les prétentions fondées sur une atteinte à la personnalité liées au traitement de données personnelles (cf. en particulier art. 139 LDIP[26]). Selon le groupe d'accompagnement, cette réglementation permet d'appliquer les dispositions de droit privé de la LPD de manière assez large (soit aussi à certains traitements de données à l'étranger). Il ne propose par conséquent aucune modification dans ce domaine.

Le droit public par contre ne connaît pas de règles spécifiques de conflits de lois internationaux. C'est le principe de la territorialité qui s'applique aux dispositions de droit public de la LPD, à savoir que le droit suisse ne s'applique qu'aux faits qui se produisent en Suisse. Selon la jurisprudence du Tribunal fédéral, le droit public suisse peut, dans certaines circonstances, être appliqué aussi à des faits survenus à l'étranger lorsque ceux-ci ont des répercussions suffisantes sur le territoire suisse (principe des effets)[27]. *Une majorité du groupe d'accompagnement* propose de codifier explicitement cette jurisprudence dans la LPD pour

---

[23] Cf. le rapport du Conseil fédéral sur l'évaluation de la loi sur la protection des données, FF 2012 255, 260 s., 267.

[24] Art. 129, al. 1, LDIP: « Les tribunaux suisses du domicile ou, à défaut de domicile, ceux de la résidence habituelle du défendeur sont compétents pour connaître des actions fondées sur un acte illicite. Sont en outre compétents les tribunaux suisses du lieu de l'acte ou du résultat et, pour connaître des actions relatives à l'activité de l'établissement en Suisse, les tribunaux du lieu de l'établissement. »

[25] Art. 130, al. 3, LDIP: « Les actions en exécution du droit d'accès dirigées contre le maître du fichier peuvent être intentées devant les tribunaux mentionnés à l'art. 129 ou devant les tribunaux suisses du lieu où le fichier est géré ou utilisé. »

[26] En vertu de l'art. 139, al. 3, en relation avec l'al. 1 LDIP, les prétentions fondées sur une atteinte à la personnalité résultant du traitement de données personnelles sont régies, « au choix du lésé: a. par le droit de l'État dans lequel le lésé a sa résidence habituelle, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État ; b. par le droit de l'État dans lequel l'auteur de l'atteinte a son établissement ou sa résidence habituelle, ou c. par le droit de l'État dans lequel le résultat de l'atteinte se produit, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État. »

[27] Pour le principe des effets comme particularité du principe de territorialité, voir en particulier ATF 133 II 331, 341 consid. 6.1. S'agissant du droit sur la protection des données, le Tribunal fédéral a retenu, par exemple dans ATF 138 II 346, 352 s. consid. 3.3 (« Google Street View »), que les images qui ont été prises en Suisse et sont publiées d'une façon qui permet d'y accéder en Suisse également ont un lien prépondérant avec la Suisse, même si les images sont traitées à l'étranger et ne sont pas mises en ligne directement depuis la Suisse.

le droit public de la protection des données[28]. L'intention est de souligner que la LPD s'applique également à des faits qui ont des répercussions en Suisse, même si le traitement des données a lieu à l'étranger. De tels faits doivent en outre relever du domaine de compétence de l'autorité de contrôle. *Une minorité du groupe d'accompagnement* se prononce contre cette proposition. Elle est d'avis qu'une codification de la jurisprudence du Tribunal fédéral relative aux principes de territorialité et des effets déboucherait sur une insécurité juridique. Elle relève qu'il n'y a pas non plus de définition légale du principe de territorialité dans d'autres domaines du droit. Cette solution entraînerait des incertitudes sur la question de savoir si et dans quelle mesure la jurisprudence du Tribunal fédéral continuera à s'appliquer à la protection des données. On risquerait d'aboutir à des divergences – non prévues par le groupe d'accompagnement – par rapport à la pratique du Tribunal fédéral.

Etant donné que la LPD peut être appliquée aussi à des auteurs de traitements de données qui n'ont pas de domicile (siège) en Suisse, le groupe d'accompagnement propose en outre d'obliger, dans certains cas, ces personnes à indiquer une adresse de correspondance en Suisse afin d'accélérer la procédure (cf. plus bas, ch. 4.10.2 let. a/aa).

d) Exceptions au champ d'application

da) Traitement à des fins exclusivement personnelles

L'exception prévue à l'actuel art. 2, al. 2, let. a, LPD devrait être adaptée à l'art. 3, al. 1bis, du projet de modernisation de la Convention STE 108[29]. Le groupe d'accompagnement propose de supprimer la condition de la non-communication à des tiers, et de reformuler la disposition en ce sens que la LPD ne s'applique pas aux traitements de données effectués par une personne physique pour des activités exclusivement personnelles. Sont ici visées principalement les communications à des parents et des amis proches. Les « amis » sur les réseaux sociaux[30] n'entrent pas dans cette catégorie s'il n'y a pas de lien étroit.

db) Autres exceptions

Vu le statut particulier dont jouit le Comité international de la Croix-Rouge (CICR), le groupe d'accompagnement propose de maintenir l'actuelle clause d'exception de l'art. 2, al. 2, let. e, LPD, qui exclut du champ d'application de la loi les données personnelles traitées par celui-là. Le groupe d'accompagnement part donc du principe qu'une telle dérogation restera possible selon le projet de modernisation de la Convention STE 108. La raison de cette exception réside dans le fait que le CICR est de plus en plus reconnu comme un sujet de droit international public et que ces sujets ne peuvent pas être soumis sans autre au droit interne d'un Etat[31]. La doctrine critique notamment le fait que d'autres organisations internationales ne soient pas mentionnées dans cette clause d'exception de la LPD, soulignant que cette différence de traitement est problématique en regard du principe d'égalité inscrit dans la

---

[28] On trouve une disposition analogue dans le droit sur la concurrence par exemple, à l'art. 2, al. 2, de la loi sur les cartels (LCart; RS 251): « La présente loi est applicable aux états de fait qui déploient leurs effets en Suisse, même s'ils se sont produits à l'étranger. »

[29] Art. 3, al. 1bis, du projet de modernisation de la Convention STE 108: « La présente Convention ne s'applique pas aux traitements de données effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. »

[30] Sur la problématique des réseaux sociaux, voir le rapport du Conseil fédéral « Cadre légal pour les médias sociaux: Rapport en réponse au postulat Amherd 11.3912 du 29 septembre 2011 ».

[31] Cf. le message du 23 mars 1988 concernant la loi fédérale sur la protection des données (LPD), FF 1988 II 421, 447 s..

Constitution (art. 8 Cst.)[32]. Dans le message du 19 février 2003 relatif à la révision de la LPD[33], le Conseil fédéral avait exprimé l'intention d'exclure expressément du champ d'application de la LPD toutes les organisations internationales établies sur le territoire de la Confédération avec lesquelles un accord de siège a été conclu. Cette réglementation n'a toutefois pas été reprise par la Parlement, raison pour laquelle le groupe d'accompagnement ne propose pas non plus, dans le cadre des présents travaux, une extension dans ce sens de l'art. 2, al. 2, let. e, LPD.

Les autres exceptions au champ d'application de la LPD ne pourront à notre sens être maintenues que si les exigences du projet de modernisation de la Convention STE 108 sont remplies dans le domaine concerné. Ce projet abroge la possibilité pour les États de faire des réserves concernant le champ d'application de la Convention [34].

- Le groupe d'accompagnement est d'avis que l'exception concernant les registres publics relatifs aux rapports juridiques de droit privé doit être supprimée (art. 2, al. 2, let. d, LPD), et ce pour plusieurs raisons. D'abord, le fait que ces domaines soient régis par des lois spéciales ne justifie pas une exception. En effet, d'autres secteurs, bien que réglés par des lois spéciales, sont aussi soumis à la LPD (p. ex : le casier judiciaire). Ensuite, cette exclusion est aujourd'hui artificielle dans la mesure où le PFPDT est très souvent sollicité dans ces domaines pour des questions relevant justement de la LPD. Enfin, ces matières sont bien souvent imbriquées avec d'autres, qui, elles, sont soumises à la LPD, ce qui rend la dichotomie difficile à mettre en œuvre. Il sera toujours possible de tenir compte des particularités des registres dans des dispositions spéciales.
- Pour les autres exceptions (soit l'art. 2, al. 2, let. b et c, LPD), il faudrait examiner si elles restent valables, si elles doivent être modifiées ou si les exigences du projet de modernisation de la Convention STE 108 (voire du droit UE) doivent être transposées dans les législations spéciales. Deux options concrètes sont ressorties des discussions au sein du groupe d'accompagnement : soit on supprime les exceptions et le domaine est alors soumis à la LPD, soit on les maintient et on vérifie que les lois spéciales sont à niveau.

4.2.2 Définitions

Le groupe d'accompagnement propose de maintenir la définition actuelle de « données personnelles » (art. 3, let. a, LPD) ainsi que celle de « fichier » (art. 3, let. g, LPD) et de « communication » (art. 3, let. f, LPD). Il ne voit en effet aucune raison de modifier ces notions, qui sont aujourd'hui bien intégrées dans la pratique des autorités de contrôle et des tribunaux suisses.

La liste des définitions et la terminologie devront au besoin être adaptées à celle du projet de modernisation de la Convention STE 108. Cela vaut en particulier pour la définition des « données sensibles » (art. 3, let. c, LPD). Le projet prévoit d'y inclure les données génétiques et les données biométriques. Pour éviter d'aller trop loin (p. ex. pour que toute photo ne soit *per se* considérée comme une donnée sensible), on pourrait restreindre la définition sur le modèle de l'art. 6, al. 1, du projet de modernisation de la Convention STE 108[35]. Le

---

[32] Cf. MAURER-LAMBROU/KUNZ, in: « Basler Kommentar DSG/BGÖ », 3e éd., Bâle 2014, N 41 ad art. 2 LPD.

[33] Cf. FF 2003 1915, 1926 s.

[34] La Suisse, au moment de son adhésion à l'actuelle Convention STE 108, avait déclaré que celle-ci ne s'appliquait pas aux fichiers constitués et utilisés par les parlements fédéral et cantonaux dans le cadre de leurs délibérations et aux fichiers du Comité international de la Croix-Rouge ; RO 2002 2847, 2869.

[35] Art. 6, al. 1, du projet de modernisation de la Convention STE 108 : « Le traitement de données génétiques ou

groupe d'accompagnement propose au surplus de prévoir, si les personnes morales devaient être maintenues dans le champ d'application de la loi (ch. 4.2.1, let. b), que seules les données concernant les personnes privées sont susceptibles d'être considérées comme sensibles.

S'agissant du terme « maître du fichier »/« Inhaber der Datensammlung » (art. 3, let. i, LPD), le groupe d'accompagnement a débattu de l'opportunité d'aligner la terminologie sur celle de la Convention STE 108 et du droit européen, qui utilisent la notion respectivement de « responsable du traitement »[36] et « für die Verarbeitung Verantwortlichen »[37]. Les conséquences matérielles d'une telle adaptation, étant donné que les notions utilisées dans le droit suisse et dans le droit européen ne se recoupent pas totalement, doivent encore être examinées en détail. Un alignement terminologique ne doit pas déboucher sur une insécurité juridique.

Il pourrait être opportun de définir dans la loi les notions de « sous-traitants » et de « destinataires ». Dans le cas contraire, la formulation de l'actuel art.10a LPD pourrait être revue afin d'éviter une confusion avec la notion de « tiers » utilisée dans d'autres dispositions (p. ex: art. 9, 12, 13 ou 14 LPD).

Le groupe d'accompagnement propose enfin d'abandonner la notion de « profils de la personnalité », qui est propre à la Suisse et qui a peu d'effets en pratique, dans la mesure où les obligations particulières liées à l'existence de tels profils (p. ex : art. 4, al. 5, et 14 LPD) sont rarement respectées, principalement dans le secteur privé. Le groupe d'accompagnement propose d'appréhender la problématique par des moyens plus efficaces, tels une règlementation sur les décisions automatisées (ch. 4.4.6) ou une approche fondée sur le risque (cf. ch. 4.3.2).

4.3 Principes généraux de protection des données personnelles

4.3.1 Transparence des traitements

Actuellement, la question de la reconnaissabilité de la collecte des données et celle du devoir d'information sont réglées à des endroits différents, soit à l'art. 4, al. 4, LPD, et aux art. 14 (secteur privé) et 18 à 18b LPD (organes fédéraux). *Une majorité du groupe d'accompagnement* propose de traiter ces deux thèmes dans une seule et même disposition, applicable aux secteurs privé et public, ce qui aurait le mérite de simplifier la loi et d'éviter les redondances. Cette disposition prévoirait une *obligation d'informer* pour toutes les catégories de données traitées, comme c'est déjà le cas actuellement pour le secteur public (et comme cela est prévu par le projet de modernisation de la Convention STE 108[38] et le droit de l'UE[39]). On renoncerait donc à faire une distinction entre données sensibles et données non sensibles. La personne concernée devrait être informée – dans la mesure où elle ne l'est pas déjà – des données qui sont collectées et dans quel but elles le sont, des éventuelles caté-

---

de données concernant des infractions, condamnations pénales et mesures de sûreté connexes, le traitement de données biométriques identifiant un individu de façon unique, ainsi que le traitement de données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle, n'est autorisé qu'à la condition que la loi applicable prévoit des garanties appropriées, venant compléter celles de la présente Convention. »

[36] Cf. art. 2, let. d, du projet de modernisation de la Convention STE 108.

[37] Cf. art. 4, al. 5, du projet de règlement UE ainsi que l'art. 3, al. 6, du projet de directive UE.

[38] Cf. art. 7bis du projet de modernisation de la Convention STE 108.

[39] Cf. art. 14 du projet de règlement UE et art. 11 du projet de directive UE.

gories de destinataires ainsi que des droits qui lui sont conférés par la loi. Les coordonnées du responsable du traitement devraient par ailleurs lui être communiquées afin qu'elle puisse le contacter. Le devoir d'information serait réputé être respecté s'il découle manifestement des circonstances que la personne devrait avoir connaissance de tous les éléments pertinents. Les modalités de ce devoir pourraient être précisées dans des règles de bonnes pratiques ou dans des règles contraignantes (cf. ch. 4.1.2, let. b). Outre le cas où la personne concernée a déjà été informée, il conviendrait de prévoir une exception au devoir d'informer lorsque le traitement est prévu par la loi ou lorsque l'information implique des efforts disproportionnés, ou encore lorsqu'il s'agit de préserver la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers. La disposition concernant le devoir d'information serait conçue comme un principe de traitement des données.

Une minorité du groupe d'accompagnement s'oppose à l'introduction d'un devoir général d'information. Elle estime, notamment, que cela représenterait une charge de travail disproportionnées pour les entreprises.

Un autre instrument important de la transparence des traitements est le droit d'accès de la personne concernée, qu'elle peut exercer auprès du maître du fichier. Le groupe d'accompagnement propose de renforcer ce droit. Ce thème est abordé plus loin, au ch. 4.4.3.

4.3.2 Mesures de diligence

Conformément à ce que prévoient les art. 7 et 8bis, al. 2, 3 et 4, du projet de modernisation de la Convention STE 108, et de manière à mettre en œuvre les postulats Schwaab 13.3806 « La protection de la sphère privée doit être garantie par défaut » et 13.3807 « Un renforcement de la protection des données grâce au „privacy by design" »[40] et le postulat Recordon 13.3989 « Violations de la personnalité dues au progrès des techniques de l'information et de la communication »[41], le groupe d'accompagnement propose d'introduire une obligation pour le responsable du traitement ou, le cas échéant, pour le sous-traitant, de prendre certaines mesures afin de prévenir les violations de la loi[42] et de les éliminer, ou d'en réduire les conséquences[43].

Les devoirs de diligence suivants en font notamment partie :

– Mesures d'ordre technique et organisationnel garantissant la sécurité des données.

---

[40] Les postulats Schwaab 13.3806 et 13.3807 du 25 septembre 2013 n'ont pas encore été traités par le Conseil national.

[41] Le postulat Recordon 13.3989 du 27 septembre 2013 a été adopté par le Conseil des Etats le 11 décembre 2013.

[42] À ce propos, il conviendra d'étudier, lors de la suite des travaux de révision de la LPD, si le principe de précaution, qui prend ses racines dans le droit environnemental, ne pourrait pas être repris comme principe général dans le domaine de la protection des données. Concernant le principe de précaution dans le droit de l'environnement, voir en particulier l'art. 1, al. 2, de la loi sur la protection de l'environnement (LPE; RS 814.01): « Les atteintes qui pourraient devenir nuisibles ou incommodantes seront réduites à titre préventif et assez tôt. » Voir aussi sur ce sujet le document de synthèse du groupe de travail interdépartemental "principe de précaution" d'août 2003 intitulé « Le principe de précaution en Suisse et au plan international ».

[43] Le 17 septembre 2014, un postulat Schwaab 14.3739 « Control by design: Renforcer les droits de propriété pour empêcher les connexions indésirables » a été déposé. Le Conseil fédéral propose son adoption. Les mesures de diligence envisagées dans ce chapitre pourraient concrétiser en partie le postulat, s'il était adopté par la suite.

- Principe du « Privacy by Design »: obligation pour les responsables du traitement de données (ou de leurs éventuels sous-traitants), dès la conception du traitement – pour autant qu'il porte sur des données personnelles – de tenir compte des exigences en matière de protection des données[44] et de prévoir des mesures de protection adéquates (p. ex : limitation au strict minimum des données traitées par l'application; sauvegarde décentralisée des données personnelles obtenues; intégration de mesures de sécurité techniques permettant de réduire le risque de traitements illicites des données). Pour l'application de cette obligation, il convient de prendre en considération notamment les risques que le traitement de données prévu présente pour la protection de la personnalité, les possibilités techniques, les standards reconnus ainsi que les coûts liés aux mesures. Dans ce cadre, on portera une attention particulière aux besoins de protection des mineurs et d'autres groupes de personnes particulièrement vulnérables.
- Principe du « Privacy by Default » : si les utilisateurs d'une application traitant des données ont la possibilité de choisir entre différents paramétrages, le réglage par défaut sera celui qui assure la plus grande protection des données personnelles [45]. Il convient de tenir compte tout spécialement du besoin de protection des mineurs et d'autres groupes de personnes particulièrement vulnérables.
- Documenter des processus de traitement des données : l'idée est que la protection des données ne peut être garantie que par celui qui sait quelles données il traite et comment ; cette condition ne peut être remplie que par une documentation adéquate lorsque la taille et la complexité d'une entreprise ainsi que la quantité de données traitées dépassent un certain niveau. Dans les grandes entreprises, une telle documentation doit retranscrire, avec une certaine précision, le traitement des données, les procédures et les opérations, l'organisation et les attributions ainsi que les moyens. Il existe des réglementations similaires dans d'autres textes législatifs (voir p. ex. art. 4 de l'ordonnance concernant la tenue et la conservation des livres de comptes ([Olico ; RS 221.431]). Cette documentation pourrait remplacer l'actuel registre des fichiers au sens de l'art. 11a LPD (cf. ch. 4.7) et peut-être aussi le règlement de traitement. Selon le groupe d'accompagnement, il n'est pas opportun de prévoir un droit d'accès à la documentation. Ce dernier ne contribuerait guère à la transparence, et la documentation en question contiendrait généralement aussi de nombreux secrets d'affaires, ainsi que des informations relatives à la sécurité. L'accès du PFPDT est réservé.
- Analyses d'impact: lorsque le traitement est susceptible de créer un risque accru d'atteinte à la personnalité, le responsable du traitement devrait procéder à des analyses de l'impact potentiel du traitement de données envisagé sur les droits des personnes concernées et fournir sur demande cette analyse à l'autorité de contrôle; là aussi, une attention particulière devrait être portée à l'impact sur les personnes mineures et les autres personnes vulnérables. On trouve des exemples d'analyses d'impact dans la législation

[44] On trouve un dispositif de réglementation analogue dans le domaine du droit de l'environnement et de l'aménagement du territoire, par exemple à l'art. 3 de l'ordonnance sur les chemins de fer (OCF ; RS 742.141.1): « Il y a lieu de tenir compte, dès la planification et l'établissement des projets, des exigences de l'aménagement du territoire, de la protection de l'environnement, ainsi que de celle de la nature et du paysage » (al. 1). « Il sera tenu compte de manière appropriée des besoins des handicapés » (al. 2).

[45] Le principe du « Privacy by Default » est étroitement lié au principe de la proportionnalité et à celui du « Privacy by Design ». Pour les auteurs de traitements de données, il peut en découler, dans certains cas, une obligation d'offrir aux utilisateurs un choix entre différents paramétrages du système.

suisse[46] (p. ex : art. 7 de l'ordonnance relative à l'étude de l'impact sur l'environnement[47], à l'art. 5 de la loi sur les produits chimiques[48] ou art. 5 de l'ordonnance de la Commission fédérale des maisons de jeu sur le blanchiment d'argent[49]).

– Obligation de signaler les violations des données à l'autorité de contrôle: à l'instar des réformes visées par le Conseil de l'Europe, le groupe d'accompagnement propose l'introduction d'une obligation de signaler les violations de données à caractère personnel (« data breaches »; pour la définition de ce terme, voir l'art. 4, al. 9, de la du projet de règlement UE[50]). L'art. 7, al. 2, du projet de modernisation de la Convention STE 108 stipule – en se fondant sur le droit de l'UE[51] – que l'autorité de contrôle (à tout le moins) doit être informée, sans retard injustifié, de violations de données qui pourraient porter gravement atteinte aux droits de la personnalité des personnes concernées. Pour déterminer quelles violations doivent être signalées, il convient de définir des critères dans la loi ou dans des règles de concrétisation (p. ex. des règles de bonnes pratiques ; voir ch. 4.1.2, let. b). *Une partie du groupe d'accompagnement* estime que l'obligation d'aviser l'autorité de contrôle ne doit être prévue que pour les cas où un grand nombre de personnes sont concernées par la violation de données. *D'autres membres du groupe* doutent en revanche qu'une telle réglementation ne satisfasse aux exigences du projet de modernisation de la Convention STE 108. Ils prônent dès lors l'établissement d'un catalogue de critères non exhaustif, qui prenne en compte notamment le type de données concernées et le risque concret pour les droits de la personnalité des personnes concernées. Outre l'obligation d'aviser l'autorité de contrôle, le groupe d'accompagnement propose d'obliger d'une manière générale les auteurs de traitements de données (ou leurs éventuels sous-traitants) à prendre des mesures appropriées pour limiter les dommages (p. ex : information des personnes concernées de la violation de données).

– Institution d'un conseiller à la protection des données : *une partie des membres du groupe d'accompagnement* propose de prévoir, dans les mesures de diligence, l'obligation pour les entreprises d'une certaine taille (p. ex. plus de 250 personnes en équivalent plein-temps), d'instituer un conseiller à la protection des données. Le Conseil fédéral pourrait étendre cette obligation aux entreprises plus petites qui présentent un risque accru. La notion de « risque accru » serait précisée dans le message, l'ordonnance ou encore des règles de bonnes pratiques ou des dispositions règlementaires (cf. ch. 4.1.2, let. b). Il s'agirait vraisemblablement des cas impliquant des données sensibles, des données per-

---

[46] Cf. aussi le rapport britannique suivant: <https://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment>.

[47] OEIE; RS 814.011.

[48] LChim; RS 813.1.

[49] OBA CFMJ; RS 955.021.

[50] En vertu de l'art. 4, al. 9, du projet de règlement UE une « violation de données à caractère personnel » est « une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière ».

[51] Concernant l'actuelle situation juridique, voir l'art. 4, al. 3, de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ainsi que le règlement (UE) N° 611/2013 du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE. *De lege ferenda* voir les art. 31 s. du projet de règlement UE et les art. 28 s. du projet de directive UE.

sonnelles concernant des mineurs ou d'autres personnes vulnérables, des données qui servent au profilage ou encore qui sont interconnectées à d'autres données (voir p. ex. art. 21 de l'ordonnance relative à la loi fédérale sur la protection des données [OLPD; RS 235.11]). À noter que les entreprises pourraient recourir à des conseillers externes afin notamment de bénéficier d'un savoir-faire qu'elles n'auraient pas autrement, sauf à engager une personne expressément, ou à former un employé dans ce but, ce qui pourrait constituer une charge financière importante. *Une autre partie du groupe d'accompagnement* estime qu'il ne faut pas mentionner cette obligation dans la loi, mais laisser aux règles de bonnes pratiques (cf. ch. 4.1.2 let. b) le soin de prévoir le ou les moyens les plus adéquats pour assurer un traitement des données respectueux des droits des personnes concernées selon les entreprises en cause (p. ex. la désignation d'un conseiller à la protection des données).

Au sein des organes fédéraux, il devrait impérativement y avoir un conseiller (« Datenschutzverantwortlicher ») au sens des art. 12a et 12b OLPD, qui exerce ses fonctions de façon indépendante et sans recevoir d'instructions[52] (cf. plus bas, ch. 4.9.4), à la place de l'actuel conseiller (« Berater für den Datenschutz ») selon l'art. 23 OLPD. Cette obligation doit s'appliquer au moins au niveau des départements. L'obligation pour les offices de disposer d'un conseiller à la protection des données pourrait dépendre du type et de la quantité de données traitées.

– Aux fins d'améliorer la prise en compte de la protection des données, en particulier dans les projets informatiques, une *partie du groupe d'accompagnement* propose d'examiner l'opportunité d'obliger les organes fédéraux à mettre en place dans les départements des systèmes de gestion de la protection des données et de la sécurité informatique. D'autres devoirs de diligence (p. ex. le principe du « Privacy by Design » ou l'obligation d'évaluer l'impact sur la protection des données) pourraient toutefois déjà suffire à imposer une telle mesure ; ce point devrait plutôt être réglé au niveau ordonnance.

4.3.3 Consentement

Pour ce qui est des exigences liées au consentement, traitées actuellement dans les principes (art. 4, al. 5, LPD), le groupe d'accompagnement propose, pour autant que cette solution soit compatible avec le projet de modernisation de la Convention STE 108, de maintenir le système en vigueur. *Le groupe d'accompagnement* estime par ailleurs qu'il convient de prendre des mesures pour améliorer la qualité du consentement. En effet, à l'heure actuelle, en raison d'un défaut d'information ou d'un processus informatif trop complexe, mais aussi parfois d'un défaut de curiosité, les personnes concernées consentent à des traitements qu'elles ne connaissent pas, ne comprennent pas, qui ne les intéressent pas, ou parfois même qu'elles ne choisissent pas. Un renforcement du devoir d'information (ch. 4.3.1), le choix systématique de technologies respectueuses des droits des particuliers (ch. 4.3.2), ou encore une sensibilisation accrue par l'autorité de contrôle (ch. 4.10.2, let. d) permettraient d'améliorer la situation. Ces mesures pourraient être concrétisées par des règles de bonnes pratiques, voire des réglementations contraignantes (ch. 4.1.2, let. b).

4.3.4 Autres principes

Les autres principes contenus dans les actuels art. 4 et 5, al. 1, et 7 LPD devraient être

[52] Les tâches et la position du conseiller à la protection des données (Datenschutzverantwortlicher) sont expliquées sur le site du PFPDT, à l'adresse suivante : http://www.edoeb.admin.ch/datenschutz/00626/00743/00874/01051/index.html?lang=fr.

maintenus dans la mesure où ils ont fait leurs preuves.

4.4 Droits des personnes concernées

4.4.1 Introduction

La protection des droits individuels, parallèlement à la surveillance par l'autorité de contrôle, joue un rôle central dans la garantie du respect du droit de la protection des données. Comme cela a été expliqué plus haut, *une partie du groupe d'accompagnement* estime que les possibilités de renforcer la protection des droits individuels par le biais des dispositions légales sont minces (voir ch. 4.1.2, let. a, ainsi que ch. 4.8.3 et 4.9.5). Quoi qu'il en soit, l'évaluation de la LPD a révélé que les personnes concernées font rarement valoir leurs droits à l'encontre des auteurs de traitements de données, surtout dans le secteur privé. Cette retenue pourrait résider dans une méconnaissance des prétentions existantes et des procédures applicables [53]. Le groupe d'accompagnement propose par conséquent :

- d'améliorer la structure et la lisibilité de la LPD afin que les personnes concernées voient clairement quels sont leurs droits (cf. ch.4.4.2) ; et
- de renforcer, au moins ponctuellement, les droits des personnes concernées (cf. ch. 4.4.3 ss) ainsi que les procédures de mise en œuvre (voir ch. 4.8.3, let. b, et 4.9.5, let. c), en particulier dans les domaines où des lacunes subsistent en comparaison des travaux de réforme de la protection des données entrepris par le Conseil de l'Europe.

4.4.2 Catalogue des prétentions

Les dispositions concernant les droits des personnes concernées sont actuellement réparties dans différents articles et sections de la loi (le droit à la rectification est ainsi réglé à l'art. 5, al. 2, à l'art. 15, al. 1, et à l'art. 25, al. 3, let. a, LPD). Les prétentions sont en partie formulées aussi sous forme de moyens procéduraux, qui ne sont pas toujours délimités nettement les uns par rapport aux autres, mais se recoupent en partie. Il est par conséquent difficile pour les intéressés de connaître précisément leurs droits. Le groupe d'accompagnement estime également que la structure de l'actuelle LPD ne fait pas clairement ressortir que les personnes concernées peuvent (et devraient) faire valoir directement leurs droits (d'accès, d'opposition, à la rectification, à l'effacement, de blocage etc.) auprès des auteurs de traitements et qu'il n'est pas nécessaire d'introduire d'abord une action en justice. Le groupe d'accompagnement propose donc de dresser un catalogue des prétentions que peuvent faire valoir les personnes concernées, comme l'ont fait du reste le Conseil de l'Europe[54] et l'UE[55] dans leurs projets de réforme, ou comme c'est le cas à l'art. 25 LPD (prétentions et procédure en rapport avec le traitement de données par des organes fédéraux). Il serait ainsi plus facile pour les personnes concernées de savoir quels droits elles peuvent faire valoir à l'encontre de qui et, cas échéant, d'agir judiciairement. Les prétentions devraient autant que possible être les mêmes pour les secteurs public et privé. En font notamment partie :

- le droit d'accès (« Auskunftsrecht »; cf. plus bas, ch. 4.4.3) ;
- le droit à la rectification de données personnelles erronées (« Berichtigung »; cf. plus bas, ch. 4.4.4);

---

[53] Voir le rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255, 260 s.

[54] Cf. l'art. 8 du projet de modernisation de la Convention STE 108.

[55] Cf. le chapitre III du projet de règlement et du projet de directive UE.

- le droit à l'effacement (« Löschung ») ou le droit à la destruction (« Vernichtung ») de données personnelles ayant fait l'objet d'un traitement illicite (cf. plus bas, ch. 4.4.5);
- le droit de faire interdire un traitement illicite ou la communication de données personnelles à des tiers (« Sperrung ») ;
- le droit de faire mentionner le caractère litigieux (« Bestreitungsvermerk »), lorsque ni l'exactitude ni l'inexactitude d'une donnée personnelle ne peut être établie ;
- le droit d'opposition (« Widerspruch ») à un traitement de données sans motif justificatif ;
- le droit pour la personne concernée de ne pas être soumise à une décision fondée sur un traitement purement automatique de données qui la touche de manière substantielle, sans qu'elle ne puisse faire valoir son point de vue (cf. ch. 4.4.6).

Ce catalogue des droits doit permettre aux intéressés de mieux comprendre la loi sur la protection des données. En revanche, l'actuel système d'exercice des droits (p. ex. s'agissant de la légitimation active et passive) doit pour l'essentiel rester inchangé sur le plan matériel. Les prétentions en réparation (dommages-intérêts, réparation pour tort moral, remise de gain) doivent continuer à obéir aux conditions générales du droit de responsabilité civile et publique (voir pour l'ensemble, voir ch. 4.8.3 et 4.9.5).

Différentes mesures sont proposées ci-après pour renforcer les droits des personnes concernées en matière de protection des données.

4.4.3 Droit d'accès

Le groupe d'accompagnement propose de compléter les dispositions sur le droit d'accès de manière à améliorer la transparence des traitements. Sur demande, et comme le prévoit le projet de modernisation de la Convention STE 108, le responsable du traitement devrait également communiquer à la personne concernée la durée de conservation ainsi que le raisonnement qui sous-tend le traitement de données dont les résultats lui sont appliqués (cf. art. 8, let. c et d, du projet de modernisation de la Convention STE 108).

De plus en plus souvent, les données personnelles sont structurées en fonction des applications pour établir des profils éphémères. Il n'existe alors pas de fichier permanent, ce qui rend le droit d'accès inopérant. Le groupe d'accompagnement est conscient de ce problème. *Une partie du groupe* estime qu'il doit être résolu par le biais du devoir d'information (voir ch. 4.3.1) et non par le biais du droit d'accès.

Il faut en outre examiner l'opportunité de concrétiser les modalités du droit d'accès selon l'art. 8, al. 5, LPD. Il pourrait par exemple être arrêté que la charge (coûts compris) que représente la fourniture des renseignements doit être proportionnelle par rapport au but du droit d'accès (p. ex. consultation des informations sur place à la place d'une notification par écrit).

L'art. 8, al. 6, LPD doit être revu de manière à ce qu'il ressorte clairement de sa formulation ou de sa structure qu'il est possible de renoncer par avance à la fourniture de renseignements par écrit, pour autant que la consultation soit dûment assurée.

Une partie du groupe d'accompagnement souhaite introduire de manière générale une pesée des intérêts pour l'exercice du droit d'accès, lorsque les données sont archivées ou stockées en raison d'une obligation légale. Il s'agira de vérifier si cette solution est compatible avec le projet de modernisation de la Convention STE 108, ce dont doutent certains membres du groupe.

Pour ce qui est des restrictions au droit d'accès, *une partie du groupe d'accompagnement* estime qu'il convient de supprimer la condition de la non-communication des données à un

tiers qui figure à l'actuel art. 9, al. 4, LPD, dans la mesure où ce critère n'a aucun lien avec les intérêts prépondérants du maître de fichier. La loi contiendrait plutôt une liste exemplative de ce qui est susceptible de constituer un tel intérêt. Il s'agirait par exemple de la sauvegarde d'intérêts commerciaux ou industriels, de l'atteinte grave aux intérêts de la source d'information, de la non-révélation d'une stratégie judiciaire dans une procédure qui opposerait le responsable du traitement à la personne concernée ou des demandes d'accès chicanières. *Une autre partie du groupe d'accompagnement* estime qu'une telle option affaiblirait la position de la personne concernée et propose de conserver la condition de l'absence de communication des données à un tiers. La loi ou l'ordonnance prévoiraient alors des exceptions, dans le respect de l'art. 9 du projet de modernisation de la Convention STE 108.

Il faut enfin réfléchir à l'opportunité d'insérer dans la loi la teneur de l'actuel art. 1, al. 7, OLPD, qui concerne la consultation des données d'une personne décédée. Cette disposition est en effet dépourvue de base légale, dans la mesure où la LPD ne régit pas les données des personnes décédées.

4.4.4 Droit à la rectification

Le droit à la rectification doit être complété de la manière suivante : si une personne responsable du traitement de données reçoit une demande de rectification de données et la considère comme justifiée, elle doit en informer les éventuels destinataires dont elle a connaissance afin que ces informations soient également corrigées en aval. Cette exigence ne doit pas être absolue ; il est possible de prévoir des restrictions (p. ex. si l'information aux destinataires est impossible ou disproportionnée par rapport à l'importance de l'erreur).

4.4.5 Droit à l'effacement

Ce droit existe aujourd'hui déjà; la personne dont les données sont traitées en violation de la LPD peut demander à l'auteur du traitement et au juge, sous réserve de l'existence d'un motif justificatif, que ses données soient effacées ou retirées d'un site internet par exemple, mais aussi d'un programme informatique (cf. art. 15 et 25 LPD). Il s'agit ici plus de mentionner expressément ce droit à titre symbolique, dans la perspective de faciliter la compréhension de la loi pour les personnes concernées. Cette mention expresse ne changera rien au plan matériel. Il sera par exemple toujours possible de traiter des données contre la volonté des personnes concernées en présence d'intérêts prépondérants, tels l'intérêt des médias ou la recherche historique[56].

Le groupe d'accompagnement propose d'utiliser les termes de « droit à l'effacement » plutôt que de « droit à l'oubli », cela principalement pour coller à la terminologie du Conseil de l'Europe (art. 8, let. e, du projet de modernisation de la Convention STE 108). Le droit à l'effacement sera renforcé par l'introduction des mesures de diligence (ch. 4.3.2), le renforcement du droit d'accès (ch. 4.4.3) et ses modalités précisées dans des règles de bonnes pratiques ou des règles contraignantes (ch. 4.1.2, let. b).

Le groupe d'accompagnement estime qu'avec ces mesures, il aura réalisé le postulat Schwaab 12.3152 « Droit à l'oubli numérique »[57] et partiellement réalisé le postulat Recordon 13.3989 « Violations de la personnalité dues au progrès des techniques de l'information et de la communication ».

---

[56] Voir pour une décision en ce sens l'arrêt de la CEDH n° 33846/07 «Wegrzynowski et Smolczewski c. Pologne» du 16 juillet 2013.

[57] Le postulat Schwaab 12.3152 du 14 mars 2012 a été adopté par le Conseil national le 15 juin 2012.

4.4.6 Décisions individuelles automatisées

Les nouvelles technologies de l'information et de la communication, font que de plus en plus souvent, des décisions produisant des effets juridiques pour les personnes concernées ou pouvant les affecter de manière significative sont prises dans le cadre de procédures automatisées, voire sur la base de profils reposant sur des données statistiques et des calculs (profilage). *Une majorité du groupe d'accompagnement* estime qu'il y a un besoin accru de protection en particulier lorsque de telles procédures de décision portent sur les caractéristiques d'une personne, par exemple sa solvabilité[58], sa fiabilité, son comportement ou des risques spécifiques[59]. L'UE s'est dotée il y a quelque temps déjà de prescriptions sur l'admissibilité de décisions individuelles automatisées[60]. La mise en œuvre de ces dispositions ne pose pas, à notre connaissance, de problème dans les États membres.

La majorité du groupe d'accompagnement propose dès lors de conférer à toute personne le droit – en conformité avec l'art. 8, let. a, du projet de modernisation de la Convention STE 108[61] – de ne pas être soumise à une décision fondée sur un traitement purement automatique et qui l'affecterait de manière significative, sans que son point de vue ne soit pris en compte, avant ou après la décision automatique. Le but est d'empêcher que l'évaluation d'aspects de la personnalité se fasse de façon entièrement automatique, sans intervention humaine et sans que la personne concernée n'apprenne comment cette décision a été prise. Celle-là doit avoir la possiblité de faire valoir ses arguments et d'éventuels faits qui n'auraient pas été pris en compte dans l'évaluation afin que la dimension humaine soit intégrée en dépit du traitement automatisé des données.

Dans ce contexte, il faut encore examiner plus précisément quelles procédures doivent être qualifiées de décisions individuelles automatisées au sens décrit ci-dessus. Le retrait d'argent à un guichet automatique ou l'envoi de prospectus à une série de personnes déterminées par ordinateur ne devraient par exemple, pas être soumis à la réglementation proposée, comme c'est le cas en droit européen. Par ailleurs, il ne doit pas s'agir d'un droit absolu, des exceptions légales pouvant être prévues. Il convient de préciser que la réglementation proposée ne doit pas empiéter sur la liberté de se déterminer et la liberté contractuelle (pas d'obligation de contracter), ni entraîner une obligation de motiver les décisions individuelles automatisées.

Une minorité du groupe d'accompagnement souhaite que ce droit soit complété par un droit de s'opposer au profilage prédictif automatisé, sous réserve d'exceptions, comme le prévoit l'art. 20 du projet de règlement UE. Les profils qui en résultent peuvent en effet entraîner des erreurs d'appréciation ou des discriminations.

---

[58] Le profilage est utilisé dans le secteur bancaire par exemple en rapport avec l'octroi de crédits et l'analyse de risque de clients, présents ou futurs (credit-scoring).

[59] Cf. le message du Conseil fédéral du 19 février 2003 relatif à la révision de la loi sur la protection des données (LPD), FF 2003 1915, 1945: ce serait le cas par exemple si une assurance responsabilité civile rangeait une conductrice possédant une petite voiture dans une classe de risque moins élevée qu'un conducteur qui a une voiture de sport.

[60] Voir en particulier l'art. 15 de la directive 95/46/CE et l'art. 7 de la décision-cadre 2008/977/JAI. Le projet de règlement UE prévoit à l'art. 20 des dispositions relatives aux « mesures fondées sur le profilage », tout comme l'art. 9 du projet de directive UE.

[61] Art. 8, let. a, du projet de modernisation de la Convention STE 108 : « Toute personne doit pouvoir: (...) ne pas être soumise à une décision l'affectant de manière significative, qui serait prise sur le seul fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte ».

Une autre minorité du groupe d'accompagnement s'oppose à l'introduction d'un tel droit.

Concernant le droit de renseignement sur la structure logique du traitement des données, voir plus haut ch. 4.4.3.

4.4.7 Droit à la portabilité des données

Une partie du groupe d'accompagnement propose que l'on introduise dans la LPD un droit à la portabilité des données pour les personnes concernées, comme le prévoit le projet de règlement UE (art. 18 du projet de la Commission). *Une autre partie du groupe d'accompagnement* est d'avis que ce droit relève plus du droit de la concurrence ou du droit des médias[62] que de la protection des données et estime ainsi que l'on ne doit pas l'introduire dans la LPD. Le groupe d'accompagnement propose de suivre les travaux au plan européen, et de réexaminer la question si ce droit devait être maintenu dans le projet de règlement UE.

4.5 Communication transfrontière de données

Pour l'essentiel, les règles contenues dans l'actuel art. 6 LPD ont fait leurs preuves. Le groupe d'accompagnement prévoit toutefois quelques modifications.

L'art. 6, al. 2, let. d, LPD — qui prévoit que malgré l'absence d'une législation assurant un niveau de protection adéquat à l'étranger, des données personnelles peuvent être communiquées à l'étranger si la communication est, en l'espèce, indispensable à l'exercice ou la défense d'un droit en justice — pose un problème d'interprétation. Le texte allemand diverge des textes français et italien. Alors que ces derniers parlent de « la constatation, l'exercice ou la défense d'un droit en justice » et de « accetertare, esercitare o far valere un diritto in giustizia » respectivement, la version allemande parle de « Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht ».

Certains auteurs considèrent que l'exception doit être interprétée largement, la procédure ne devant pas forcément se dérouler devant un tribunal[63]. *Une partie du groupe d'accompagnement* soutient cette opinion, et estime qu'il convient d'adapter le texte allemand aux textes français et italien. *Une autre partie du groupe* estime au contraire que les exceptions, sous peine de vider la protection des données de son contenu en cas d'échange de données avec l'étranger, ne doivent concerner que les procédures devant un tribunal et préconise ainsi d'adapter les textes latins à l'allemand.

Le groupe d'accompagnement propose au surplus d'étendre l'exception de l'actuel art. 6, al. 2, let. e, LPD à la vie et à l'intégrité corporelle de tiers. Il est en effet possible que des données personnelles de la personne concernée soient indispensables à la sauvegarde de tels intérêts mais que celle-là ne soit pas atteignable (p. ex. : une adresse, un numéro de téléphone, ou des données médicales).

---

[62] Pour ce qui est de la problématique de la portabilité des données dans le cadre de l'utilisation des médias sociaux, et du besoin de légiférer dans ce domaine, voir le rapport du Conseil fédéral «Cadre légal pour les médias sociaux : Rapport en réponse au postulat Amherd 11.3912 du 29 septembre 2011», pp. 37 s. et 78.

[63] MEIER, Protection des données, Fondements, principes généraux et droit privé, Berne 2011, N 1375, pour qui il s'agit de « toute procédure pendante devant un organe étatique (y compris de juridiction administrative interne) ou reconnu par l'Etat »; MAURER-LAMBROU/STEINER, in: Maurer-Lambrou/Blechta (édit.), Datenschutzgesetz – Öffentlichkeitsgesetz, 3e éd., Bâle 2014, art. 6 LPD, N 33, qui estime qu'il s'agit de « jede Instanz mit Rechtsprechungsfunktion ».

En lien avec l'art. 6, al. 3, LDP, on pourrait prévoir que les garanties mentionnées à l'art. 6, al. 2, let. a, et les règles de protection des données mentionnées à l'art. 6, al. 2, let. g, LPD valent comme protection adéquate lorsque l'autorité de contrôle les a approuvées. L'obtention de l'approbation de l'autorité de contrôle serait facultative. Les entreprises qui le souhaitent pourraient soumettre leurs « Binding Corporate Rules » (BCR)[64]. Les conditions à remplir ainsi que la procédure pourraient être prévues par des règles de bonnes pratiques ou des règles contraignantes (cf. ch. 4.1.2, let. b).

Il convient en outre d'adapter la formulation allemande de la phrase introductive de l'art. 6, al. 2 à la version française (adjonction après « wenn » de « eine der folgenden Bedingungen erfüllt ist »).

Enfin, il faudrait préciser que l'adéquation de la protection des données dans le cadre de la communication transfrontière de données selon l'art. 6, al. 1, LPD ne suppose pas la protection des données de personnes morales (cf. ch. 4.2.1, let. b).

4.6 Procédure de certification

La possibilité de certification selon l'art. 11 LPD doit être maintenue. La formulation de cette disposition mérite cependant d'être revue. S'agissant de la certification de produits, dont la mise en oeuvre a présenté certaines difficultés, le mandat donnée à l'autorité de contrôle d'édicter des directives (voir art. 5, al. 3, de l'ordonnance sur les certifications en matière de protection des données [OCPD; RS 235.13]) doit être transformé en une disposition potestative (Kann-Vorschrift). L'autorité de contrôle jouirait ainsi d'une plus grande marge de manœuvre. Il faut en outre examiner s'il convient d'introduire une certification pour les prestations de service, en tenant compte des développements au niveau européen. La certification devrait de manière générale demeurer facultative. La possibilité de prévoir une certification obligatoire dans des lois spéciales serait maintenue (voir p. ex. art. 59a de l'ordonnance sur l'assurance-maladie [OAMal; RS 832.102]).

4.7 Registre des fichiers

Le groupe d'accompagnement propose de renoncer à la tenue d'un registre des fichiers telle qu'elle est prévue à l'art. 11a LPD, car elle constitue une lourdeur bureaucratique qui a peu d'utilité pratique dans le secteur privé, d'autant que la loi actuelle prévoit déjà des exceptions à l'obligation d'annoncer les fichiers. En lieu et place, le groupe d'accompagnement propose d'introduire, dans les mesures de diligence, un devoir de documenter de manière adéquate les traitements de données (voir ch. 4.3.2). La tenue du registre pourrait être maintenue pour le secteur de l'administration fédérale.

4.8 Dispositions particulières relatives au traitement de données personnelles par des particuliers

4.8.1 Conception de la réglementation

Selon la conception actuelle de la LPD, la protection des données de droit privé complète et concrétise la protection de la personnalité du code civil. Les droits de la personnalité sont indissociables de la personne concernée. Il s'agit de droits absolus, hautement personnels et incessibles. La loi mentionne de façon exemplative les cas dans lesquels un traitement de données constitue une atteinte à la personnalité et indique quels motifs peuvent justifier une

[64] Les « Binding Corporate Rules » désignent, dans l'UE, un code de conduite qui définit la politique interne d'un groupe en matière de transferts de données personnelles hors de l'UE.

telle atteinte. Ce système doit être maintenu. Il n'est pas prévu actuellement de passer à un modèle où les données personnelles seraient protégées par l'attribution de droits de propriété (c.à-d. un droit des disposer et d'utiliser des données personnelles[65]). En effet, le groupe d'accompagnement considère que l'opportunité d'un tel changement de système n'est pas établi. Un droit de maîtrise absolu de chacun sur ses données serait en désaccord flagrant avec d'autres intérêts, tels que la liberté d'opinion et d'information. Le groupe d'accompagnement propose en lieu et place une série d'autres mesures afin d'assurer aux personnes concernées une meilleure maîtrise de leurs données (cf. p. ex. les réglementations proposées pour renforcer l'obligation d'informer [ch. 4.3.1], pour les principes du « Privacy by Design » et du « Privacy by Default » [ch. 4.3.2] ainsi que pour les tâches de l'autorité de contrôle visant à sensibiliser la population aux questions de protection des données [ch. 4.10.2, let. d]).

4.8.2 Atteintes à la personnalité et motifs justificatifs

Les art. 12 et 13 LPD, qui arrêtent les conditions auxquelles les traitements de données personnelles par des privés sont licites, doivent être maintenus. Le groupe d'accompagnement propose toutefois les modifications suivantes :

Répartition du fardeau de la preuve : selon les règles générales en vigueur (art. 8 CC), la personne concernée doit en principe apporter la preuve de l'atteinte à la personnalité, tandis que l'auteur du traitement doit prouver l'existence d'un motif justificatif. La personne concernée pourrait rencontrer des difficultés à apporter cette preuve vu la complexité croissante des méthodes de traitement des données que permettent les développements technologiques. *La majorité du groupe d'accompagnement* souhaite tenir compte de cette évolution et alléger le fardeau de la preuve. À cet effet, elle propose un renversement du fardeau de la preuve, sur l'exemple de l'art. 13a. al. 1, LCD[66]. Le juge pourrait exiger de l'auteur d'un traitement de données qu'il prouve, dans le cas particulier, que le traitement est conforme aux dispositions sur la protection des données, si, compte tenu des intérêts légitimes des parties à la procédure, une telle exigence paraît appropriée (concernant la présomption légale de la régularité d'un traitement de données lorsque les règles de bonnes pratiques sont respectées, voir plus haut ch. 4.1.2, let. b). Une telle exigence pourrait s'appliquer lorsque l'administration des preuves est particulièrement difficile pour la personne concernée, parce que les faits à prouver sont dans la sphère d'influence de l'auteur du traitement (p. ex. en

---

[65] Dans la doctrine, la question de l'introduction de droits de maîtrise ou de droits similaires est discutée depuis quelques temps en lien avec l'exigence d'une amélioration du contrôle sur les données. Chaque personne pourrait avoir un droit absolu et illimité de disposer de ses données. Les avantages avancés pour ce système sont notamment un meilleur contrôle et la participation de chacun au produit financier résultant de l'utilisation de ses données. La critique, elle, concerne la maîtrise absolue des données, qui pourrait déboucher sur une monopolisation du savoir et de l'information. En outre, il est précisé que même dans un tel système il n'y aurait guère de partenaires contractuels égaux dans le « commerce des données ». Voir à ce propos par exemple FLÜCKIGER, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, AJP 2013, pp. 837–864 ou SCHUNCK, Propertisierung von Personendaten?, digma 2013, pp. 66–72. Dans ce contexte, il faut aussi prendre en considération l'initiative parlementaire Derder 14.434 « Protéger l'identité numérique des citoyens », qui vise à inscrire à l'art. 13, al. 2, Cst. que « Ces données sont la propriété de la personne […] ». Cette initiative n'a pas encore été traitée.

[66] Art. 13a, al. 1, LCD: « Le juge peut exiger que l'annonceur apporte des preuves concernant l'exactitude matérielle des données de fait contenues dans la publicité si, compte tenu des intérêts légitimes de l'annonceur et de toute autre partie à la procédure, une telle exigence paraît appropriée en l'espèce. »

rapport avec le respect du devoir de diligence selon le ch. 4.3.2). *Une minorité du groupe d'accompagnement* estime par contre qu'une telle réglementation n'est pas nécessaire, dans la mesure où l'administration des preuves ne constitue pas un problème central dans la pratique. En cas de difficultés concernant la preuve de faits qui sont du ressort de l'auteur du traitement, le juge civil en tient compte dans le cadre de l'obligation de collaborer et de l'appréciation des preuves.

Atteintes à la personnalité : *une partie du groupe d'accompagnement* estime qu'il faut réintroduire explicitement dans l'art. 12, al. 2, let. a, LPD – qui stipule qu'un traitement de données personnelles fait en violation des principes généraux définis constitue toujours une atteinte à la personnalité – la possibilité de faire valoir des motifs justificatifs. La réserve des motifs justificatifs a en effet été rayée de l'art. 12, al. 2, let.a, LPD lors de la révision de la loi du 24 mars 2006[67], à la différence des let. b et c du même article. Pour motiver cette proposition de modification (p. ex. dans le commentaire d'un éventuel projet de révision), il faut souligner que la doctrine majoritaire et le Tribunal fédéral partent du principe qu'une justification du traitement de données personnelles en violation des principes généraux n'est pas exclue d'une manière générale, mais que le motif justificatif ne peut être admis qu'avec la plus grande retenue. *D'autres membres du groupe d'accompagnement* tiennent en revanche à conserver la formulation actuelle. Ils estiment qu'il n'est pas nécessaire de modifier l'art. 12, al. 2, let. a, LPD, vu que le Tribunal fédéral admet, dans certains cas, des motifs justificatifs même avec la teneur actuelle de la disposition.

Motifs justificatifs : le groupe d'accompagnement propose de compléter l'énumération exemplative de l'art. 12, al. 2, LPD, en ajoutant d'autres situations dans lesquelles le traitement de données peut être justifié par des intérêts privés prépondérants, à savoir :

- Traitement de données de personnes morales dans le cadre de leur activité commerciale (p. ex. lorsqu'une personne traite des données concernant sa clientèle et ses fournisseurs ou lorsqu'il s'agit de l'exécution d'un contrat avec ces derniers ; cf. ch. 4.2.1, let. b). *Une partie du groupe d'accompagnement* propose d'étendre ce motif justificatif aux entreprises qui n'ont pas la qualité de personne morale (p. ex. des sociétés simples ou des communautés d'héritiers). Les conséquences juridiques qu'aurait une telle extension doivent encore faire l'objet d'un examen approfondi.
- Traitement de données personnelles en vue de procédures judiciaires ou administratives (en Suisse ou à l'étranger) (par analogie à l'art. 6, al. 2, let. d, lorsque le traitement est indispensable à la constatation, à l'exercice ou à la défense d'un droit). Le groupe n'est toutefois *pas unanime* sur l'opportunité d'inclure aussi les procédures administratives ; cf. ch. 4.5.
- Conclusion ou exécution d'un contrat comme motif justificatif selon l'art. 13, al. 2, let. a, LPD : *une partie du groupe d'accompagnement* estime qu'il faut examiner si les exigences pour justifier un traitement de données ne devraient pas être assouplies, en particulier si le motif justificatif de l'art. 13, al. 2, let. a ne pourrait pas être étendu à des situations où le contrat n'a pas été conclu formellement avec la personne concernée, mais où celle-ci en bénéficie (p. ex. dans le cadre d'un contrat de travail)[68]. Le groupe

[67] Cf. RO 2007 4983.

[68] Concernant la communication de données personnelles à l'étranger ou les échanges entre services internationaux ou intergouvernementaux, la loi allemande sur la protection des données (Bundesdatenschutzgesetz ; BDSG) arrête par exemple à son § 4c, al. 1, ch. 3, que dans le cadre d'activités qui entrent, partiellement ou intégralement, dans le champ d'application du droit de la Communauté européenne, une communication de données

d'accompagnement a décidé de laisser cette question ouverte[69],[70].

- Une *partie du groupe d'accompagnement* souhaite introduire un autre motif justificatif, à savoir le traitement de données personnelles à des fins d'archivage ou de sécurité.

4.8.3 Prétentions et procédures

a) Prétentions

Comme mentionné aux ch. 4.4.1 et 4.4.2, il est prévu d'adapter la structure et la clarté de la LPD afin qu'il soit plus aisé pour les personnes concernées de voir quelles sont leurs prétentions. Il doit notamment ressortir plus clairement de la loi que les personnes concernées peuvent dans un premier temps faire valoir leurs droits auprès des auteurs privés de traitements de données seuls et directement, sans devoir intenter une action en justice. À cet effet, il est prévu notamment de dresser un catalogue des prétentions des personnes concernées, comprenant notamment les droits d'accès, de contestation, de rectification ou d'effacement.

Une majorité du groupe d'accompagnement est en revanche d'avis qu'il ne faut rien changer matériellement à l'actuel système d'exercice des droits (p. ex. s'agissant de la légitimation active et passive). De même, les prétentions en dommages-intérêts ou en réparation pour tort moral doivent continuer à obéir aux règles générales du droit de la responsabilité civile. S'agissant de la remise de gain, les dispositions du CO relatives à la gestion d'affaires sans mandat[71] restent applicables telles quelles (cf. art. 15, al. 1, LPD, en relation avec l'art. 28a, al. 3, CC et les art. 41 ss, 49 et 423 du code des obligations [CO; RS 220]). *Quelques membres du groupe d'accompagnement* proposent en revanche de supprimer la relation avec les dispositions du CC et du CO, et de régler les prétentions qui y sont régies dans la LPD même.

Le groupe d'accompagnement est partagé sur l'opportunité d'introduire une responsabilité objective pour les actions en réparation. Certains estiment qu'il y a dans le domaine de la protection des données trop peu de cas de dommages financiers ou de tort moral pour justifier l'introduction d'une telle responsabilité. D'autres estiment en revanche que le peu d'affaires portées devant les tribunaux ne permet pas de tirer de conclusions quant à l'importance et à la fréquence des cas dans lesquels une indemnité serait justifiée. Ils estiment dès lors que l'introduction d'une responsabilité objective permettrait aux particuliers de faire valoir leurs droits plus facilement. Certains préconisent même d'instituer un système d'indemnisation forfaitaire sur le modèle de l'art. 336a CO pour le licenciement abusif.

---

personnelles à des services autres que ceux qui sont énumérés au § 4, al. 1, est admissible, même si le niveau de protection requis n'est pas garanti, dans la mesure où la communication des données est nécessaire pour conclure ou exécuter un contrat que le service responsable a conclu ou va conclure avec un tiers dans l'intérêt de la personne concernée (traduction non officielle).

[69] Si l'art. 13, al. 2. let. a, LPD devait être modifié, il faudrait également adapter l'art. 6, al. 2. let. c, LPD pour des raisons de cohérence.

[70] Concernant la situation juridique dans l'UE, voir l'art. 6, ch. 1, let. b, du projet de règlement UE: « Le traitement de données à caractère personnel n'est licite que si et dans la mesure où l'une au moins des situations suivantes s'applique: […] le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci » (similaire à l'art. 7, let. b, de la directive 95/46/CE).

[71] Lors des futurs travaux de révision de la LPD, il conviendra d'étudier plus en détail si le renvoi à l'art. 423 CO est un renvoi aux effets juridiques (Rechtsfolgeverweis) ou un renvoi à la cause (Rechtsgrundverweis).

b) Dispositions de procédure

L'évaluation de la LPD a montré que les personnes concernées font rarement valoir leur prétentions. Les raisons avancées dans le rapport d'évaluation du Conseil fédéral sont notamment une relative méconnaissance de ces prétentions et de leur mise en oeuvre (cf. ch. 4.4.1). Il est également possible que les personnes concernées considèrent que l'effort à fournir pour intenter une action est trop important par rapport au bénéfice diffus et incertain d'une victoire judiciaire[72]. Pour ces raisons, le groupe d'accompagnement a étudié différents modèles permettant aux individus d'obtenir la mise en œuvre de leurs droits, tels le renforcement de la position procédurale des personnes concernées dans l'exercice du droit d'opposition, l'introduction de la maxime inquisitoire ou l'application de la procédure simplifiée au sens des art. 243 ss. du code de procédure civile (CPC; RS 272) pour toutes les actions concernant la protection des données[73], l'allégement des frais de procédure ou encore le développement d'instruments d'exercice collectif des droits, sous la forme d'actions des organisations, d'actions de groupe, ou d'actions modèles ou test.

Une *partie du groupe d'accompagnement* estime que l'effet des mesures envisagées ci-dessus serait plutôt faible, c'est-à-dire que les modalités d'exercice des droits des personnes concernées ne seraient que peu facilitées. Ces mesures sont aussi considérées comme problématiques, car elles risquent de rompre le lien entre la LPD et la protection de la personnalité générale du code civil, ce qui créerait deux systèmes distincts dans le droit civil suisse pour garantir la protection de la personnalité. Cette partie du groupe d'accompagnement est donc d'avis que, pour garantir le respect des dispositions de protection des données par les auteurs de traitements privés, il faut avant tout renforcer la surveillance et étendre en conséquences les compétences de l'autorité de contrôle (ch. 4.10.2).

Une autre partie du groupe d'accompagnement est en revanche d'avis qu'il faut aussi proposer des mesures importantes pour renforcer la position des particuliers, car la protection des droits individuels est un problème avéré selon le rapport d'évaluation. Il est par ailleurs selon elle risqué de ne proposer que le renforcement des pouvoirs de l'autorité de contrôle, qui nécessitera des ressources importantes, dans le contexte actuel de restrictions budgétaires imposées par le Parlement.

Pour améliorer, au moins ponctuellement, la protection juridique des personnes concernées, les mesures suivantes sont proposées :

Allégement des frais de procédure : les avis du groupe d'accompagnement sur cette question sont partagés. Certains estiment que ce ne sont pas les frais de justice eux-mêmes, mais bien plus les avances de frais et les dépens potentiels qui dissuadent les parties de faire usage des voies de droit. *Une partie du groupe d'accompagnement* propose de fixer une fourchette nettement réduite pour les frais judiciaires dans les litiges en matière de protection des données, en prenant modèle sur l'art. 65, al. 4 et 5, de la loi sur le Tribunal fédéral (LTF; RS 173.110)[74]. Il convient en outre d'examiner quelles mesures pourraient être

---

[72] Cf. le rapport du Conseil fédéral sur l'évaluation de la loi sur la protection des données, FFI 2012 255, 261 s.

[73] *De lege lata*, la procédure simplifiée n'est applicable qu'aux actions en exécution du droit d'accès selon l'art. 8 LPD (art. 15, al. 4, LPD, en relation avec art. 243, al. 2, let. d, CPC), pour autant qu'il ne s'agisse pas d'une affaire patrimoniale dont la valeur litigieuse ne dépasse pas 30 000 francs (art. 243, al. 1, CPC). Pour le reste, la procédure ordinaire selon les art. 219 ss CPC est applicable à toutes les autres actions en matière de protection des données.

[74] La teneur de l'art. 65, al. 4 et 5, LTF est la suivante : « Il [le montant des frais judiciaires] est fixé entre 200 et 1000 francs, indépendamment de la valeur litigieuse, dans les affaires qui concernent: a. des prestations

prises concernant les avances de frais afin de faciliter l'accès à la justice. *Une autre partie du groupe d'accompagnement* se prononce contre une réglementation spéciale pour le droit sur la protection des données. Si des allégements devaient néanmoins être prévus, il est proposé que, dans l'intérêt de l'unité de l'ordre juridique, ils s'appliquent non seulement aux prétentions fondées sur la LPD, mais également à celles fondées sur les art. 28 et la LCD ; il est précisé que seuls les consommateurs devraient pouvoir en bénéficier. *Plusieurs membres du groupe d'accompagnement* sont d'avis que les allégements ne devraient pas être réservés aux personnes physiques, mais que, le cas échéant, les entreprises devraient également pouvoir en profiter.

Prises de position de l'autorité de contrôle : étant donné la haute technicité de la matière, il peut arriver que l'appréciation juridique des litiges dans le domaine de la protection des données pose certaines difficultés. Dans la mesure où l'autorité de contrôle est un organe spécialisé en la matière, il devrait être possible de lui demander une prise de position dans des procédures de droit civil. Le groupe d'accompagnement propose ce qui suit : si une procédure civile porte sur la licéité d'un traitement de données, le tribunal peut, d'office ou à la demande d'une partie, soumettre l'affaire à l'autorité de contrôle pour prise de position. Celle-la n'est pas tenue de prendre position. Si elle le fait, le tribunal n'est pas obligé d'en tenir compte, et ne perd ainsi pas sa compétence décisionnelle (principe de l'indépendance du pouvoir judiciaire).

Exercice collectif des droits : la LPD ne contient pas de disposition particulière concernant l'exercice collectif des droits des personnes concernées. Ce sont donc les règles usuelles de la procédure civile qui s'appliquent en la matière.

Le Conseil fédéral a rendu un rapport sur l'exercice collectif des droits en Suisse en 2013[75]. Il y relève que le droit privé suisse connaît déjà certains instruments d'exercice collectif des droits, tels le cumul subjectif et objectif d'actions (art. 71 et 90 CPC), la jonction de cause, la suspension de la procédure et le renvoi (art. 125, let. c, 126 et 127 CPC) ou encore l'action des organisations (art. 89 CPC). Il considère que ces instruments ne sont pas toujours adéquats s'agissant de la réparation des dommages collectifs dispersés et propose plusieurs mesures pour améliorer la situation. Parmi celles-ci figurent l'extension du champ d'application de l'action des organisations à tous les domaines juridiques, voire aux actions en réparation, ou l'instauration de véritables instruments de mise en œuvre collective des droits. Dans cette seconde hypothèse, le Conseil fédéral parle soit de créer les bases légales pour des actions modèles (ou test)[76], soit d'introduire une action de groupe[77]. Deux

---

d'assurance sociale; b. des discriminations à raison du sexe; c. des litiges résultant de rapports de travail, pour autant que la valeur litigieuse ne dépasse pas 30 000 francs; d. des litiges concernant les art. 7 et 8 de la loi du 13 décembre 2002 sur l'égalité pour les handicapés. » (al. 4) « Si des motifs particuliers le justifient, le Tribunal fédéral peut majorer ces montants jusqu'au double dans les cas visés à l'al. 3 et jusqu'à 10 000 francs dans les cas visés à l'al. 4. » (al. 5).

[75] Rapport du Conseil fédéral du 3 juillet 2013 « Exercice collectif des droits en Suisse : état des lieux et perspectives ».

[76] L'action modèle ou action test permet de sauvegarder des intérêts collectifs en réalisant tout d'abord une seule « procédure modèle » typique entre deux parties sur une question litigieuse précise. La décision rendue entre ces deux parties aura alors valeur d'exemple procédural, concernant certaines questions de fait ou de droit, pour des litiges ultérieurs entre d'autres parties, de sorte que ces procédures ne devront plus répondre à la même question litigieuse. Il s'agit toujours d'une action individuelle du demandeur modèle, dont l'objectif est que le règlement des questions de fait ou de droit dans la procédure modèle ait un effet externe pour quantité de cas. La condition préalable de cet effet externe de la force de chose jugée est l'existence soit d'une base légale correspondante,

modèles seraient alors envisageables :

- l'introduction d'une action de groupe avec un système d'opt-in (le droit suisse connaît déjà des instruments juridiques qui se rapprochent très fortement de l'action de groupe)[78];
- l'introduction d'une procédure spéciale de transaction de groupe, inspirée des règles néerlandaises (extension par le juge de la force obligatoire d'une transaction à tous les lésés).

À noter qu'il n'a jamais été question d'instaurer une « class action » à l'américaine en raison notamment des risques d'abus qu'elle implique, engendrés partiellement par les conditions-cadres matérielles et procédurales en vigueur aux États-Unis[79].

Suite au rapport précité, la conseillère nationale Birrer-Heimo a déposé une motion[80] demandant au Conseil fédéral de modifier la loi afin qu'un grand nombre de personnes lésées de manière identique ou similaire puissent faire valoir collectivement leurs prétentions devant le juge. Le Conseil fédéral a répondu qu'il estimait inopportun d'élaborer une loi sur l'exercice collectif des droits (loi sur les actions collectives), mais s'est déclaré prêt à proposer des modifications ponctuelles allant dans le sens de son rapport sur l'exercice collectif des droits ou à prendre les aspects qui y sont exposés en compte dans les travaux législatifs en cours, par exemple dans la révision du droit de la société anonyme et dans la loi sur les services financiers en cours d'élaboration. La motion a été adoptée le 12 juin 2014.

La question se pose de savoir s'il faut introduire dans la LPD des instruments d'exercice collectif des droits, comme cela est d'ailleurs demandé par la motion Schwaab 13.3052 « Droit d'action collective en cas de viol de la protection des données, en particulier sur Internet »[81].

---

ou, en l'absence de base légale (comme en Suisse), d'une convention correspondante entre les parties (Rapport du Conseil fédéral du 3 juillet 2013, pp. 28 s.).

[77] Les actions de groupe sont des actions représentatives, où les prétentions individuelles sont regroupées de par le fait qu'un demandeur du groupe agit en faveur d'autres personnes. Ces dernières ne sont pas formellement parties à la procédure, mais participent tout de même au résultat, car la force de chose jugée s'étend également à leurs prétentions. La forme la plus connue d'action de groupe est l'action collective sur le modèle américain (« class action »). Selon la manière dont les tiers participent au résultat de la procédure aux côtés du demandeur de groupe, on distingue les actions de groupe avec option d'adhésion (opt-in) et les actions de groupe avec option de retrait (opt-out). Les deux modèles prévoient une procédure d'information des membres du groupe, celle-ci ayant toutefois une portée très différente dans les deux modèles. Outre les personnes individuelles touchées, des associations (à but idéal) ou des autorités sont également susceptibles de tenir le rôle de demandeurs de groupe. Les demandeurs de groupe sont en principe soumis à des exigences particulières, car ils agissent, au-delà de leurs propres intérêts, en tant que représentants du groupe et que leurs actes ont des effets pour tous les membres du groupe (Rapport du Conseil fédéral du 3 juillet 2013, pp. 32 s.).

[78] Action en examen des parts sociales et du sociétariat selon l'art. 105 de la loi sur la fusion (LFus; RS 221.301); représentant de la communauté des investisseurs selon l'art. 86 de la loi sur les placements collectifs (LPCC, RS 951.31); ou encore, dispositions spéciales pour le traitement des prétentions en responsabilité pour des dommages d'origine nucléaire (cf. art. 20 ss de loi fédérale du 13 juin 2008 sur la responsabilité civile en matière nucléaire [nLRCN; FF 2008 4843, 4845; pas encore entrée en vigueur]), voir Rapport du Conseil fédéral du 3 juillet 2013, pp. 33 ss.

[79] Sur ces questions, voir Rapport du Conseil fédéral du 3 juillet 2013, pp. 32 s.

[80] Motion Birrer-Heimo du 27 septembre 2013 13.3931 « Exercice collectif des droits. Promotion et développement des instruments ».

[81] La motion Schwaab 13.3052 du 7 mars 2013 n'a pas encore été traitée au Conseil national.

Une majorité du groupe d'accompagnement estime qu'il convient de renoncer à l'introduction de mesures particulières dans la LPD, pour deux raisons principalement. Premièrement, l'art. 89 CPC permet déjà à certaines organisations d'intenter des actions défensives en cas d'atteinte à la personnalité de membres de groupes déterminés et de solliciter du juge l'interdiction et la cessation de l'atteinte, la constatation de son caractère illicite, la publication de la rectification ou du jugement ainsi qu'un droit de réponse. Deuxièmement, en droit de la protection des données, les cas de dommages de masse ou dispersés sont plutôt rares, qu'ils soient financiers ou résultent d'un tort moral, et il paraît peu opportun d'introduire dans la LPD des mesures particulières en ce sens. Le renforcement des compétences et des pouvoirs de l'autorité de contrôle paraît plus à même d'assurer la mise en œuvre de la loi (cf. ch. 4.10.2).

Une minorité du groupe d'accompagnement est en revanche d'avis que les instruments d'exercice collectif des droits devraient être renforcés. Elle propose d'examiner la possibilité d'étendre l'art. 89 CPC aux cas dans lesquels seul un, ou peu des membres d'un groupe subissent une atteinte à la personnalité (en particulier lorsque le litige est susceptible de se reproduire et/ou est susceptible de concerner un grand nombre de personnes). Les individus pourraient ainsi être soulagés des risques du procès et confier la chose à une organisation disposant des moyens techniques et juridiques nécessaires. Il est aussi souhaité que l'art. 89 CPC soit étendu aux actions en réparation. Cumulativement à ces extensions, cette partie du groupe d'accompagnement souhaite que l'on introduise une action de groupe, avec un système d'opt-in, ou une procédure spéciale de transaction de groupe inspirée du modèle néerlandais, tant pour les actions défensives que pour les actions en réparation.

c) Mécanismes alternatifs de règlement des litiges

Outre les mesures décrites ci-dessus, le groupe d'accompagnement a également étudié l'opportunité d'introduire des mécanismes alternatifs de règlement des litiges en matière de protection des données (en particulier médiation, ombudsman)[82]. De telles procédures pourraient contribuer à régler des conflits le plus tôt possible et à l'amiable et permettraient ainsi aux parties d'épargner des frais et d'autres investissements. Les personnes désireuses de trouver une solution pragmatique à leur différend pourraient préserver leurs droits sans devoir entamer de procédure formelle. Une procédure de médiation permettrait également de prendre en compte les besoins particuliers des mineurs et de décharger considérablement les autorités (autorité de contrôle, tribunaux civils et juridictions administratives).

Au moment de l'entrée en vigueur de la LPD, l'intention du législateur était de conférer au PFPDT le rôle d'ombudsman ou de médiateur en cas de différends entre des privés et des organes fédéraux traitant des données [83]. Vu les compétences de rendre des décisions et de prononcer des sanctions dont sera éventuellement investie l'autorité de contrôle (cf. plus bas, ch. 4.10.2), certains membres du groupe d'accompagnement ont émis des réserves, estimant que le cumul d'une activité de médiation et d'un pouvoir décisionnel auprès d'une même autorité pourrait entraîner des conflits. Il est toutefois pensable que l'autorité de contrôle intervienne autant que possible dans le sens d'une médiation dans le cadre de ses tâches, sans qu'il s'agisse d'une médiation classique.

---

[82] Voir aussi l'art. 10 du projet de modernisation de la Convention STE 108 : « Chaque Partie s'engage à établir des sanctions et recours juridictionnels et non-juridictionnels appropriés visant les violations du droit interne donnant effet aux dispositions de la présente Convention. »

[83] Cf. le message du 23 mars 1988 concernant la loi fédérale sur la protection des données (LPD), FF 1988 II 421, 487.

Le groupe d'accompagnement propose ce qui suit pour ce qui est de la mise en place d'une procédure alternative de résolution des litiges: les différentes branches économiques doivent avoir la possibilité de créer ou de désigner, dans le cadre de l'autoréglementation (cf. ch. 4.1.2, let. b), un service chargé des procédures de conciliation ou de médiation relatives à des litiges en matière de protection des données. Si ces tâches étaient confiées à des bureaux d'ombudsman déjà existants, ceux-ci devraient former leur personnel dans le domaine de la protection des données. En l'absence d'une solution de branche, l'autorité de contrôle pourrait désigner un service de médiation ou un bureau d'ombudsman, à l'instar de ce que prévoit la législation sur la radio et la télévision.[84] La procédure de conciliation serait facultative.

Le groupe d'accompagnement a par ailleurs examiné la possibilité de désigner comme ombudsman les autorités de contrôle cantonales, mais l'a rejetée. Plusieurs membres du groupe sont d'avis qu'une telle attribution aboutirait à un mélange des compétences fédérales et cantonales. Ils doutent d'ailleurs que les cantons approuvent une modification de l'actuelle répartition des compétences. Qui plus est, les cantons rencontrent également des problèmes de ressources dans le domaine de la surveillance de la protection des données.

4.9 Dispositions particulières relatives au traitement de données personnelles par des organes fédéraux

4.9.1 Conception de la réglementation

Le droit sur la protection des données applicable au traitement de données personnelles par des organes de la Confédération se compose, outre de la législation générale en la matière (LPD et OLPD), de nombreuses dispositions prévues dans des lois spéciales. Le groupe d'accompagnement a examiné la question de savoir s'il ne faudrait pas rassembler dans un seul acte normatif l'ensemble des dispositions contenues dans ces lois spéciales, afin de disposer d'une seule loi régissant les traitements des données dans les différents domaines étatiques fédéraux. Il a conclu qu'une telle mesure n'était pas nécessaire du point de vue légistique et a par conséquent décidé de maintenir le système actuel. Des dispositions sur la protection des données spécifiques aux différents domaines permettent d'ailleurs de mieux tenir compte des objectifs poursuivis par les lois spéciales (cf. plus haut, ch. 4.1.1).

Le groupe d'accompagnement n'a pas non plus identifié de besoin d'agir s'agissant du champ d'application matériel des dispositions de droit public sur la protection des données, ou desexceptions régissant les activités de droit privé exercées par des organes fédéraux (art. 23 LPD).

4.9.2 Licéité du traitement de données (en particulier bases légales suffisantes)

Il est prévu de conserver les exigences posées à l'art. 17 LPD concernant les bases légales d'un traitement de données ainsi que le principe de l'autorisation spéciale, qui veut que la base légale exigée ne soit pas déjà donnée par la LPD, mais figure dans une réglementation spécifique dans le domaine concerné. Le groupe d'accompagnement estime toutefois que la conception de l'art. 17, al. 2, LPD, qui règle les cas dans lesquels une base légale n'est pas exigée (Surrogat für Rechtsgrundlage), manque de clarté. Il propose dès lors de revoir cette disposition, en particulier de préciser que l'exception mentionnée à l'art. 17, al. 2, let. c, LPD se rapporte non seulement au traitement de données personnelles sensibles, mais égale-

[84] Voir les art. 18 ss du règlement de l'autorité indépendante d'examen des plaintes en matière de radio télévision (RS 784.409).

ment à celui de données personnelles « ordinaires » selon l'art. 17, al. 1, LPD.

Il n'apparaît pas nécessaire au groupe d'accompagnement de fixer d'autres exigences dans la LPD concernant la formulation de bases légales relatives au traitement de données dans des domaines spécifiques. Il renvoie à cet égard à l'accompagnement législatif fait par l'Office fédéral de la justice, dans le cadre duquel l'existence et la suffisance des bases légales spéciales sont examinées et au fait que l'autorité de contrôle est invitée à se prononcer sur les projets d'actes législatifs (cf. art. 31, al. 1, let. b, LPD). Ces différents instruments garantissent que les exigences générales en matière de protection des données sont également respectées dans les réglementations sectorielles.

Une *partie du groupe d'accompagnement* propose toutefois d'examiner s'il ne serait pas judicieux de fixer dans la LPD les exigences essentielles concernant les bases légales pour les systèmes d'information. Selon la pratique actuelle[85] en effet, de très nombreux détails doivent être arrêtés au niveau de la loi formelle.

La disposition relative au traitement de données automatisé dans le cadre d'essais pilotes n'a joué qu'un rôle mineur dans la pratique (art. 17a LPD). Le groupe d'accompagnement estime par conséquent judicieux de faciliter cette procédure. Il propose d'attribuer la compétence d'évaluer l'autorisation (par décision) à l'autorité de contrôle, en lieu et place du Conseil fédéral. Cette disposition devrait par ailleurs être raccourcie et les détails réglés au niveau ordonnance. L'art. 17a LPD porte sur une exception à l'exigence d'une base légale pour traiter des données personnelles sensibles. Pour des raisons de systématique, cette exception ne devrait pas être réglée séparément, mais devrait figurer à l'art. 17, al. 2, LPD.

4.9.3 Dispositions particulières pour certaines formes de traitement de données

La LPD contient des prescriptions particulières à l'intention des organes fédéraux pour différentes formes de traitement (p. ex. collecte, communication, anonymisation ou destruction). Ces dispositions ont dans l'ensemble fait leurs preuves.

Dispositions particulières relatives à la communication de données personnelles : le rapport entre l'art. 19 LPD (communication de données personnelles) et l'art. 17 LPD (bases juridiques), spécialement en ce qui concerne les exceptions à l'exigence de la base légale pour communiquer des données personnelles sensibles, doit être clarifié. Selon le groupe d'accompagnement l'art. 19 LPD doit se rapporter à toutes les données personnelles, y compris au données sensibles. Il propose également d'étendre le catalogue des exceptions de l'art. 19 LPD, en ce sens que la communication de données personnelles par des organes fédéraux est autorisée même en l'absence de base légale, lorsque cela est nécessaire pour protéger des intérêts prépondérants ou vitaux (p. ex. la vie ou l'intégrité physique) de la personne concernée ou de tiers. Enfin, le groupe d'accompagnement est d'avis que l'art. 19, al. 3, LPD qui concerne la mise à disposition en ligne des données (procédure d'appel) peut être abrogé. Avec l'évolution de la technique, l'accès en ligne est devenu courant ; il n'est donc plus aussi imprévisible pour les personnes concernées qu'il ne l'était au moment de l'introduction de cette disposition. Le groupe d'accompagnement estime que l'exigence de la base légale énoncée à l'art. 19, al. 1, LPD est suffisante à cet égard.

Dispositions particulières relatives au devoir d'informer lors de la collecte de données *:* voir le ch. 4.3.1. Il faut relever à ce propos que la teneur de l'art. 18 LPD est d'ores et déjà couverte par celle de l'art. 18a LPD. L'art. 18 LPD peut donc être abrogé.

---

[85] Voir à ce propos le Guide de l'OFJ du 16 décembre 2010 pour l'élaboration des bases légales nécessaires pour exploiter un système de traitement automatisé de données personnelles.

4.9.4 Mesures organisationnelles

Il convient de renforcer et d'encourager la responsabilisation des organes fédéraux en ce qui concerne le respect des dispositions sur la protection des données. À cet effet, il faudrait que les conseillers à selon l'art. 23 OLPD que doivent désigner la Chancellerie fédérale et chaque département, aient les mêmes tâches et la même position que les « conseillers» selon les art. 12a et 12b OLPD (voir plus haut, ch. 4.3.2)[86]. Cela signifie en particulier que les premiers cités doivent pouvoir exercer leur activité de façon indépendante sur le plan organisationnel et professionnel, et disposer des ressources nécessaires à cet effet. Un renforcement de la position des conseillers internes de l'administration pourrait par ailleurs contribuer à décharger l'autorité de contrôle.

4.9.5 Prétentions et procédures

a) Prétentions

Comme cela a été expliqué aux ch. 4.4.1 et 4.4.2, les différentes prétentions en matière de protection des données doivent être réunies dans un catalogue commun pour les secteurs public et privé. Cette simplification doit améliorer la lisibilité de la LPD et donner aux personnes concernées une meilleure vue d'ensemble de leurs droits à l'encontre des auteurs de traitements de données. En revanche, il ne faut rien changer matériellement à l'actuel système d'excercie des droits (p. ex. s'agissant de la légitimation active et passive ou des voies de recours). S'agissant du traitement de données par des organes fédéraux, il convient toutefois d'examiner de plus près s'il ne faudrait pas, par analogie à la solution retenue en droit privé, introduire un droit d'opposition pour tous les traitements. Actuellement, les personnes concernées peuvent uniquement exiger de l'organe fédéral responsable qu'il ne communique pas des données personnelles déterminées à des tiers (art. 20 LPD).

Les actions en dommages-intérêts ou en réparation pour tort moral doivent continuer à obéir aux conditions générales du droit de responsabilité de l'Etat. Les conséquences financières de traitements de données illicites continueront donc à être appréciées sous l'angle des art. 3 ss de la loi sur la responsabilité (LRCF ; RS 170.32).

b) Répartition du fardeau de la preuve

Les personnes concernées doivent bénéficier d'un allégement du fardeau de la preuve lorsqu'elles font valoir leurs droits à l'encontre d'organes fédéraux, comme le propose le groupe d'accompagnement pour les traitements de données par des privés (cf. ch. 4.8.2). Il s'agit en l'occurrence d'un renversement du fardeau de la preuve, sur le modèle de l'art. 13a, al. 1, LCD[87], à savoir qu'il peut être exigé de l'organe fédéral, de prouver qu'il se conforme au droit de la protection des données si, compte tenu des intérêts légitimes des parties à la procédure, une telle exigence paraît appropriée (concernant la présomption légale de la régularité d'un traitement de données lorsque les règles de bonnes pratiques sont respectées, voir plus haut, ch. 4.1.2, let. b). Tel pourrait être le cas lorsque l'administration des preuves est particulièrement difficile pour la personne concernée, par exemple quant les faits sont dans la sphère d'influence de l'auteur du traitement (p. ex. en rapport avec le respect du devoir de

---

[86] Concernant les tâches et la position des conseillers à la protection des données (Datenschutzverantwortliche), voir les explications sur le site du PFPDT, http://www.edoeb.admin.ch/datenschutz/00626/00743/00874/01051/index.html?lang=fr.

[87] Art. 13a, al. 1, LCD: « Le juge peut exiger que l'annonceur apporte des preuves concernant l'exactitude matérielle des données de fait contenues dans la publicité si, compte tenu des intérêts légitimes de l'annonceur et de toute autre partie à la procédure, une telle exigence paraît appropriée en l'espèce. »

diligence selon le ch. 4.3.2).

c) Dispositions de procédure

L'évaluation de la loi sur la protection des données a montré que les personnes concernées vont plus souvent en procédure contre des organes fédéraux que contre des privés. Dans l'absolu, les prétentions sont toutefois rarement exercées dans le secteur public également[88]. Il n'y a selon le groupe d'accompagnement que peu d'options pour améliorer la protection juridique individuelle dans la procédure de droit public (comme dans la procédure civile d'ailleurs). En clair, la mise en œuvre des dispositions de droit public sur la protection des données doit prioritairement passer par une extension des compétences de l'autorité de contrôle (cf. ch. 4.10.2).

Comme pour la procédure civile, le groupe d'accompagnement propose de prévoir pour les autorités administratives de première instance ou de recours la possibilité de demander une prise de position à l'autorité de contrôle (cf. ch. 4.8.3, let. b): si une procédure porte sur l'admissibilité d'un traitement de données, l'autorité administrative compétente ou l'instance de recours peut, d'office ou à la demande d'une partie, soumettre l'affaire à l'autorité de contrôle pour prise de position. Celle-ci n'est pas tenue de se prononcer. Si elle le fait, son avis n'est pas contraignant.

d) Modes alternatifs de règlement des litiges

Il est prévu de proposer, comme pour le secteur privé, un mode alternatif pour le règlement des litiges ayant trait au traitement de données par des organes fédéraux. La procédure seraitêtre confiée à un service de médiation ou d'ombudsman à désigner par l'autorité de contrôle (cf. ch. 4.8.3, let. c).

4.9.6 Relation entre les dispositions de la LPD et de la LTrans

La loi fédérale sur le principe de la transparence dans l'administration (LTrans ; RS 152.3) présente plusieurs points de recoupement avec la LPD. Or, la LTrans fait actuellement l'objet d'une évaluation concernant sa mise en œuvre et son efficacité. Il apparaît par conséquent au groupe d'accompagnement peu opportun de formuler en ce moment des propositions tombant dans le champ d'application de cette loi[89].

4.10 Autorités de contrôle

4.10.1 Introduction

On l'a vu, l'évaluation de la LPD a mis pour *une majorité du groupe d'accompagnement* en évidence des lacunes dans la mise en œuvre (« Durchsetzung ») de la loi. Ces carences peuvent certes être atténuées par un renforcement des droits procéduraux des parties et un accès à la justice facilité. Le groupe d'accompagnement estime cependant qu'on ne peut réellement améliorer l'efficacité de la loi sans renforcer de manière significative les pouvoirs de l'autorité de contrôle, en lui conférant un pouvoir de décision (voir les réflexions menées au ch. 4.1.2, let. a). Le projet de modernisation de la Convention STE 108 prévoit aussi une

---

[88] Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz du 10 mars 2011, pp. 86 ss, 133 ss, 208; disponible en ligne (en allemand) <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

[89] Cf. l'évaluation de la LTrans <http://www.admin.ch/aktuell/00089/index.html?lang=fr&msg-id=52653>. L'OFJ soumettra au Conseil fédéral son rapport concernant les résultats de cette évaluation d'ici à la fin de 2014. Peut-être faudra-t-il intégrer ces conclusions dans la suite des travaux de révision de la LPD.

telle compétence. Dans cette entreprise, une attention toute particulière devrait être portée au maintien, voire à l'amélioration de l'indépendance de l'autorité de contrôle, qui est un thème toujours actuel, en Suisse[90], mais aussi au plan européen[91].

Compte tenu des compétences et pouvoirs plus étendus que le groupe d'accompagnement propose de conférer au PFPDT, la question de savoir s'il ne serait pas adéquat de modifier son organisation pour en faire une autorité collégiale se pose. Des propositions en ce sens sont faites au ch. 4.10.3 ci-dessous.

À noter *qu'une minorité du groupe d'accompagnement* s'oppose à ce que les pouvoirs de l'autorité de contrôle – en particuliers de décision et de sanction – soient renforcés. Des éventuelles modifications législatives ne devraient par ailleurs intervenir à ses yeux que dans la mesure de ce qui est nécessaire, en regard du droit UE et du projet de modernisation de la Convention STE 108, pour l'accès au marché (cf. ch. 3).

4.10.2 Tâches et pouvoirs de l'autorité de contrôle

a) Dans le secteur privé

aa) Surveillance des personnes privées

Réalisation d'une enquête préalable *:* le groupe d'accompagnement propose d'introduire une procédure d'enquête préalable sur le modèle de l'art. 26 LCart[92]. Cette procédure serait très informelle et le plus simple possible afin de faciliter la recherche de solutions à l'amiable. Il ne s'agirait pas d'une étape obligatoire et l'autorité pourrait, dans certains cas, ouvrir directement une procédure formelle.

La procédure préalable aurait comme fonction d'assurer le tri des affaires nécessitant l'ouverture d'une enquête proprement dite, et permettrait aux particuliers, notamment aux personnes dont les données font l'objet d'un traitement, de s'adresser facilement à l'autorité de contrôle pour lui demander des conseils. Elle serait menée par le secrétariat permanent de l'autorité de contrôle (cf. ch. 4.10.3). Cette dernière pourrait ouvrir une enquête préalable d'office, à la demande des personnes concernées par un traitement de données, ou sur dénonciation de tiers. Elle n'aurait pas l'obligation de le faire, et il n'existerait pas de voie de recours contre un refus d'entrer en matière. La procédure serait gratuite.

Au terme de l'enquête préalable, l'autorité de contrôle aurait plusieurs options. En l'absence d'indices sur la présence d'une situation justifiant l'ouverture d'une enquête formelle (art. 29 LPD), elle en informerait simplement par écrit les intervenants. En présence d'indices sur la présence d'une situation justifiant l'ouverture d'une enquête, elle pourrait :

– Proposer des mesures pour supprimer ou empêcher une violation de la LPD. L'approbation de la proposition par l'auteur du traitement ne constituerait pas un accord à l'amiable dont la violation pourrait être sanctionnée. Il s'agirait de simples engagements unilatéraux, qui ne seraient soumis à aucune forme. En cas de respect des engagements pris, l'autorité de contrôle n'ouvrirait pas d'enquête.

---

[90] Rapport du Conseil fédéral sur l'évaluation de la loi sur la protection des données du 9 décembre 2011, FF 2012 255 ss, 269.

[91] Arrêts de la CJUE C-614/10 du 16 octobre 2012 et C-288/12 du 8 avril 2014.

[92] Art. 26 LCart : « Le secrétariat peut mener des enquêtes préalables d'office, à la demande des entreprises concernées ou sur dénonciation de tiers. » (al. 1). « Il peut proposer des mesures pour supprimer ou empêcher des restrictions à la concurrence. » (al. 2). « La procédure d'enquête préalable n'implique pas le droit de consulter les dossiers. » (al. 3).

– Ouvrir une enquête formelle.

L'information et les propositions de l'autorité de contrôle, de même que l'ouverture de l'enquête, ne seraient pas sujettes à recours.

Ouverture d'une enquête formelle : le groupe d'accompagnement propose de ne plus limiter le champ du pouvoir d'enquête de l'autorité de contrôle aux cas prévus à l'actuel art. 29 LPD. En raison de ses ressources limitées, l'autorité de contrôle devra toutefois dans les faits se concentrer sur les cas qui présentent un intérêt public et définir ses priorités.

Instruction lors de la procédure d'enquête formelle : afin que l'autorité de contrôle puisse établir les faits le plus rapidement et le plus exactement possible, le groupe d'accompagnement propose de renforcer ses pouvoirs d'instruction. Outre la possibilité de demander aux responsables de traitements qu'ils lui fournissent tous les renseignements et documents nécessaires et lui présentent les traitements (art. 29 al. 2 LPD), elle pourrait à certaines conditions également demander à pouvoir accéder aux locaux et aux programmes informatiques, effectuer des saisies ou faire poser des scellés. La procédure serait régie par la loi fédérale sur la procédure administrative (PA ; RS 172.021), voire, par analogie et selon les mesures envisagées, par la loi fédérale sur le droit pénal administratif (LPA ; RS 313.0; art. 45 ss).

Pouvoirs de décision et de sanction [93]: l'autorité de contrôle aurait un pouvoir de décision, c'est-à-dire qu'elle pourrait imposer des mesures, telles la suspension ou la cessation d'un traitement de données. Elle aurait également le pouvoir de prononcer, à certaines conditions, des sanctions pécuniaires. Concrètement, si l'autorité de contrôle, au terme de son enquête formelle, constate que le traitement n'est pas conforme à la loi, elle impartirait un délai au responsable pour régulariser la situation. Elle pourrait parallèlement proposer un accord à l'amiable, de manière analogue à ce que prévoit l'art. 29 LCart[94] par exemple. Si la situation n'est pas régularisée au terme du délai fixé, ou en exécution de l'accord à l'amiable, l'autorité de contrôle pourrait rendre une décision interdisant ou suspendant le traitement et/ou enjoignant au responsable du traitement de prendre des mesures. En cas de non-respect d'une décision entrée en force ou de non-respect d'un accord à l'amiable, l'autorité de contrôle pourra prononcer une sanction pécuniaire. Dans certains cas de violation crasse de la loi, l'autorité pourrait directement (c'est-à-dire sans passer par l'accord à l'amiable ou la fixation d'un délai) prononcer une sanction pécuniaire, et ce cumulativement à une mesure (interdiction, suspension, autres mesures). Au surplus, le refus de collaborer pourrait aussi être sanctionné. Dans tous les cas, l'autorité de contrôle pourrait prendre les mesures provisionnelles nécessaires.

➢ Variante : une partie du groupe de travail propose que l'autorité de contrôle ne sanctionne pas elle-même le non-respect de ses décisions entrées en force, mais qu'elle mentionne dans les dispositifs de ces dernières l'art. 292 du code pénal suisse (CP ; RS 311.0). La poursuite incomberait alors aux cantons.

Le groupe d'accompagnement s'est demandé s'il fallait conférer à la personne qui a signalé le cas à l'autorité de contrôle la qualité de partie à la procédure et ou la qualité pour recourir.

---

[93] La Commission des institutions politiques du Conseil national (CIP-CN) a décidé, le 29 août 2014, de ne pas donner suite à l'initiative parlementaire Schwaab 14.404 du 19 mars 2014 « Pour des sanctions réellement dissuasives en cas de violation de la protection des données ».

[94] Art. 29 LCart: « Si le secrétariat considère qu'une restriction à la concurrence est illicite, il peut proposer aux entreprises concernées un accord amiable portant sur les modalités de la suppression de la restriction. »(al. 1). « L'accord requiert la forme écrite et doit être approuvé par la commission. » (al. 2).

Il propose d'y renoncer, dans la mesure où l'autorité de contrôle doit à l'avenir rester une garante de l'intérêt public, et non trancher des litiges individuels.

Pour faciliter la mise en œuvre de la loi en présence d'auteurs de traitements qui n'ont pas de siège (domicile) en Suisse, il est prévu de les obliger à fournir, dans le cadre des investigations menées par l'autorité de contrôle, une adresse de correspondance en Suisse à laquelle des décisions pourraient leur être valablement notifiées.[95] Le non-respect de cette obligation serait sanctionné.

ab) Conseil aux privés

L'activité de conseil aux personnes privées, telle que prévue par l'actuel art. 28 LPD, est maintenue.

Pour ce qui est du conseil aux responsables de traitement, le groupe d'accompagnement propose d'introduire une sorte de procédure d'examen préalable semblable à ce qui existe en droit des cartels afin d'éviter notamment que la double activité de conseil et de contrôle de l'autorité de contrôle ne les dissuade de s'adresser à elle. À la différence de la notification prévue dans la LCart, l'annonce serait facultative. Il s'agirait de permettre au responsable du traitement de connaître les éventuelles objections de l'autorité de contrôle avant la mise en œuvre d'un nouveau traitement et d'éviter par la suite des sanctions pécuniaires. Pratiquement, la personne pourrait soumettre les traitements de données envisagés à l'autorité, qui aurait alors un certain délai (p. ex. un mois) pour décider s'il y a lieu de procéder à un examen du traitement (sur le modèle de l'art. 32 LCart[96]). Faute de communication de la part de l'autorité de contrôle dans ce délai, le traitement pourrait être effectué sans encourir le risque d'une sanction de l'autorité, pour autant que le traitement effectué soit celui annoncé. Il y aurait lieu de prévoir, de manière analogue à l'art. 38 LCart[97], des conditions qui permettraient, malgré l'écoulement du délai, de procéder à un examen (p. ex. le responsable du traitement a fourni des données inexactes, il existe un risque d'atteinte grave qui ne pouvait être détecté sur la base des informations fournies, etc.). S'il existe des règles de bonnes pratiques en la matière (cf. ch. 4.1.2 let. b), et que l'auteur du traitement s'y conforme, il n'encourrait aucune sanction pécuniaire. S'il soumet son cas à l'autorité malgré l'existence de règles de bonnes pratiques, cette dernière pourrait se contenter d'y renvoyer sans examen au fond. En l'absence de règles de bonnes pratiques, l'autorité pourrait suggérer au comité

---

[95] On trouve par exemple une prescription de ce type à l'art. 5 de l'ordonnance sur les services de télécommunication (OST, RS 784.101.1): « Les fournisseurs de services de télécommunication obligés de s'annoncer dont le siège se trouve à l'étranger doivent indiquer une adresse de correspondance en Suisse à laquelle des communications, des citations et des décisions peuvent notamment leur être valablement notifiées. »

[96] Art. 32 LCart: « A la réception de la notification d'une concentration d'entreprises (…), la commission décide s'il y a lieu de procéder à un examen de l'opération de concentration. La commission communique, dans le délai d'un mois à compter de la notification de l'opération de concentration, l'ouverture de l'examen de la concentration aux entreprises participantes. Faute de communication dans ce délai, la concentration peut être réalisée sans réserve. » (al. 1). « Les entreprises participantes s'abstiennent de réaliser la concentration pendant le délai d'un mois suivant sa notification, à moins que, à leur requête, la commission ne les ait autorisées à le faire pour des motifs importants. » (al. 2).

[97] Art. 38 LCart: 1 « La commission peut rapporter une autorisation ou décider l'examen d'une concentration malgré l'écoulement du délai de l'art. 32, al. 1, lorsque: a. les entreprises participantes ont fourni des indications inexactes; b. l'autorisation a été obtenue frauduleusement; c. les entreprises participantes contreviennent gravement à une charge dont a été assortie l'autorisation. » (al. 1). « Le Conseil fédéral peut rapporter une autorisation exceptionnelle pour les mêmes motifs. » (al. 2).

compétent d'édicter de telles règles pour le cas en question.

b) Dans le secteur public

ba) Surveillance des organes fédéraux

Le groupe d'accompagnement propose de renforcer la surveillance des organes fédéraux également, dans la mesure du possible de manière analogue à ce que qui est prévu pour le secteur privé (cf. ch. 4.1.1).

Réalisation d'une enquête préalable : le groupe d'accompagnement propose d'introduire une enquête préalable comme dans le secteur privé (cf. 4.10.2, let. a/aa).

Ouverture d'une enquête formelle : lorsque l'enquête préalable aura démontré des indices de violation des prescriptions sur la protection des données, ou en cas de violation claire, l'autorité pourrait ouvrir une enquête formelle (cf. ch. 4.10.2, let. a/aa).

Instruction lors de la procédure d'enquête : outre les pouvoir dont elle dispose déjà, le groupe d'accompagnement propose que l'autorité de contrôle soit autorisée à consulter par procédure d'appel les données traitées par les organes fédéraux. L'accès durerait le temps de la procédure.

Compétences de décision : le groupe d'accompagnement propose un modèle tel que le connaissent certains cantons (p. ex. Schauffhouse et Bâle-Ville). Il s'agirait de conférer à l'autorité de contrôle un pouvoir de décision, en plus de l'instrument de la recommandation prévu à l'actuel art. 27 LPD. L'idée est de renforcer les outils de contrôle et les compétences de l'autorité à l'encontre des organes fédéraux et d'améliorer la protection des données en prévision de la ratification de la Convention STE 108 modernisée et de la reprise du développement de l'acquis de Schengen/Dublin. Cette proposition permettrait par ailleurs d'harmoniser dans une certaine mesure les dispositions sur la protection des données dans les domaines public et privé. Concrètement, si l'autorité de contrôle constate une violation des prescriptions sur la protection des données, elle émet une recommandation à l'intention de l'organe fédéral responsable et en informe le département compétent ou la Chancellerie fédérale. Si la recommandation est rejetée ou n'est pas suivie, l'autorité peut transformer sa recommandation, en tout ou en partie, en une décision sujette à recours[98]. L'organe fédéral concerné peut attaquer cette décision selon les dispositions générales de l'organisation judiciaire fédérale. Il conviendrait en outre d'examiner l'opportunité d'investir l'autorité de contrôle de la compétence d'ordonner directement la restriction ou la cessation d'un traitement de données à titre de mesure provisoire[99]. Il faut encore déterminer dans quelle mesure ce modèle est susceptible d'entrer en collision avec la protection juridique conférée par l'art. 25 LPD. Qui plus est, il faut vérifier si une telle solution peut être intégrée dans le droit procédural public existant (PA, LTAF, LTF) et, le cas échéant, comment.

Une majorité du groupe d'accompagnement estime qu'il faut renoncer à ordonner des sanctions administratives (p. ex. des amendes) l'encontre des organe fédéraux, une pratique que

[98] Le canton de Bâle-Ville pose comme condition qu'il existe un intérêt prépondérant à mettre en œuvre la mesure recommandée. Pour plus de détails, voir le § 47, al. 1, 2 et 5, de la loi Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG BS; SG 153.260) ainsi que le § 26 s. de la loi Datenschutzgesetz des Kantons Schaffhausen (SHR 174.100).

[99] Cf. § 47, al. 4, IDG BS: « Si des intérêts dignes de protection sont visiblement menacés ou violés, le Préposé à la protection des données peut ordonner que l'organe public restreigne ou stoppe le traitement jusqu'à ce que la cour d'appel ait terminé son examen. » (traduction non officielle)

en vigueur dans plusieurs pays de l'UE (cf. ch. 4.1.2, let. a), du moins tant que l'acquis de Schengen/Dublin ne l'exige pas.

Les tiers qui auraient dénoncé le cas n'auraient ni la qualité de partie, ni la qualité pour recourir (cf. ch. 4.10.2, let. a/aa).

bb) Conseil aux organes fédéraux (art. 31, al. 2, LPD)

Cette activité de conseil doit être maintenue. Il s'agira d'adapter la rédaction de l'article dans le cas où l'exception de l'art. 2, al. 2, let. d, LPD devait être supprimée (voir ch. 4.10.2 let. d/db).

c) Elaboration de règles plus détaillées

La création de règles de bonnes pratiques ou de règles contraignantes, permettrait, on l'a vu (cf. ch. 4.1.2, let. b), de renforcer la sécurité du droit, dans la mesure où la LPD resterait très générale et technologiquement neutre.

La majorité du groupe d'accompagnement propose de confier l'élaboration de ces règles à un comité distinct de l'autorité de contrôle au sens étroit. Les règles de bonnes pratiques pourraient aussi être élaborées, d'office ou sur mandat des milieux concernés, qui les soumettraient à l'organe spécialisé, voire à l'autorité de contrôle pour approbation (cf. ch. 4.1.2, let. b).

d) Information et sensibilisation du public

La faculté pour l'organe de contrôle d'informer le public de ses constatations lorsqu'il en va de l'intérêt général est maintenue. Il s'agit d'un instrument de prévention important. Les éventuels secrets d'affaires ne doivent toutefois pas être mis en danger.

Le PFPDT sensibilise déjà actuellement la population, notamment par le biais d'informations sur son site internet. Le rapport d'évaluation a toutefois démontré que malgré cela, les personnes concernées ne prenaient pas toujours les précautions requises, soit parce qu'elles se sentent dépassées, soit encore parce qu'elles sous-estiment les possibilités d'exploitation de leurs données et les risques qui en découlent[100]. Le groupe d'accompagnement propose d'inscrire dans la loi, comme le fait le projet de modernisation de la Convention STE 108 (art. 12bis, al. 2, let. e) que l'autorité de contrôle est chargée de sensibiliser et d'éduquer la population à la protection des données. Cette sensibilisation pourra se faire par des règles de bonnes pratiques ou des règles contraignantes (cf. ch. 4.1.2, let. b), des campagnes d'information, voire encore des aides à la formation. Un effort particulier devra être fourni en rapport avec la question du consentement des personnes concernées (cf. ch. 4.3.3). Au surplus, il s'agira de porter une attention particulière aux mineurs et aux autres personnes vulnérables.

e) Prise de position dans une procédure civile ou administrative

Outre les tâches que l'autorité de contrôle exécute déjà, le groupe d'accompagnement propose, sur le modèle de l'art. 15 LCart[101], qu'en cas de procédure civile ou administrative, l'affaire puisse lui être transmise pour avis, à la demande d'une partie ou sur l'initiative du juge. Cela permettra d'éviter que des institutions non spécialisées aient à se prononcer seules, surtout en première instance, sur des cas parfois sensibles et techniques (cf.

---

[100] Cf. le rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi sur la protection des données, FF 2012 255ss, 261.

[101] Art. 15, al. 1, LCart: « Lorsque la licéité d'une restriction à la concurrence est mise en cause au cours d'une procédure civile, l'affaire est transmise pour avis à la Commission de la concurrence. »

ch. 4.8.3 let. b, et 4.9.5, let. c).

f) Procédure extrajudiciaire de résolution des litiges

Cf. ch. 4.8.3 let. c.

g) Fonction d'autorité de première instance

Une minorité du groupe d'accompagnement propose que l'autorité de contrôle ait une compétence générale de trancher les litiges en première instance en lieu et place du juge civil et des autorités administratives. Les actions en réparation demeureraient toutefois de la compétence de ces derniers. Cette solution aurait le mérite de faire trancher les litiges par une autorité spécialisée qui connaît bien le domaine. *Une majorité du groupe d'accompagnement* estime qu'il n'est pas judicieux de déroger au système ordinaire en instaurant une autorité spécialisée. Une telle solution constituerait une rupture dans notre ordre juridique et poserait un certain nombre de questions délicates qu'il conviendrait d'approfondir (mélange des rôles, problèmes de procédure, etc.). La possibilité évoquée plus haut de solliciter un avis de l'autorité de contrôle (cf. ch. 4.8.3, let. b, et 4.9.5, let. c) permettrait par ailleurs de suppléer d'une autre manière au manque de connaissances techniques des autorités ordinaires.

4.10.3 Organisation de l'autorité de contrôle

Le groupe d'accompagnement est divisé sur le modèle d'organisation à choisir pour l'autorité de contrôle. Certains estiment que, vu les nouveaux pouvoirs qu'il est prévu de lui conférer (cf. ch. 4.10.2), la forme de l'autorité collégiale serait plus indiquée. D'autres sont d'avis que le système actuel a fait ses preuves et qu'il n'y a pas de raison d'en changer. Dans les deux cas de figure, il se pose la question de savoir quelle serait l'autorité compétente pour adopter/avaliser les règles de bonnes pratiques ou les règles contraignantes à l'intention des auteurs de traitements (voir ch. 4.1.2, let. b). *La majorité du groupe d'accompagnement* estime qu'il convient de confier cette tâche à un comité spécialisé, alors *qu'une minorité* est d'avis que c'est à l'autorité de contrôle elle-même d'assumer ce travail.

Compte tenu des avis divergents au sein du groupe d'accompagnement, les quatre modèles d'organisation suivants sont proposés : a) mise en place d'une autorité collégiale avec comité ; b) mise en place d'une autorité collégiale sans comité; c) maintien d'une autorité personnalisée avec comité et d) maintien d'une autorité personnalisée sans comité.

a) Autorité collégiale avec comité

Selon *une partie du groupe d'accompagnement*, le modèle de l'autorité collégiale assure une meilleure acceptation politique des éventuelles décisions et sanctions rendues. Il garantit également une prise de décision plus représentative et plus équilibrée, et permet de véritablement consolider les décisions au sein d'un collège. Le modèle collégial renforcerait par ailleurs l'indépendance de l'autorité de contrôle, dans la mesure où les éventuelles influences extérieures seraient en quelque sorte diluées par leur répartition entre les membres.

Au plan fédéral, la coutume est d'ailleurs plutôt de confier les tâches de surveillance à des autorités collégiales, telles la Commission de la concurrence (ComCo), la Commission fédérale des maisons de jeu (CFMJ), la Commission fédérale de l'électricité (ElCom), l'Institut suisse des produits thérapeutiques (Swissmedic), l'Autorité fédérale de surveillance des marchés financiers (FINMA) ou encore l'Institut Fédéral de la Propriété Intellectuelle (IPI)[102]. Le seul autre exemple d'autorité fédérale unipersonnelle est le Surveillant des prix. Sa situa-

[102] Voir le rapport du Conseil fédéral du 13 septembre 2006 sur l'externalisation et la gestion des tâches de la Confédération (rapport sur le gouvernement d'entreprise), FF 2006 7799 ss, en particulier pp. 7851 s.

tion n'est toutefois pas comparable à celle du PFPDT dans la mesure où il n'est pas indépendant, mais relève du Département fédéral de l'économie, de la formation et de la recherche (DEFR). Au plan cantonal, Neuchâtel/Jura, le Tessin, Fribourg et le Valais connaissent – avec des arrangements parfois différents – le modèle de la commission. Au plan international, on connaît également dans plusieurs pays soit le modèle de la commission (par ex. la « Commission Nationale de l'Informatique et des Libertés » [CNIL] en France), soit le modèle du directoire (le « Garante per la protezione dei dati personali » en Italie [composé de quatre membres] ou l'autorité néerlandaise « College bescherming persoonsgegevens » [CBP ; composée de trois membres]).

Le groupe d'accompagnement a examiné trois formes d'autorités collégiales : l'établissement, la commission et le directoire. Il a décidé d'écarter les deux premières, trop lourdes administrativement et susceptibles de ralentir les procédures. La forme de l'établissement ne paraissait au surplus pas opportune vu la taille plutôt réduite de l'autorité de contrôle[103].

Il est donc proposé d'instituer un directoire. Ce modèle garantit des prises de décision rapides, une bonne circulation des informations au sein de l'autorité, et s'accorde bien avec la création d'un comité spécialisé pour les bonnes pratiques ou les règles contraignantes (cf. ch. 4.1.2, let. b, et ch. 4.10.2, let. c). Les avantages liés à l'institution d'une autorité collégiale sont par ailleurs en grande partie conservés (indépendance, acceptation politique des décisions et sanctions).

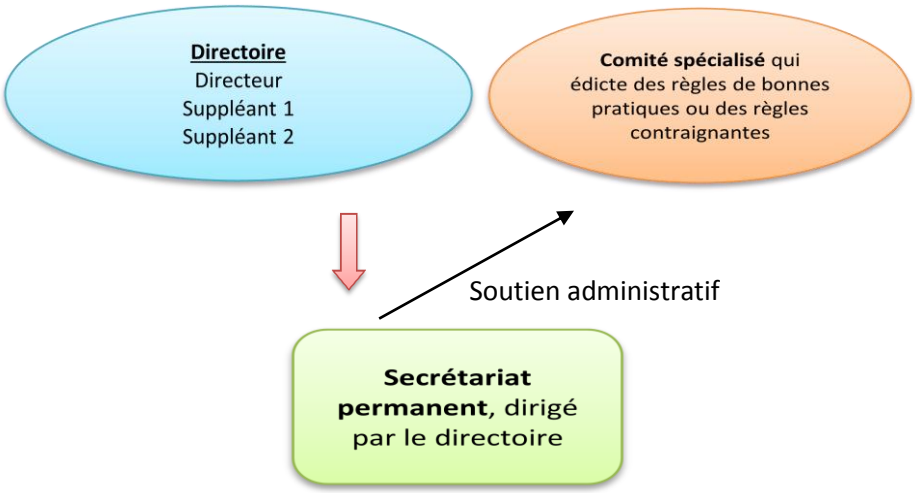
Le directoire serait composé d'un directeur et de deux suppléants, tous trois indépendants, et nommés par le Conseil fédéral, sous réserve de l'approbation de l'Assemblée fédérale. Le directoire dirigerait un secrétariat permanent qui lui assurerait un soutien administratif, préparerait ses décisions, conduirait les investigations et prendrait les décisions de procédure. Les décisions importantes devraient être prises par le collège.

L'autorité de contrôle aura peut-être à l'avenir des tâches et des compétences encore plus variées dans le domaine de la protection et dans celui de la transparence (surveillance avec pouvoir de décision [LPD] vs. médiation [art. 13 ss LTrans]). Pour éviter que ne montent au créneau ceux qui estiment qu'aujourd'hui déjà l'organisation du PFPDT conduit à des conflits d'intérêts et à un affaiblissement de la transparence, on pourrait envisager qu'un suppléant dirige l'unité consacrée à la protection des données et l'autre celle qui est dédiée à la transparence, sur le modèle de l'autorité de contrôle du canton de Fribourg (art. 29a de la loi du 25 novembre 1994 sur la protection des données; RSF 17.1)[104] . Les cas de conflits entre la protection des données et la transparence pourraient être tranchés par le directoire, qui pourrait dire ce qui prévaut dans le cas d'espèce.

---

[103] Voir le rapport du Conseil fédéral sur le gouvernement d'entreprise, FF 2006 7799 ss, 7834: « La forme organisationnelle de la commission doit être réservée aux entités nécessitant une certaine indépendance politique pour l'exécution de leurs tâches, mais pour lesquelles l'octroi de l'autonomie juridique n'est pas conseillé au niveau de l'entité (p. ex. en raison d'une taille insuffisante) ni au niveau du regroupement de plusieurs entités (p. ex. en raison d'interdépendances indésirables ou d'absence de potentiel de synergies).»

[104] Voir pour un organigramme: http://www.fr.ch/atprd/fr/pub/presentation/organisation.htm



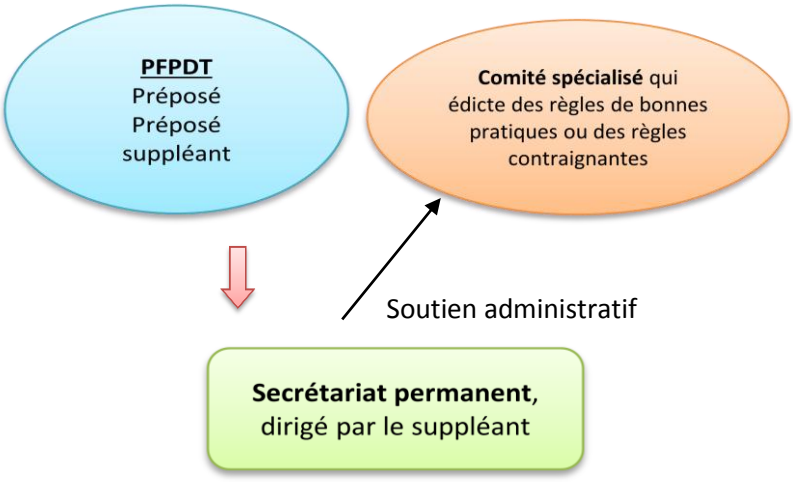
b) Autorité collégiale sans comité

Comme mentionné plus haut, *une minorité du groupe d'accompagnement* s'oppose à la création d'un comité spécialisé pour adopter/avaliser les règles de bonnes pratiques ou les règles contraignantes à l'intention des auteurs de traitements (voir ch. 4.1.2, let. b, et ch. 4.10.2, let. c). Elle estime que cela ne ferait que créer des charges administratives supplémentaires et affaiblirait au final la protection des données. Dans le cas de l'autorité collégiale sans comité spécialisé, l'élaboration et/ou l'approbation des règles de concrétisation serait assurée pas l'un des trois membres du directoire.

c) Maintien du système actuel avec comité

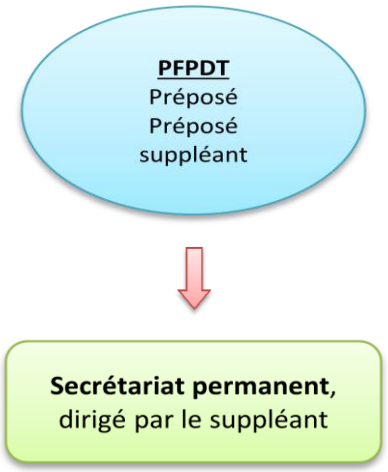
Le maintien du système actuel a pour avantage d'être simple et peu bureaucratique, et de garantir des réactions rapides de l'autorité de contrôle. On le connaît et on sait qu'il fonctionne. Le modèle du Préposé n'est au surplus pas rare. La majorité des cantons suisses a opté pour ce système, de même que de nombreux pays européens, tels l'Allemagne, le Royaume-Uni, la Hongrie, la Slovénie (sous le titre de « commissaire »), l'Espagne et la Pologne (sous le titre de « directeur »).

Pour renforcer l'indépendance de l'autorité de contrôle, il est proposé que le Préposé suppléant soit, comme le Préposé, aussi nommé par le Conseil fédéral moyennant accord de l'Assemblée fédérale.



d) Maintien du système actuel, sans comité

Comme mentionné plus haut, une *minorité du groupe d'accompagnement* s'oppose à la création d'un comité spécialisé pour adopter/avaliser les règles de bonnes pratiquesou les règles contraignantes à l'intention des auteurs de traitements (voir ch. 4.10.3, let. b, ci-dessus). Dans le cas du Préposé sans comité, l'élaboration et/ou l'approbation des règles de concrétisation serait assurée l'autorité de contrôle elle-même.



4.10.4 Renouvellement des rapports de fonction

Quel que soit le modèle d'organisation retenu, le groupe d'accompagnement propose de limiter le nombre de périodes de fonction des membres de l'autorité de contrôle à trois. Il estime que cela pourrait contribuer à leur indépendance et ouvrirait des perspectives de carrière, motivant ainsi des personnes qualifiées à postuler.

4.10.5 Collaboration entre autorités au plan national et international

En cas d'extension du champ d'application de la LPD aux traitements de données par les organes cantonaux, il aurait été opportun d'institutionnaliser et de renforcer la collaboration entre l'autorité de contrôle fédérale et les autorités cantonales. Puisque le groupe d'accompagnement a renoncé à une telle extension (ch. 4.2.1, let. a), il lui semble que la situation actuelle, basées principalement sur des échanges volontaires, ponctuels et informels, peut être maintenue.

Il faudra en revanche examiner la question de l'introduction de règles de coordination entre l'autorité de contrôle fédérale et les autorités cantonales, en cas de conflit de compétences positifs par exemple. Il faudra également examiner l'opportunité d'introduire des règles de coopération entre l'autorité de contrôle fédérale et les autorités de contrôle étrangères.

4.10.6 Financement

Le groupe d'accompagnement s'est penché sur la question de savoir comment les éventuelles nouvelles tâches de l'autorité de contrôle seraient financées. Il est en effet à prévoir que ces dernières, en particulier celles découlant du renforcement et de l'extension des attributions de l'autorité de contrôle, entraîneront un besoin en ressources supplémentaires (cf. ch. 4.10.2).

Une majorité du groupe d'accompagnement est d'avis qu'il faut mettre davantage de moyens financiers à la disposition de l'autorité de contrôle. Elle estime que ce financement doit continuer à être assuré par le biais du budget ordinaire de la Confédération, c'est-à-dire des recettes fiscales générales.

Une minorité du groupe d'accompagnement propose en revanche l'introduction d'une taxe comme source de financement supplémentaire. L'obligation de verser cette dernière pourrait être réglée de façon analogue à celui prévu par la législation britannique [105]; le traitement commercial de données électroniques serait soumis à enregistrement, lui-même soumis au paiement d'une taxe (dont le montant dépendrait par exemple de la taille de l'entreprise). Plusieurs membres du groupe d'accompagnement considèrent que cette solution entraînerait une importante charge administrative, serait difficile à mettre en œuvre dans un contexte international et pourrait entraîner une répercussion des frais sur le consommateur. En outre, il faudrait étudier plus en détail si l'introduction d'une telle taxe nécessite une base constitutionnelle. Cela dépend si l'on qualifie cette taxe d'impôt ou de contribution causale. Pour percevoir un impôt, la Confédération a besoin d'une compétence expresse et spécifique inscrite dans la Constitution fédérale. Une simple compétence matérielle ne suffit en règle générale qu'à justifier la perception d'émoluments ou de charges de préférence (contributions causales classiques), de taxes d'incitations à proprement parler ou de taxes s'en approchant. Le critère principal pour distinguer un impôt d'une contribution causale est celui de l'imputabilité. On parle d'impôt lorsque l'assujetti doit s'acquitter d'une contribution sans que l'État ne fournisse une contre-prestation qui lui profite individuellement (inconditionnalité de la contribution)[106]. Si l'on devait aménager une taxe pour financer les tâches de l'autorité de contrôle, il faudrait en particulier définir pour quelles activités de l'autorité de contrôle ou pour quelle(s) affectation(s) ces montants sont perçus, et qui y est assujetti.

Une réglementation telle que la connaît la Grande-Bretagne devrait vraisemblablement être considérée en Suisse comme un émolument administratif, ne requérant pas de base constitutionnelle. Cette taxe serait cependant limitée par les principes de la couverture des frais et de l'équivalence. Autrement dit, elle ne pourrait guère dépasser les frais administratifs liés à l'enregistrement et ne pourrait donc pas servir au financement d'autres tâches de l'autorité de contrôle. Il serait envisageable, à certaines conditions, de renoncer à la base constitutionnelle aussi pour la taxe de surveillance – à l'instar du cas de la surveillance des banques et des assurances privées – si le cercle des assujettis (p. ex. auteurs commerciaux de traitements de données électroniques) coïncidait avec delui des bénéficiaires de la redevance. Le montant devrait alors être fixé de manière à couvrir les frais du contrôle des assujettis (p.

---

[105] Le modèle britannique repose sur un enregistrement obligatoire des entreprises. En vertu du « Data Protection Act 1998 », tout « Data Controller » (en particulier des entreprises et des entreprises individuelles) doit s'enregistrer auprès de l'autorité de contrôle britannique, ICO. Des exceptions sont toutefois prévues. Les frais de la « Data Protection Registration » sont déterminés en fonction de la taille et du chiffre d'affaires de l'entreprise. Pour la plupart des entreprises, ils se montent à 35 livres. A partir d'une certaine valeur-seuil (chiffre d'affaires supérieur à 25,9 millions de livres et plus de 249 employés), la taxe atteint 500 livres. Pour les autorités étatiques comptant plus de 249 employés, les frais sont également de 500 livres. Voir à ce propos <http://ico.org.uk/for_organisations/data_protection/registration>.

[106] Voir l'expertise détaillée l'OFJ du 19 juillet 1999, in : VPB 2000, N° 25 (en allemand avec résumé en français). Dans ce document, l'OFJ a défendu une position un peu moins stricte, selon laquelle une base constitutionnelle explicite et spécifique est requise pour le prélèvement de telles redevances lorsqu'il n'y pas de lien d'imputation entre le cercle des assujettis et l'affectation de la redevance ou lorsque l'intensité de ce lien est trop faible (ch. A/III./1./b). S'agissant de la perception annuelle de taxes forfaitaires dans le domaine de la surveillance des banques et des assurances privées ainsi que de la prévention des accidents de la route, l'OFJ a conclu qu'il devait y avoir congruence entre le cercle des assujettis et le cercle de personnes qui bénéficient, comme groupe, de l'utilisation de ces fonds. Il lui paraissait par conséquent acceptable que les taxes de surveillance et la contribution à la prévention des accidents soient fondées sur la compétence matérielle de la Confédération dans les domaines concernés et qu'il soit renoncé à une base constitutionnelle explicite et spécifique pour ces redevances.

ex. auteurs commerciaux de traitements de données électroniques). Les frais de surveillance des autres auteurs de traitements (p. ex. auteurs privés et non commerciaux de traitements, organes fédéraux) ne pourraient par contre pas être couverts par une telle taxe (sans base constitutionnelle ad hoc). Un tel système serait très complexe dans sa mise en œuvre et générerait de nouveaux investissements en personnels et financiers.

Le groupe d'accompagnement a également examiné un modèle (appliqué en Espagne p. ex.) où les recettes du budget proviennent des amendes prononcées par l'autorité de contrôle, mais il l'a rejeté pour plusieurs raisons. Tout d'abord, il n'a pas encore été décidé si l'autorité de contrôle sera investie de compétences de prononcer des sanctions pécuniaires et, dans l'affirmative, si ces dernières permettraient de générer suffisamment de rentrées (cf. ch. 4.10.2). Ensuite, la majorité du groupe d'accompagnement est d'avis qu'une telle approche serait en contradiction avec les principes de la politique financière. Enfin, il ne faut pas que l'on ait l'impression que l'autorité de contrôle prononce des sanctions pour s'autofinancer.

Pour renforcer l'indépendance de l'autorité de contrôle, le groupe d'accompagnement propose de lui octroyer une compétence budgétaire similaire à celle du Contrôle fédéral des finances[107]. La conséquence serait que le budget de l'autorité de contrôle serait soumis directement au Parlement (sans modification par le Conseil fédéral).

4.11 Dispositions pénales

La LPD contient actuellement deux dispositions pénales, les art. 34 et 35. D'autres dispositions figurent dans le code pénal aux art. 179 ss CP, soit dans la partie consacrée aux infractions contre le domaine privé ou secret. Il s'agit d'examiner si ces articles, compte tenu notamment des développements technologiques (drônes, Google Glasses, Dashcams, etc.) doivent être maintenus tels quels, doivent être renforcés (p. ex. en en faisant des infractions poursuivies d'office), ou encore s'il convient d'en créer d'autres.

Une partie des membres du groupe d'accompagnement estime qu'il faut introduire dans le code pénal une disposition concernant l'usurpation d'identité. Il est dans un premier temps proposé d'attendre de voir si le Conseil national donne suite ou non à la motion Comte 14.3288 « Faire de l'usurpation d'identité une infraction pénale en tant que telle », dont le Conseil fédéral proposait le rejet, mais qui a été acceptée par le Conseil des États le 12 juin 2014[108].

4.12 Dispositions finales

Les dispositions relatives aux compétences législatives du Conseil fédéral (art. 36 LPD) et à l'exécution par les cantons (art. 37 LPD) doivent être adaptées aux modifications décrites aux ch. 4.1 à 4.11. Enfin, il faut prévoir des dispositions transitoires pour les innovations proposées (cf. art. 38 LPD).

5. Forme de l'acte normatif et contexte normatif

Bases constitutionnelles : la Constitution fédérale ne contient aucune disposition attribuant expressément à la Confédération une compétence législative dans le domaine de la protec-

[107] Voir art. 2, al. 3, de la loi sur le Contrôle des finances (LCF, RS 614.0).

[108] Lors de sa séance du 17 octobre 2014, la Commission des affaires juridiques du Conseil national a recommandé, par 19 voix contre 1, l'adoption de la motion Compte 14.3288.

tion des données[109]. En revanche, certaines compétences fédérales englobent la faculté pour la Confédération d'édicter aussi des dispositions en matière de protection des données. Dans le secteur privé, le législateur peut notamment s'appuyer sur sa compétence législative dans le domaine du droit civil (art. 122 Cst.)[110]. Dans le domaine du droit public, la compétence de la Confédération d'édicter des dispositions de protection des données applicables à l'administration résulte de son pouvoir d'organisation selon l'art. 173, al. 2, Cst. La Confédération n'a en revanche pas la compétence d'édicter des dispositions sur la protection des données pour les administrations cantonales et communales[111],[112]. Les mesures prévues au ch. 4 de la présente esquisse d'acte normatif peuvent, selon le groupe d'accompagnement, être fondées sur les bases constitutionnelles existantes. Une révision partielle de la Constitution serait toutefois requise si :

- la répartition des compétences entre Confédération et cantons dans le domaine de la protection des données devait être modifiée et si le champ d'application de la LPD devait être étendu aux organes cantonaux (cf. ch. 4.2.1, let. a, où il est toutefois proposé de renoncer à une telle mesure) ; et
- une taxe prenant la forme d'un impôt devait être introduite pour financer les tâches de l'autorité de contrôle (cf. ch. 4.10.6).

Réglementation aux niveaux de la loi et de l'ordonnance : les adaptations proposées au ch. 4 visent essentiellement la révision de la LPD elle-même. Vu que plus de la moitié de ses dispositions seront touchées, une révision totale de la loi est indiquée.

Une révision de la loi nécessitera une adaptation des ordonnances d'exécution (OLPD, OCPD). Il se peut que des modifications ponctuelles soient nécessaires aussi dans des lois procédurales (CPC, PA, LTAF, LTF). En outre, une révision de la LPD impliquera de vérifier si les dispositions de protection des données contenues dans des lois spéciales (cf. ch. 4.1 et 4.9.1) satisfont encore aux nouvelles exigences de la LPD. Enfin, il faudra examiner la nécessité de modifier les dispositions pénales sur la protection de la sphère secrète et privée (en particulier les art. 179 ss CP) (cf. ch. 4.11).

Droit international : les travaux de révision de la LPD doivent prendre en compte les réformes en cours en matière de protection des données au Conseil de l'Europe et dans l'UE. Ils doivent en particulier créer les conditions nécessaires à une éventuelle ratification de la Convention STE 108 modernisée (cf. le ch. 2 à ce propos).

---

[109] L'art. 13, al. 2, Cst. stipule certes que « toute personne a le droit d'être protégée contre l'emploi abusif des donées qui la concernent ». Mais il s'agit ici d'un droit fondamental, qui ne confère aucune compétence à la Confédération. Une révision de cette disposition constitutionnelle fait d'ailleurs l'objet de l'initiative parlementaire Vischer 14.413 « Droit fondamental à l'autodétermination en matière d'information », qui vise la modification de l'art. 13, al. 2, Cst. de sorte « à faire de la protection des données un droit fondamental à l'autodétermination en matière d'information au lieu d'un droit à la protection contre les abus ». La Commission des institutions politiques du Conseil national (CIP-CN) a donnée suite à cette initiative parlementaire le 29 août 2014.

[110] D'autres normes constitutionnelles pertinentes sont par exemple l'art. 95 Cst. (compétence de la Confédération pour légiférer sur l'activité économique lucrative privée) et l'art. 97 Cst. (compétence de la Confédération en matière de protection des consommateurs).

[111] Sous réserve des cas dans lesquels les cantons traitent des données en exécution du droit fédéral (cf. art. 37 LPD).

[112] Cf. le message du Conseil fédéral du 19 février 2003 relatif à la révision de la loi sur la protection des données (LPD), FFI 2003 1915, 1961 s.

6. Structure générale de la réglementation

Le groupe d'accompagnement propose de maintenir pour l'essentiel la structure de l'actuelle LPD et de la compléter là ou cela est nécessaire (cf. ch. 4). La nouvelle loi comprendrait vraisemblablement plus d'articles et contiendrait des dispositions :

- relatives au but, au champ d'application et aux définitions ;
- générales sur la protection des données, applicables aussi bien aux organes de la Confédération qu'aux privés (principes du traitement de données, droits des personnes concernées, communication transfrontière, procédures de certification) ;
- relatives au traitement de données par des particuliers (états de fait portant atteinte à la personnalité, motifs justificatifs, dispositions procédurales)
- relatives au traitement de données par des organes fédéraux (en particulier exigence de bases légales suffisantes pour le traitement, dispositions de traitement spécifiques, dispositions procédurales) ;
- relatives à l'organisation et aux tâches de l'autorité de contrôle ;
- relatives à la procédure de contrôle ;
- relatives au mode alternatif de règlement des litiges et à la création d'un organe de médiation ;
- relatives au comité chargé d'édicter ou d'approuver les réglementations de détail concernant l'application de la LPD ou les règles de bonnes pratiques ;
- pénales ; et
- finales (exécution, dispositions transitoires).

7. Densité normative (degré de détail)

La loi sur la protection des données est conçue de manière technologiquement neutre. Elle contient surtout des règles de fond qui sont valables pour toute utilisation de données personnelles. Il faudra par conséquent éviter une trop grande spécialisation et une trop grande précision. Les principes généraux de traitement des données doivent en particulier être formulés de manière assez abstraite afin de laisser aux autorités une marge de manœuvre suffisante. Le groupe d'accompagnement propose par conséquent de maintenir l'actuelle densité normative de la LPD.

Pour améliorer la mise en œuvre de la loi et la sécurité du droit, le groupe d'accompagnement estime qu'il faut d'avantage concrétiser le droit de la protection des données à un autre niveau réglementaire. Il est ainsi prévu de préciser la LPD par le biais de bonnes pratiques ou de dispositions réglementaires plus détaillées (ch. 4.1.2, let. b). Une majorité du groupe d'accompagnement est d'avis que ce but peut être atteint au moyen de règles de bonnes pratiques non contraignantes. Ces règles devraient être établies ou approuvées par un comité d'experts (cf. 4.1.2, let. b, 4.10.2, let. c, et 4.10.3).

8. Calendrier

Le Conseil fédéral a chargé le DFJP de lui soumettre, d'ici à la fin de 2014, des propositions sur la suite des travaux pour une éventuelle révision de la LPD. À cet effet, l'OFJ va élaborer – en tenant compte de la présente esquisse d'acte normatif – une note de discussion à l'intention du Conseil fédéral. Étant donné que le CAHDATA achèvera vraisemblablement ses travaux concernant le projet de modernisation de la Convention STE 108 en décembre

2014 (cf. ch. 2), il pourrait être judicieux de ne soumettre la note de discussion au Conseil fédéral qu'au début de 2015, de manière à ce que les résultats au sein du Conseil de l'Europe puissent être pris en compte dans le processus de prise de décision.

La note de discussion doit répondre à des questions fondamentales sur le contenu et proposer un calendrier pour la suite des travaux. Pour ce dernier, le groupe d'accompagnement envisage trois options :

- Attendre que les réformes européennes dans le domaine de la protection des données soient terminées avant d'entamer la révision de la LPD.
- Charger le DFJP d'élaborer un avant-projet de révision de la LPD sans attendre la fin des travaux de réforme européens.
- Charger le DFJP d'élaborer un avant-projet de révision de la LPD, en prévoyant un délai suffisamment long (p. ex. deux ans) afin que l'on sache quelles adaptations du droit suisse sur la protection des données sont nécessaires pour une ratification de la Convention STE 108 modernisée et qu'il puisse en être tenu compte.

Annexe : prises position de certains membres du groupe d’accompagnement

economiesuisse

per Mail
Frau Monique Cossali Sauvain
Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz (BJ)
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik
Bundesrain 20
3003 Bern

23. September 2014

Stellungnahme economomiesuisse zum Normkonzept Revision Datenschutzgesetz (DSG)

Sehr geehrte Frau Cossali

Sie haben uns eingeladen, zum Normkonzept zur Revision Datenschutzgesetz (DSG) (Fassung vom 10. September 2014) Stellung zu nehmen, falls wir dies wünschen. Für die gebotene Gelegenheit zur Meinungsäusserung danken wir Ihnen bestens und machen nachfolgend gerne davon Gebrauch. Zu diesem Zeitpunkt beschränken wir uns dabei auf die wichtigsten Punkte mit grundlegendem Charakter und ohne einen Anspruch auf Vollständigkeit zu erheben.

Ein funktionierender Datenschutz ist aus Sicht der Wirtschaft wichtig

Die Diskussion über den Datenschutz ist vor dem Hintergrund des technologischen Wandels angebracht und muss geführt werden. **Für die Wirtschaft ist ein angemessenes und wirksames Datenschutzgesetz wichtig. Massvolle und klare Bestimmungen lassen Raum für die wirtschaftliche Entfaltung und dienen der Rechts- und Investitionssicherheit. Sie ermöglichen die Entwicklung und den Einsatz von innovativen digitalen Produkten und industriellen Anwendungen.**

Darüber hinaus sind Akzeptanz und Vertrauen der Nutzer in den Datenschutz eine zentrale Voraussetzung für die Fortentwicklung der immer wichtiger werdenden digitalen Wirtschaft und die Nutzung des damit verbundenen wirtschaftlichen Potenzials. Der überwältigende Teil der Unternehmen hat denn auch ein grosses Interesse daran, dass datenschutzrechtliche Vorschriften eingehalten werden – nicht nur im eigenen Haus, sondern auch durch die anderen Wettbewerber. Andernfalls drohen massive Reputationsschäden, die nicht nur die unmittelbar betroffenen Unternehmen belasten, sondern gleich ganze Branchen in Mitleidenschaft ziehen können. Ausserdem besteht das Risiko, dass nicht datenschutzkonforme Produkte, Dienstleistungen und ganze Geschäftsmodelle nachträglich verboten werden und damit bereits getätigte Investitionen verloren gehen.

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

Intelligente Datenschutzvorschriften, die ein gutes Datenschutzniveau bieten, sind für die Unternehmen und für den Wirtschaftsstandort Schweiz ein Vorteil. Überschiessende und im Geschäftsalltag nicht praktikable Regulierungen wirken sich hingegen innovationshemmend aus und können der Wettbewerbsfähigkeit von Unternehmen im internationalen Umfeld schaden. Sie treffen ebenso die Nutzer, die nicht von neuen Produkten und Dienstleistungen profitieren können. Nicht umsonst heisst es denn auch in der Botschaft zum geltenden DSG, dass die durch die immer besseren Technologien ermöglichte Entwicklung nicht verhindert oder eingeschränkt werden soll (Bundesrat / BBl 1988 II 417). Diese Feststellung gilt uneingeschränkt auch für die Gegenwart.

Bei einer geplanten DSG-Revision ist auch zu beachten, dass beim Datenschutzrecht, das eine Konkretisierung des Grundrechts zum Schutz auf Privatsphäre (Art. 13 BV) darstellt, der Schutzaspekt im Verhältnis *zwischen Staat und Bürger* die höchste Bedeutung ist. Demgegenüber ist das Verhältnis *zwischen Privaten* vom Grundsatz der Privatautonomie geprägt, weshalb in diesem Bereich übermässige Datenschutzregulierungen besonders problematisch und rechtfertigungsbedürftig sind und nur mit Zurückhaltung erlassen werden dürfen. Der Nutzen, den die sich verbessernden Informationstechnologien bieten, soll nicht leichtfertigt geopfert werden. Jeder Einzelne soll im Privatbereich grundsätzlich selbst entscheiden können, ob er ein bestimmtes (allenfalls mit einer Bekanntgabe gewisser Daten verbundenes) Angebot nutzen möchte oder nicht. Als mündiger Bürger ist er dazu auch ohne weiteres in der Lage.

Weiter gilt es auch im Blick zu behalten, dass Datenschutzrecht nicht Konsumentenrecht ist. Die beiden Bereiche verfolgen unterschiedliche Schutzzwecke und sollen folglich nicht vermischt werden: Während das erste nämlich auf den Grundrechtschutz ausgerichtet ist; bezieht sich das zweite auf kommerzielle Beziehungen zwischen Anbietern und Abnehmern. Daher haben etwa Instrumente wie Sammelklagen oder vom allgemeinen haftpflichtrechtlichen Regime abweichende Schadenersatzklagen etc. keinen Platz im DSG.

<u>Grundsätzliche Bemerkungen zum gesellschaftspolitischen Umfeld und zum Revisionsprojekt DSG</u>

In den letzten Jahren ist die Präsenz des Themas Datenschutz in den Medien und der öffentlichen Wahrnehmung gestiegen, und es hat in der politischen Agenda an Bedeutung gewonnen. Das hat verschiedene Gründe: Zum einen haben spektakuläre Überwachungs- und Spionageaffairen und das Bekanntwerden schwerwiegender Eingriffe in die Privatsphäre der Bürger durch geheimdienstliche Behörden die Sensibilität für den Datenschutz erhöht (obschon es hier eigentlich nicht um Probleme des Datenschutzes sondern vielmehr der Datensicherheit geht). Sie haben teilweise auch ein diffuses Unbehagen gegenüber den Möglichkeiten, die mit den neuen Informations- und Kommunikationstechnologien einhergehen, hervorgerufen. Dieser Eindruck wird zusätzlich verstärkt durch Meldungen über Hackerattacken und Datendiebstahl bzw. -verluste bei einzelnen grossen in- und ausländischen Unternehmen. Weiter hat mit den verbesserten Bearbeitungsmöglichkeiten und höheren Speicherkapazitäten die Menge der verarbeiteten Daten zugenommen. Gleichzeitig entstehen zahlreiche neue internetbasierte Geschäftsmodelle und Anwendungen, und die Sozialen Medien erleben einen regelrechten Boom. Mit diesen Entwicklungen gehen auch Fragen betreffend den (zu leichtfertigen) Umgang mit persönlichen Daten einher. Zudem ergingen einige vielbeachtete letztinstanzliche Grundsatzentscheide zu relevanten datenschutzrechtlichen Fragen, die eine Handvoll besonders technologienaher Unternehmen betrafen (vgl. die Bundesgerichtsentscheide betreffend Logistep und Google Street View oder das EuGH-Google-Urteil betreffend Löschungsrecht).

So notwendig die Diskussion um den Datenschutz in diesem sich verändernden gesellschaftlich-technologischen Umfeld ist, so essentiell ist es mit Blick auf eine mögliche Revision des DSG, dass

das bewährte heutige Datenschutzregime nicht ohne Notwendigkeit und zeitliche Dringlichkeit über den Haufen geworfen wird; vor allem Im Privatbereich. **Bevor eine Revision an die Hand genommen wird, müssen zwingend der tatsächliche Handlungsbedarf anhand von Fakten und empirischen Untersuchungen konkret ausgewiesen sowie das angestrebte Ziel klar definiert sein. Es ist transparent und detailliert aufzuzeigen, inwiefern genau die geltenden Regelungen ihre Wirkung verfehlen und ob bzw. mit welchen Mitteln ein allfälliger Missstand effektiv behoben werden kann.** Nur so lassen sich die verschiedenen Alternativen (inklusive eines „Nichtstuns“) abschätzen. Und nur so lassen sich die Interessen gegeneinander abwägen und ausgleichen, und lässt sich die Verhältnismässigkeit von neu vorgeschlagenen Vorschriften überprüfen. Diese Kriterien sind beim laufenden Revisionsprojekt jedoch nicht erfüllt.

Darüber hinaus darf eine Revision auch nicht nur auf einige wenige vielbeachtete Einzelfälle bzw. auf eine Branche oder gar ein paar wenige internationale Konzerne gemünzt sein. Denn **das DSG gilt für die gesamte Wirtschaft – für alle Industriezweige, grosse und kleine, national wie international tätige Unternehmen. Durch unpassende Regulierungen, die ihr eigentliches Ziel verfehlen oder darüber hinausschiessen, werden alle Unternehmen getroffen. Deshalb muss sich eine Revision auf die wesentlichen Punkte beschränken auf einer konkreten und detaillierten Risikoanalyse aufbauen. Dabei sind die angeblichen Lücken genau aufzuzeigen, und es ist zu benennen, was die Folge einer Nichtregelung im Privatbereich wäre.**

Fehlender Handlungsbedarf für eine umfassende DSG-Revision

Der Bedarf für eine umfassende DSG-Revision ist nach wie vor nicht konkret bzw. unzureichend ausgewiesen. Nur sechs Jahre nach der letzten Revision braucht es für den Privatbereich keine neuerliche Überarbeitung des Gesetzes, die über formelle Anpassungen wie z.B. eine übersichtlichere Darstellung oder allenfalls einzelne punktuelle Verbesserungen hinausgeht. Allein der Umstand, dass sich das technologische und gesellschaftliche Umfeld weiterentwickelt, ist jedenfalls kein Anlass, von einem funktionierenden System abzuweichen. Das DSG wurde bewusst technologieneutral ausgestaltet, und es hat sich seither bestens bewährt. economiesuisse lehnt daher eine Revision in der vorgesehenen Form ab. Insbesondere sehen wir nicht, wo und inwiefern beim geltenden Recht Mängel bestehen sollten, die einen so weitgehenden gesetzgeberischen Eingriff erforderlich machen würden.

Ziel der 2010 im Auftrag des Bundsamts für Justiz (BJ) durchgeführten Evaluation des DSG war es, das DSG auf seine Wirksamkeit hin zu überprüfen. Im Vordergrund standen erstens die Bekanntheit und die Durchsetzungsmechanismen des Gesetzes einerseits sowie die Stellung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) andererseits. Der Schlussbericht zur Evaluation vom 9. Dezember 2011 weist zusammenfassend auf die technologische Entwicklung als Herausforderung hin (S. I), er stellt aber keine schweren Mängel fest. Vielmehr hält als Gesamtbilanz fest, dass der EDÖB seinen gesetzlichen Auftrag erfülle und dabei eine hohe Wirksamkeit erziele und seine Aufsichtstätigkeit im Einzelfall wirksam sei: In der Mehrheit der Sachverhaltsabklärungen stelle er nur geringfügige Probleme fest, welche die Datenbearbeiter anschliessend freiwillig behöben. Spreche er bei grösseren Mängeln Empfehlungen aus, würden diese grossmehrheitlich umgesetzt, entweder direkt oder nach einem Gerichtsurteil. Bei Bearbeitungen, die intransparent sind oder im Ausland erfolgen, stosse die Aufsicht an Grenzen. Zudem mache der EDÖB heute aus Ressourcengründen keine stichprobenartigen Kontrollen, was der Breitenwirkung der Aufsicht abträglich sei. Mit einer präventiven Wirkung auf andere Datenbearbeiter sei aber insofern zu rechnen, als bekannt werdende Missstände öffentliches Interesse erregen (S. III f.). Es gebe auch deutliche Hinweise, dass das Risiko eines Imageschadens das Verhalten zugunsten des Datenschutzes beeinflusst (S. II). Auch die Beratungs- und Informationstätigkeit würden von den

Bearbeitern insgesamt als nützlich, praxisnah und konstruktiv bewertet (S. III f.). Bezüglich des Verhaltens der Nutzer hält der Bericht fest, dass die Betroffenen die neuen Möglichkeiten der Informationsgesellschaft mehrheitlich begrüssten (S. 66). Sie erachteten Datenschutz zwar als wichtig, schützten sich aber nicht immer konsequent selbst und gäben persönliche Daten bisweilen grosszügig preis. Betreffend die Schutzrechte gelangt der Bericht zum Schluss, dass die im DSG verankerten Durchsetzungsrechte der Betroffenen im internationalen Rechtsvergleich gut ausgebaut seien sowie dass Betroffene den Rechtsweg selten beschritten (S. II). Das Fazit des Berichts lautet: Vom DSG gehen klare Wirkungen zugunsten des Datenschutzes aus. Gleichzeitig sind die Wirkungen des EDÖB in verschiedener Hinsicht begrenzt und die Betroffenen machen wenig Gebrauch von den vorhandenen Durchsetzungsrechten (S. IV). Über die Gründe hierfür kann im Bericht nur spekuliert werden: Als mögliche Erklärung wird „erstens die vermutlich geringe Bekanntheit der Durchsetzungsrechte und des Rechtswegs sowie das geringe Wissen über die Anwendung dieser Rechte" genannt. Und zweitens „dürfte aus Sicht der Betroffenen ein vergleichsweise beträchtlicher Aufwand einer Klage einem diffusen und nicht gesicherten Nutzen gegenüberstehen" (S. II f.).

Aus dem Bericht des Bundesrates vom 9. Dezember 2011 zur Evaluation des DSG drängt sich kein dringender Handlungsbedarf auf, weder in inhaltlicher noch zeitlicher Hinsicht. Insbesondere lässt sich aus dem Papier nicht herleiten, dass das DSG seine bzw. die gewünschte Schutzwirkung nicht entfalte. Ebenso wenig legt es nahe, dass etwa die Durchsetzungsrechte oder die Kompetenzen der Aufsichtsbehörde zu schwach wären und daher ausgebaut werden sollten oder gar müssten. Vielmehr hält der Bericht fest, dass es in einem weiteren Schritt Aufgabe der Politik sei zu entscheiden, ob eine umfassende Diskussion über den Datenschutz geführt werden soll und welches das gewünschte Schutzniveau des DSG sein solle (S. IV, S. 215). So werden im Bericht denn auch ausdrücklich nicht Empfehlungen ausgesprochen, sondern mögliche Handlungsoptionen angedacht. Diese (teilweise sehr einschneidenden) Optionen haben „eher der Charakter von Gedankenanstössen als derjenige eines Arbeitspapiers im Hinblick auf die Formulierung im Einzelnen analysierter Vorschläge" (S. 215, 217).

economiesuisse fordert, dass keine umfassende DSG-Revision wie die geplante in Angriff genommen wird, ohne dass angebliche Missstände unter dem geltenden DSG klar belegt sind. Hierbei muss auf Fakten abgestellt werden. Gesetzgeberischer Aktivismus, getrieben von einem unbestimmten Misstrauen gegenüber dem veränderten technologischen Umfeld und ausgehend von Stimmungen oder blosse Vermutungen, ist verfehlt. So kann etwa aus der Tatsache, dass die Nutzer selten den Rechtsweg beanspruchen, keineswegs automatisch auf Defizite des DSG geschlossen werden. Die geringe Beanspruchung der Gerichte sehen wir im Gegenteil als Hinweis darauf, dass das heutige Datenschutzsystem seinen Zweck erfüllt. So lieferten denn auch etwa die Fälle Logistep, Google Streetview oder Moneyhouse – die gerne als Beispiele für die mit den neuen Technologien verbundenen Problematiken angeführt werden – keinerlei Hinweise darauf, dass im geltenden Recht etwa die Klagerechte zu schwach ausgestaltet wären, Beweisschwierigkeiten bestünden, die Kompetenzen des EDÖB zu wenig weit reichten oder Sanktionsmöglichkeiten fehlten. Vielmehr ging es in diesen Fällen jeweils um Auslegungsfragen des DSG, in denen die angerufenen Gerichte Klarheit schafften.

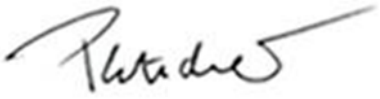
<u>Anpassung an internationale Bestrebungen (EU/Europarat) nur sofern für Marktzugang zwingend</u>

Das durch das geltende DSG garantierte Schutzniveau ist im internationalen Vergleich bereits hoch; eine Verschärfung insbesondere im Privatbereich ist unnötig. Ein überzogenes, „veradministriertes" Datenschutzrecht würde die Schweiz global gesehen ins Hintertreffen bringen. Dabei darf sich der Vergleich nicht allein an Europa orientieren, sondern der Blick ist darüber hinaus insbesondere auch auf die USA und Asien zu richten. Ein im Verhältnis zur EU schlank

ausgestaltetes, „smartes“ Datenschutzrecht ist ein willkommener Wettbewerbsvorteil für die Schweizer Wirtschaft.

Wenn überhaupt, besteht Handlungsbedarf aus Sicht von economiesuisse nur für den Fall und insoweit, als durch die Revisionen auf europäischer Ebene der Marktzugang zur EU betroffen ist. Bevor das Schweizer Recht erneut revidiert wird, sollten unbedingt zuerst die Resultate der laufenden Entwicklungen in der EU und im Europarat abgewartet werden. Eine allfällige Anpassung an das europäische Recht bzw. Umsetzung ins nationale Recht soll schliesslich nur dort erfolgen, wo dies unter dem Gesichtspunkt des Marktzugangs zwingend notwendig ist. Dazu muss bei jeder vorgeschlagenen Änderung nachvollziehbar sein, welches das unbedingte gesetzgeberische Minimum ist, um die Gleichwertigkeit mit dem europäischen Datenschutzstandard zu erfüllen. Hierbei ist zu bedenken, dass es keiner absoluten Gleichwertigkeit bedarf (vgl. die Safe-Harbor-Lösungen im Verhältnis CH/EU-USA). Der Schweizer Gesetzgeber darf auf keinen Fall überhastet und ohne ausgewiesene Notwendigkeit übertriebene Regelungen ungeprüft aus dem europäischen Umfeld übernehmen. Der vorhandene Spielraum ist weitestmöglich auszunützen.

Freundliche Grüsse
economiesuisse



Thomas Pletscher
Mitglied der Geschäftsleitung

Dr. Marlis Henze
Wissenschaftliche Mitarbeiterin

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

Aktennotiz

Geht an Bundesam für Justiz, Frau Monique Cossali, Leiterin der Belgeitgruppe DSG

Bern, 6. Oktober 2014 sgv-Kl

Stellungnahme des sgv zum Normkonzept zur Revision des Datenschutzgesetzes (DSG) (Version vom 10.9.2014)

Die vorliegende Stellungnahme bezieht sich auf das Normkonzept vom 10. September 2014 und erhebt keinen Anspruch auf Vollständigkeit. Sie gibt lediglich die Position des sgv in den wichtigsten Punkten wieder.

Grundsätzliche Bemerkungen

Die letzte grössere Revision des DSG liegt 6 Jahre zurück. Nach Ansicht des sgv ist es verfrüht, an den eben erst geschaffenen Grundlagen zu rütteln. Eine Revision des DSG rechtfertigt sich derzeit nicht. Zuerst sollen die Ergebnisse der Diskussionen in der EU und im Europarat abgewartet und dann allenfalls notwendige Anpassungen des DSG vorgenommen werden.

Aus dem Bericht des Bundesrates vom 9. Dezember 2011 wird nicht klar ersichtlich, wo genau eine Revision des DSG ansetzen soll. Ziel des Berichts war es gemäss Bundesrat, „das Datenschutzgesetz auf seine Wirksamkeit hin zu überprüfen. Im Vordergrund der Untersuchung standen die Bekanntheit des Gesetzes und seine Durchsetzungsmechanismen einerseits sowie die Stellung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) andererseits“. Im Bericht wird festgehalten, dass die technologischen Entwicklungen das DSG herausfordern. Zudem würde es immer schwieriger, die Kontrolle über einmal bekannt gegebene Daten zu behalten. Aufgrund der Ergebnisse der Evaluation ist der Bundesrat der Auffassung, dass zu prüfen ist, inwieweit und in welcher Weise die Datenschutzgesetzgebung anzupassen ist, um den rasanten technologischen und gesellschaftlichen Entwicklungen Rechnung zu tragen. Aus dem Bericht wird klar, dass der EDÖB zusätzliche Ressourcen geltend macht.

Der Schweizerische Gewerbeverband sgv ist der Auffassung, dass die Öffentlichkeit gut informiert ist. Dafür sorgen nicht nur zahlreiche Publikationen von Konsumentenorganisationen, sondern z.B. auch die Webseite des EDÖB, von der sich jedermann nützliche Informationen zur Rechtslage herunterladen kann. Die Diskussion um social media und den Schutz der Persönlichkeit gegen den Missbrauch von grundsätzlich frei zugänglichen Daten ist berechtigt und notwendig. Sie darf aber nicht zum Aufbau einer weiteren Bürokratie führen.

Stellungnahme zu den Eckwerten des Normkonzepts (contenu essentiel de la révision)

4.1 Concept et mise en oeuvre

Der sgv unterstützt die Stossrichtung, dass das Datenschutzgesetz technologieneutral ist und sich auf die grundlegenden Prinzipien fokussiert. Da der Datenschutz sehr unterschiedliche Anforderungen haben kann, macht es Sinn, weiterhin sowohl ein allgemeines DSG als auch die spezialgesetzlichen Regelungen zu haben.

Allein aus der Tatsache, dass heute betroffene Personen ihre Rechte gegenüber Datenbearbeitern nur selten beanspruchen, nur wenige Betroffene Klage einreichen und Prozesse über datenschutzrechtliche Fragen führen, ist kein hinreichender Grund zur Stärkung der Kontrollbehörde. Die relativ geringe Zahl gerichtlicher Verfahren kann ebenso gut mit einem von der Öffentlichkeit insgesamt als

befriedigend empfundenen System erklärt werden. Dass heute die Nachfrage danach so klein ist, ist ein deutliches Zeichen dafür, dass kein Handlungsbedarf besteht. Eine Stärkung des Datenschutzbeauftragten drängt sich aus Sicht des sgv im heutigen Zeitpunkt nicht auf. Neue gesetzliche Vorschriften sind nicht notwendig. Ein wichtiger Grundstein für den wirtschaftlichen Erfolg in der Schweiz ist die Wirtschaftsfreiheit. Unnötige, neue Einschränkungen - in welchem Bereich auch immer - sind zu vermeiden. Der bestehende Datenschutz hat sich bewährt. Die Wirtschaft sieht sich einer starken, mündigen Abnehmer- und Konsumentenschaft gegenüber, die ihren Ansprüchen schon jetzt durchaus Gehör zu verschaffen weiss. Zusätzliche Kontrollgremien sind nach Ansicht des sgv nicht nötig.

4.2 Champ d'application et définitions

Der sgv ist der Auffassung, dass sich die heute dualistische Verantwortung von Bund und Kantonen in der Datenschutzgesetzgebung bewährt hat. Eine Mehrheit der Begleitgruppe schlägt das Auswirkungsprinzip vor. Das Datenschutzrecht würde damit auch Anwendung auf Sachverhalte finden, die sich im Ausland zutragen, aber die in einem wesentlichen Rahmen Auswirkungen auf die Schweiz haben. Der sgv lehnt diese Position ab und unterstützt das Territorialitätsprinzip, da sich doch zu einem wesentlichen Zusatzaufwand bei international tätigen Firmen führen könnten. Zudem ist die Durchsetzbarkeit in der Praxis fraglich.

4.3 Principes généraux de protection des données personelles

Im Normkonzept wird die Stärkung der Informationspflicht des Datenbearbeiters gefordert. Bereits heute gibt es das Auskunftsrecht. Dieses wird – wie im Bericht festgestellt – eher zurückhaltend genutzt. Eine generelle Informationspflicht für jegliches Bearbeiten von Daten ist unverhältnismässig.

Das dem Obligationenrecht zugrundeliegende Zug-um-Zug Geschäft (Ware gegen Barzahlung) wird tendenziell an Bedeutung verlieren. Kann die Bezahlung nicht mehr Zug um Zug abgewickelt werden, so übernimmt notwendigerweise eine der involvierten Parteien das Risiko der Vorleistung und damit das Risiko eines Zahlungsausfalls. Zu den involvierten Parteien können nicht nur der Lieferant gehören, sondern auch aussenstehende Finanzierer (Leasinggeber, Kreditkartenunternehmen). Für den gewerblichen Alltag ist der einfache Zugang zu gesicherten Daten (z.B. zu Bonitätsprüfungen) deshalb von zentraler Bedeutung. Zahlreiche Lieferanten, welche täglich Waren gegen Rechnung liefern, erleiden in der Schweiz Jahr für Jahr hohe Verluste. Schon allein die amtlich erfassten, jährlichen Forderungsausfälle belaufen sich auf Milliarden. Die Betreibungs- und Konkursstatistik des BFS weist für die Zeit zwischen 2008 und 2013 Konkursverluste von mehr als 2 Mia pro Jahr aus. Zahlenmässig werden nur Ausfälle aus den durchgeführten Konkursverfahren erfasst. Weitaus grössere Verluste resultieren aus den mangels Aktiven eingestellten Konkursen (ca. 50 % aller Verfahren) sowie aus zehntausenden von Pfändungsverlustscheinen, die gegen Private und nicht im Handelsregister eingetragene Kleinunternehmen oder wegen unbeglichener Steuerforderungen ausgestellt werden. Laut der offiziellen Statistik mussten 2013 knapp 2.8 Mio. Zahlungsbefehle ausgestellt und mehr als 1,45 Mio. Pfändungen vollzogen werden. Nach Branchenschätzung bescheren Insolvenzen und fruchtlose Pfändungen Wirtschaft und Fiskus Jahr für Jahr Verluste von gegen CHF 11 Mia.

Informationspflichten, die grundsätzlich jedes Personendatum bis hin zur Adresse umfassen, haben übermässig aufwändige Rapport- und Dokumentationspflichten zur Folge und sind im gewerblichen Alltag nicht praktizierbar. Neue Rechtsunsicherheiten und Regulierungen mit hohen Folgekosten werden geschaffen. Unabhängig, ob es sich um eine gesetzliche Vorgabe oder um „good practice" handelt, die aktive Informationspflicht über jegliches bearbeitetes Personendatum wäre mit einem enormen administrativen Aufwand für jeden Inhaber einer Datei verbunden. Oftmals wird sich zudem kaum abschätzen lassen, ob die betroffene Person davon nun Kenntnis hat oder es zumindest wissen müsste, oder eben nicht. Die Rechtsunsicherheit wäre gewaltig. Informationspflicht kann aus Sicht des sgv aus den dargelegten Gründen nicht Bearbeitungsgrundsatz sein.

Dass die Bonitätsauskunft nicht allein auf das Betreibungsregister abstützten kann, zeigt das Beispiel eines Bauherren, der den Generalunternehmer oder die anderen am Bau beteiligten Personen prüfen

will, um sicherzustellen, dass Garantieleistungen auch in der Zukunft erbracht werden können. Eine Garantieverpflichtung nützt nichts, wenn ein Anbieter bereits vor dem Konkurs steht und nur darum ein günstiges Angebot abgegeben hat. In einem solchen Fall reicht die Betreibungsauskunft schon deswegen nicht, weil viele Forderungen aus Kostengründen schon vor der Betreibung abgeschrieben werden. Diese Ausfälle müssen dann von den ehrlichen und pflichtbewussten Konsumenten übernommen werden. Dies widerspricht der geltenden Auffassung, dass derjenige, der einen Schaden verursacht, diesen auch tragen soll. Betreibungsinformationen fallen erst zu einem späten Zeitpunkt an. Es ist für jede Vertragspartei wichtig, frühzeitig zu erfahren, ob die Gegenpartei Zahlungsprobleme hat oder nicht. In Anbetracht der sich gegenüberstehenden Interessen ist es fehl am Platz, Zahlungsinformationen und damit verbundene Angaben der Bearbeitung durch die willkürliche Unterstellung unter den Begriff des Persönlichkeitsprofils der Bearbeitung ganz oder teilweise entziehen zu wollen. Überdies hat ein Anbieter sicherzustellen, dass sich eine Person nicht unnötig überschuldet. Dies kann er nur sicherstellen, wenn er Zugang zu entsprechenden Bonitätsinformationen hat.

Pflicht zur Ernennung eines Datenschutzbeauftragten

Der Verwaltungsrat trägt die oberste Verantwortung und muss die Organisation der Unternehmung nach den Risiken des Unternehmens ausrichten. Im Übrigen auferlegt OR 716a dem Verwaltungsrat die unübertragbaren und unentziehbaren Verpflichtungen. Er hat die Pflicht zur Oberleitung der AG und haftet, wenn er diese Pflicht missachtet. Hierfür führt er eine Risikobeurteilung bzw. ein IKS. Die Pflicht zur Einsetzung eines Datenschutzbeauftragten macht in diesem Zusammenhang keinen Sinn und schiesst über das Ziel hinaus. Mit dem gleichen Recht könnte von jedem Unternehmen ein Produktionsverantwortlicher gefordert werden.

Das heutige DSG ermöglicht Zertifizierungsverfahren und die freiwillige Ernennung eines Datenschutzbeauftragten oder einer Datenschutzbeauftragen in einer Firma. Jede Firma, die überdies mit sensiblen Personendaten operiert, hat ein ureigenes Interesse daran, keine Reputationsschäden zu riskieren.

Der sgv lehnt eine generelle gesetzliche Pflicht zur Ernennung eines Datenschutzbeauftragten für Unternehmen ab, nicht aber für die öffentliche Hand.

Von einer aktiven Meldepflicht von Datenschutzverletzungen ist mindestens im Einzelfall abzusehen. Eine Meldepflicht macht dann allenfalls Sinn, wenn eine sehr grosse Öffentlichkeit, z.B. Tausende von Personen betroffen sind und die Umstände eine Meldung erst rechtfertigen (z.B. verschickt eine Bank an Tausende von Kundinnen und Kunden falsche Kontoauszüge).

4.4 Rechte der betroffenen Personen – Katalog der Rechtsansprüche

Auskunftsrecht: Der wichtigste Grundsatz für eine funktionierende Wirtschaft und ein vertrauensvolles Zusammenarbeiten ist eine objektive Abwägung der sich gegenüberstehenden Interessen. Nicht nur Lieferanten sind an der Möglichkeit von Bonitätsprüfungen interessiert. Auch Konsumentinnen und Konsumenten möchten prüfen, ob sie eine Vorauszahlung an einen Lieferanten leisten sollen oder nicht.

Recht auf Berichtigung: Die Möglichkeit, die Empfänger von Personendaten in Erfahrung zu bringen, widerspricht dem Recht des Datenbearbeiters auf Schutz seiner Kunden. Die Korrekturen haben ohne weitere Angaben über die Informationsempfänger zu erfolgen.

Recht auf Löschung: Zu unterscheiden ist zwischen dem Recht auf „Löschung“ und dem Recht auf „Sperrung“. Für die Sperrung braucht es eine Personenidentifikationsnummer die referenziert werden kann. Bei der Löschung sind in jedem Fall die Daten weg und es kann nicht sichergestellt werden, dass diese in der Zukunft nicht wieder aufgenommen werden. Der Kunde muss sich aber der Folgen bewusst sein. Zudem dürfen nur in begründeten Fällen Daten gelöscht werden, die nicht aus hoheitlichen Quellen stammen. Daten, die von der öffentlichen Hand publiziert werden, sollten nicht gelöscht

werden können. Das Recht auf Löschung darf nicht missbraucht werden um Gutgläubige zu täuschen.

Automatisierte Entscheidungsfindung: Es gibt keinen Anspruch auf Kredit. Insofern muss auch kein „erhöhtes Schutzbedürfnis“ bestehen. Es gibt auch keine Regeln oder Bestimmungen, welche Grundlagen in die Entscheidungsfindung für einen Lieferantenkredit oder Kredit miteinfliessen. Jede Person ist frei in der Auswahl ihrer Kriterien. Die Bonität ist auch nur eines davon. So zählt am Schluss oftmals das Bauchgefühl. Bei der Bearbeitung von einer kleinen Anzahl von Geschäften kann dies individuell gemacht werden und wird von den Unternehmen vielfach in einer „Creditpolicy“ zusammengefasst. Dies ist nötig, damit die Mitarbeitenden wissen wie sie vorzugehen haben. In diesem Fall gibt es für den Betroffenen kein Recht zu erfahren, warum ihm kein Lieferantenkredit gewährt wird. Er kann die Ware ja in jedem Fall kaufen, nur eben nicht auf Kredit sondern gegen Vorauskasse.

Der Vorschlag einer Mehrheit der Begleitgruppe zielt darauf ab, „jeder Person das Recht einzuräumen, keiner auf einer rein automatisierten Bearbeitung von Daten basierenden Entscheidung unterworfen zu werden. Bei einer automatisierten Kreditentscheidung ist das Vorgehen gleich wie im Einzelfall, mit dem Unterschied, dass die Kriterien aufgrund der grossen Anzahl von Transaktionen systemgestützt aufbereitet werden. Subjektive gestützte Beurteilungen werden hingegen eliminiert, was ein Vorteil ist. Das Nichtzulassen automatisierter Einzelentscheidungen ist allerdings ein Eingriff in die Wirtschaftsfreiheit.

Die Abbildung von zahlungsrelevanten Informationen stellt kein Persönlichkeitsprofil dar. Bezahlt jemand eine Rechnungen nicht, oder ist er im Konkursverfahren, so hat der zukünftige Gläubiger das Recht, vor der Gewährung eines Lieferantenkredits zu prüfen, ob bereits Anzeichen auf Zahlungsschwierigkeiten bestehen.

4.8 Besondere Bestimmungen betreffend das Bearbeiten von Personendaten durch private Personen

Beweislastumkehr: Nach den allgemein geltenden Regeln der Beweislastverteilung muss heute die betroffene Person den Nachweis einer Persönlichkeitsverletzung erbringen. Eine Mehrheit der Begleitgruppe möchte die Beweislast umkehren und das Gericht ermächtigen, vom Datenbearbeiter im Einzelfall den Nachweis einer datenschutzkonformen Bearbeitung verlangen zu können. Der sgv lehnt eine solche Beweislastumkehrung ab. Die vorgeschlagene Beweislastumkehr wird im Ergebnis dazu führen, dass Datenbearbeiter alle möglichen Interna offenlegen müssen, um sich gegen die unsubstanzierte Behauptungen zu verteidigen, sie hätten sich nicht datenschutzkonform verhalten. Die Beweislastumkehr läuft auf eine Verschuldensvermutung hinaus und wird vom sgv abgelehnt. Ebenso unterstützt der sgv eine Kausalhaftung zu Lasten des privaten Datenverarbeiters nicht.

Der Vorschlag, die Bearbeitung von Daten juristischer Personen im Rahmen ihres Geschäftszwecks als Rechtfertigungsgrund aufzunehmen, ist zu unterstützen. Nur müsste dieser Rechtfertigungsgrund auf alle Unternehmen ausgedehnt werden, also auch auf Einzelfirmen und Personengesellschaften. Damit ist auch die haftende Person miteinbezogen. Die Anbieterseite ist als Ganzes gleich zu behandeln, zumal sie selbst wählen kann in welcher Rechtsform sie am Markt auftreten will.

Massnahmen zur verbesserten Durchsetzung individueller Ansprüche

Kostenerleichterungen: Mit der Einführung der neuen Prozessordnungen auf 1.1.2011 sind in den Kantonen Kostenvorschüsse für Kläger vor Gerichten eingeführt bzw. massiv erhöht worden. Damit ist die Hürde vor allem auch für gewerbliche Kreise, vor Gericht Recht zu erhalten, erhöht worden. In gewissen Kantonen und Gerichten bewirken hohe Gebühren faktisch eine Zugangsbarriere. Vor diesem Hintergrund ist es schwer vorstellbar, für den partikulären Fall von Datenschutzverletzungen „erheblich reduzierte“ Gerichtskosten festzulegen. Dass die reduzierten Kosten nur für natürliche, nicht aber für juristische Personen gelten sollen, ist ebenfalls schwer nachvollziehbar. Auch juristi-

sche Personen im kleingewerblichen Bereich verfügen nicht über finanzielle Mittel auf Vorrat.

Sammelklagen: Der sgv hat gegenüber Sammelklagen im Bereich des Datenschutzes grosse Vorbehalte.

4.10 Autorités de contrôle

Vorgeschlagen wird, der eidgenössischen Datenschutzbehörde ein Untersuchungsrecht, vergleichbar mit demjenigen der Wettbewerbsbehörde nach Art. 26 KartG zu geben. Nach einer informellen Voruntersuchung hätte die Datenschutzbehörde die Möglichkeit, eine formelle Untersuchung zu eröffnen und auch Bussen zu verteilen. Sie würde damit eine Verfügungsbefugnis erhalten.

Der sgv vertritt die Auffassung, dass die heutigen Möglichkeiten gemäss Art. 29 DSG genügen, wonach der Datenschutzbeauftragte von sich aus oder auf Meldung Dritter einen Sachverhalt im Privatrechtsbereich abklärt, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler); Datensammlungen registriert werden müssen (Art. 11*a*) oder eine Informationspflicht nach Artikel 6 Absatz 3 DSG besteht. Der Datenschutzbeauftragte kann entsprechende Empfehlungen erlassen. Aus Sicht des sgv sind zusätzliche Gremien nicht nötig.

Finanzierung des Datenschutzes: Der Schweizerische Gewerbeverband sgv unterstützt die bisherige Alimentierung des Datenschutzbeauftragten und seiner Mitarbeitenden aus dem Bundeshaushalt. Zusätzliche Finanzierungsmittel wie z.B. eine Abgabepflicht für Betriebe lehnt der sgv ab. Auch eine Finanzierung aus Bussen ist für den sgv nicht zielführend.

Schlussbemerkungen

Die Diskussion um den Datenschutz vor dem Hintergrund neuer Technologien und Entwicklungen ist wichtig. Datenschutz darf nicht nur aus der Optik von „Social media“, „Google“, usw. betrachtet werden. Aufgrund der hohen Nutzerzahl der sozialen Medien haben sich die Datenschutzbedürfnisse stark verändert. Das „Recht auf Vergessen“ wird stipuliert und ohne weiteres auf alle Datenverarbeiter und jede Form der Datenbearbeitung ausgedehnt. Den Auswirkungen auf Gewerbe und Wirtschaft muss dabei viel mehr Beachtung geschenkt werden. Datenschutz darf nicht dazu führen, dass Schuldner ein Recht auf die Löschung ihres negativen Zahlungsverhaltens erhalten. Die kürzlich erschienene Studie von Deloitte „Economic impact assessment of the proposed European General Data Protection Regulation“ zeigt unter anderem auf, was die wirtschaftlichen Auswirkungen sind und was für Bereiche von der Novellierung der Datenschutzgrundverordnung betroffen sind.[1]

Ebenfalls mit in die Überlegungen einzubeziehen sind:

- **Direct Marketing** als grundlegende Quelle der Kommunikation zwischen den Anbietern und deren Kunden. Die Möglichkeit, bestimmte Gruppen von Kunden zielgerichtet anzusprechen, ist das Schlüsselkriterium für die Abgrenzung von anderen Formen des Marketings.
- **Online Behavioural Advertising** bezieht sich auf die Verwendung von Online-Daten um die Interessen von Usern mit den spezifischen Angeboten abzustimmen.
- **Web Analytics** hilft Anbietern dem Konsumenten mit einer besseren Qualität und relevanteren Inhalten zu versorgen.
- **Credit Information**: Bonitätsinformationen sind wichtige „Enabler“ der Wirtschaft und versorgen die sie mit den notwendigen Tools, um das Ausfallrisiko zu bestimmen. Dies hilft die Kosten für die Güter zu verringern und vereinfacht den Onlinebezug von Gütern.

---

[1] Deloitte, Economic impact assessment of the proposed European General Data Protection Regulation, 2013; Seite 6 ff.

Diese vier Bereiche sind von erheblicher wirtschaftlicher Bedeutung und müssen in die Erwägungen miteinbezogen werden. Insgesamt ist sicherzustellen, dass nicht auf Kosten der Wirtschaft vermeintlich konsumentenfreundliche Regulierungen erfolgen, die anschliessend auf die Konsumenten zurückfallen.

Dieter Kläy

Ressortleiter

Bemerkungen Normenkonzept Revision DSG

VUD | David Rosenthal, 30. September 2014

Die folgenden Kommentare beziehen sich auf das Normenkonzept und Kommentare anderer Mitglieder der Begleitgruppe. Sie stützen sich auf Inputs aus dem VUD und meine persönlichen Erfahrungen.

A. Einleitende Bemerkungen

Der Bundesrat hat dem BJ den Auftrag erteilt, eine Revision des DSG zu prüfen. Wir sind jedoch nach wie vor der Ansicht, dass in der Sache kein Bedarf an einer Revision steht. Zwar ist der Datenschutz in den Schlagzeilen wie nie zuvor, doch das hat nur damit zu tun, dass er heute verstärkt Beachtung findet und durchgesetzt wird, nicht, dass er nicht hinreichend ist.

Sämtliche Fälle, die in der Schweiz zu einer gerichtlichen Beurteilung führten oder in denen die Behörden aktiv geworden sind, haben bewiesen, dass die gesetzlichen Grundlagen genügen. Sie haben sogar aufgezeigt, dass der Datenschutz heute tendenziell zu weit geht.

Als Beispiel sei ein ganz aktueller Fall erwähnt, in welchem ein Schweizer Gericht unter dem Titel des Datenschutzes selbst die Bearbeitung von *anonymen* Daten verboten hat, und das DSG anwandte, obwohl unbestrittenermassen gar keine Personendaten vorlagen.

Das Beispiel zeigt – wie etliche andere Prozesse im Bereich des Datenschutzrechts auch – dass die betroffenen Personen keineswegs am kürzeren Hebel sind. DSG ist technologieneutral und die darin enthaltenen Grundsätze sind nach wie vor richtig. Dass der Datenschutz mit den aktuellen technologischen Entwicklungen nicht Schritt halten kann, ist zwar eine weitverbreitete, politisch attraktive Behauptung, aber letztlich durch nichts belegt.

Richtig ist, dass die Fälle, in denen die Regeln verletzt wurden oder in denen die zur Anwendung dieser Regeln nötigen Wertungen diskutiert werden, sehr viel medienträchtiger sind und mehr Personen betreffen und vor allem internationaler sind als in der Vergangenheit. Die Regeln deswegen als ineffektiv oder gar überholt zu bezeichnen, ist ein Trugschluss.

Auch die in den Arbeiten immer wieder gehörte Aussage, niemand ausser einigen Experten würden das DSG verstehen, ist aus unserer Sicht falsch. Abstrakte Regeln gehören zum Wesen des schweizerischen Rechts und sind gerade einer der Gründe, warum das DSG auch heute noch funktioniert. Wird kritisiert, dass der Normalbürger bei der Lektüre des DSG nicht wisse, was er zu tun habe, so gilt dasselbe für das ZGB und OR. Kein "Normalbürger" kennt sich heute noch z.B. mit den Regeln im Kündigungsschutz im Arbeitsbereich oder Mietrecht aus; der Blick ins Gesetz genügt schon lange nicht mehr. Man muss Experte im Arbeits- oder Mietrecht sein, um zu verstehen, was wirklich gilt.

Das ist aber kein Fehler des Rechts, sondern zeigt die Entwicklungsfähigkeit abstrakter Regeln und es belegt die Komplexität unserer Welt. Die Dinge sind eben nicht so simpel, und wer

glaubt, dies auf einfache Weise mit neuen Regeln zu lösen, schadet der Sache. Es wäre schade, wenn wir die Schweizer Rechtstradition durch die heute leider weit verbreiteten populistischen und sehr eingängigen, aber zu kurz gedachten Forderungen im Bereich des Datenschutzes über Bord zu werfen.

Übrigens ist auch das heutige Instrument von Art. 29 DSG, dass dem EDÖB ein umfassendes Klagerecht gibt, vollauf genügend und sehr effizient ist. Es ist klar, dass dies eine politisch nicht opportune Aussage ist, da alles nach "Stärkung" des Datenschutzes schreit und ein EDÖB, der lediglich "Empfehlungen" aussprechen statt verfügen kann, als zahnlos erscheinen mag (auch wenn dies in der Praxis seinem Klagerecht in keiner Weise gerecht wird; er kann heute faktisch genauso Druck ausüben wie wenn er selbst Anordnungen treffen könnte, wie zahlreiche Beispiele zeigen). Dass der EDÖB selbst Verfügungskompetenz möchte, ist vor diesem Hintergrund zwar nachvollziehbar, aber nicht zielführend und notwendig.

Aber bei Lichte betrachtet ist das einzige Problem, das der Durchsetzung des DSG durch den EDÖB im Wege steht, der Mangel an Ressourcen des EDÖB. Dieses Problem werden die vorgeschlagenen Anpassungen nicht lindern, sondern verschärfen. Sie mögen politisch unvermeidlich sein, aber die Schweiz wird dem Datenschutz (und der Wirtschaft, die die Kosten zu tragen hat) damit keinen Gefallen erweisen; die Anwälte und Berater werden sich hingegen freuen. Sie haben es schon im Bereich des Kartellrechts getan, aber die Kosten der Datenschutzaufsicht werden explodieren oder, falls die Ressourcen nicht zur Verfügung gestellt werden, in den eigenen Verfahrensbestimmungen stecken bleiben.

Es ist klar, dass die Schweiz im Falle einer Verabschiedung der revidierten Europaratskonvention 108 deren Regelungen irgendwie übernehmen muss. Sie sollte dabei jedoch nicht einfach etwas weltfremde Regelungen (wie z.B. bei den automatisierten Einzelfallentscheidungen oder der Transparenz, welche zu einer Inflation an "Hinweisen" führen wird, die am Ende nicht mehr Transparenz verschaffen werden, als es die kleingedruckten Geschäftsbedingungen von iTunes schon tun) mit dem Argument übernehmen, man müsse das eben tun. Die Schweiz hat in solchen Fällen einen erheblichen Spielraum bei der Umsetzung und sollte ihn mit Augenmass nutzen, auch wenn zu wünschen gewesen wäre, dass die Revision der Konvention von einem etwas ausgeglichenerem Gremium ausgearbeitet worden wäre.

B. Einige konkrete Bemerkungen

1. Best Practice

Die Best Practice-Regeln werden nur dann ihren Zweck erfüllen, wenn sie den Datenbearbeitern Rechtssicherheit geben. Der VUD regt an, ausdrücklich auf die Regelung in Österreich zu verweisen, wo es "genehmigte" Good-Practice-Regelungen schon gibt. Hier findet sich ein Beispiel:

https://www.wko.at/Content.Node/branchen/sbg/BankVersicherung/Banken-und-Bankiers/Verhaltensregeln-fuer-Gluecksspielbetreiber-1.html

2. Begriffsdefinitionen

Es ist nicht sinnvoll, Begriffe wie das "Territorialitätsprinzip", die durch die Rechtssprechung vor dem Hintergrund der laufenden gesellschaftlichen Entwicklung ständig weiterentwickelt werden, festzuschreiben und damit einer Weiterentwicklung zu entziehen. Damit wird genau jener Fehler begangen, von dem man glaubt, ihn mit der jetzigen Revision beheben zu müssen, nämlich dass das DSG von der technologischen und gesellschaftlichen Entwicklung überholt wird. Dies ist nicht der Fall, doch gewisse der ins Auge gefassten Anpassungen werden das DSG so sehr auf ganz bestimmte Praxisanwendungen konkretisieren, dass das DSG nicht mehr "passen" wird, wenn sich die Fragestellungen, Wertvorstellungen oder andere Aspekte auch schon nur leicht ändern. Das DSG ist zwar schon viele Jahre alt, aber der Umstand, dass es so allgemeingültig formuliert ist, macht es auch sehr flexibel. Der Fall Google Street View hat bewiesen, dass sich das DSG bestens auch im Zeitalter der internationalen Internetdienste anwenden lässt.

Beim Umgang mit Personendaten sind grundsätzlich folgende Funktionen zu unterscheiden: (A) die natürliche oder juristische Person, welche für die Bearbeitung von Daten in irgend einer Form zuständig und verantwortlich ist: “controller“ im Sinne von Art. 2.d RL 95/46/EG; (B) der “Inhaber einer Datensammlung“ im Sinne von Art. 3 Bst. i DSG; (C) der “Auftragsdatenbearbeiter“ (“processor“ im Sinne von Art. 2.e RL 95/46/EG), d.h. jener Dritte im Sinne von Art. 10a DSG, welcher Daten im Auftrag eines Auftraggebers bearbeitet. Bisher fehlt im schweizerischen Datenschutzrecht eine Definition welche in Abgrenzung zum “Inhaber der Datensammlung“ nach Art. 3 Bst. i DSG und Art. 2 d) der Europaratskonvention ETS Nr. 108 “controller of the file“ die für eine Bearbeitung von Personendaten verantwortliche Person oder Stelle definiert. Wir betrachten die beiden Begriffe “Inhaber der Datensammlung“ sowie “bearbeitende Stelle“ keineswegs als gleichwertig, wie u.E. zu Unrecht im Normkonzept angenommen wird, sondern als auf erheblich verschiedene Tatbestände bezogene Begriffe bzw. Funktionen. Auch wenn im europäischen Ausland die verschiedenen Begriffe zum Teil durchmischt werden, erachten wir es als sinnvoll, hier weiterhin klar zwischen den verschiedenen Funktionen zu trennen.

Nach geltendem schweizerischen Recht werden die “Persönlichkeitsprofile“ gemäss Art. 3 Bst. d DSG durchgehend den gleichen Anforderungen unterstellt wie die “besonders schützenswerten Personendaten“ nach Art. 3 Bst. c DSG. Nun soll die für das schweizerische Datenschutzrecht von 1992 originelle und weit in die Zukunft greifende Definition des “Persönlichkeitsprofils“ gestrichen und durch spezielle Regelungen zum “Profiling“ ersetzt werden. Es stellte sich bei uns bei nochmaliger Betrachtung die Frage, wieviel damit gewonnen würde. Denn auch bei den Bestimmungen über das “Profiling“ wird man um eine entsprechende, wegen der Tragweite der Bestimmung heikle Definition der “Persönlichkeitsprofile“ nicht herumkommen.

3. Informationspflicht

Es ist sinnvoll, die heute in Art. 14 und 18a/b DSG zusätzlich vorgesehene Informationspflicht zugunsten eines allgemeinen Grundsatzes der Transparenz aufzuheben. Es muss jedoch darauf geachtet werden, dass die selbständige Informationspflicht nicht zu einem übermässigen bürokratischen Aufwand führt wie bei den heute in der Praxis kaum sinnvoll umsetzbaren Art.

14 und 18-18b DSG. Eine Pflicht zur Information der betroffenen Personen über jede der heute allgegenwärtigen, aber auch alltäglichen Datenerfassungen und -bearbeitungen bei jeder Art elektronischer Kommunikation geht schlicht zu weit, Europarat hin oder her. Hier ist im Normenkonzept nochmals zu betonen, dass eine vernünftige, sachgerechte und zurückhaltende Umsetzung anzustreben ist, die nicht zu einer Inflation der Information führt, die gar nichts bringt, ja sogar kontraproduktiv ist.

4. Auskunftsrecht

Der Zugang externer Personen zu firmeninternen Unterlagen muss restriktiv gehandhabt werden, schon aus Gründen der Datensicherheit. Es besteht heute schon eine Tendenz der Gerichte, externen Personen durch ausufernde Auskunftsansprüche Zugang zu allen möglichen internen Unterlagen von Unternehmen zu geben, selbst wenn es überhaupt nicht um den Datenschutz geht; das Auskunftsrecht wird immer häufiger missbraucht, um Beweismittel für datenschutzfremde Zwecke zu sammeln, Unternehmen zu schikanieren und auszuforschen. Ein Ausbau der Zugangsrechte, wie teilweise auch hier gefordert, ist nicht angezeigt.

Bezüglich der heutigen Regelung ist es zwingend, dass im Falle eines strittigen Auskunftsgesuchs, die Interessenabwägung immer auch die Interessen des Inhabers der Datensammlung berücksichtigt werden. Es gibt keinen sachlogischen Grund, warum seine Interessen per se nicht beachtlich sind, wenn er die Daten, um die es geht, bereits an Dritte weitergegeben hat (wozu z.B. ein konzerninterner Datenverkehr schon genügen kann). Genau dies sieht Art. 9 Abs. 4 DSG heute aber vor. Der bestehende Zusatz "und er die Personendaten nicht Dritten bekannt gibt" ist in dieser Bestimmung daher ersatzlos zu streichen. Es gibt keinen Grund zur Befürchtung, dass die Gerichte, welche die Interessenabwägung letztendlich vornehmen müssen, dies nicht sachgerecht tun werden. Heute wird ihnen aber in den erwähnten Fällen die Vornahme einer Interessenabwägung untersagt.

Es wurde im Kreise des VUD noch angeregt, beim Auskunftsrecht vorzusehen, dass die betroffene Person dann, wenn sie Auskunft über Sicherungs- und Archivdaten sucht, ein rechtlich geschütztes Interesse glaubhaft zu machen hat; hier also höhere Anforderungen gelten sollen (vgl. dazu § 19(1) und (2) sowie §§ 33(2) Ziff. 2 und 34 (7) BDSG). Das rechtfertigt sich umso mehr, als Unternehmen immer stärker durch den Gesetzgeber zur Aufbewahrung von Daten verpflichtet werden. Als sinnvoll erachtet wird auch, eine Mitwirkungspflicht der betroffenen Person zum Auffinden der Daten zu statuieren.

5. Zustimmung

Die geltende Regelung betreffend Zustimmung soll beibehalten werden. Die im Europarat und in der EU teilweise diskutierten Anpassungen rühren von einem dort – anders als in der Schweiz – praktizierten Verständnis des Begriffs der Einwilligung her. In der Schweiz sind die Anforderungen an eine Einwilligung schon relativ hoch. Der Unterschied z.B. zwischen einer "klaren" und "nicht klaren" Einwilligung ist dem Schweizer Recht wesensfremd; entweder liegt eine Einwilligung vor oder aber eben nicht. Wir möchten zudem ausdrücklich davor warnen, von einer fehlenden Einwilligung auszugehen, wenn eine betroffenen Person sich über die Datenbearbeitung nicht erkundigt, welche die von der bearbeitenden Stellen zugänglich gemachten

Angaben über die Bearbeitung der Daten nicht gelesen oder diese nicht verstanden hat, und unüberlegt das “Gelesen und Verstanden-Häklein“ unter ein Angebot im Web gesetzt hat. Voraussetzung für eine gültige Einwilligung ist natürlich eine “angemessene vorangehende Information“ im Sinne von Art. 4 Abs. 5 DSG. Es kann diesbezüglich auf die Gerichtspraxis zu “ungelesenen oder nicht verstandenen AGB“ unter Vorbehalt der Ungültigkeit von ungewöhnlichen, einseitigen, irreführenden AGB verwiesen werden: Zusammengefasst in BGE 109 II 213. Es gibt auch hier keinen Grund, dies im Datenschutz anders als im ganzen Rest des Schweizer Rechts zu regeln.

6. Widerspruchsrecht

Das Widerspruchsrecht ist nicht auszubauen, weil es heute schon besteht und nicht erwiesen ist, warum es nicht genügen soll. Im Gegenteil: hat das Google-Urteil des EuGH jüngst gerade wieder belegt, wie streng das heutige Datenschutzrecht sein kann, wenn es tatsächlich genutzt wird. Das Urteil zeigt aber auch die Schattenseiten auf (Zensurdiskussion). Das Datenschutzrecht sollte zudem wertungsfrei bleiben und nicht dafür benutzt werden, die Weiterentwicklung unserer Wertordnung aufzuhalten, bloss weil man sie für heikel hält. Die Profilbildung wird in unserer Gesellschaft immer wichtiger, weil es je längers je mehr Möglichkeiten gibt, solche zu bilden; sie hat aber wie alles ihre guten und schlechten Seiten. Profile können etwa auch dazu dienen, Entscheide vorhersehbarer, transparenter zu machen. Und Unternehmen können durch Profile missbräuchliche Verhaltensweisen immer besser erkennen. Die Profilbildung zu verteufeln, ist nicht sachgerecht. Es kann daher nicht Sache des Datenschutzrechts sein, der Profilbildung durch ein spezifisches Widerspruchsrecht pauschal einen Riegel schieben zu wollen.

7. Datenportabilität

Das Recht auf Datenportabilität hat im Datenschutzrecht nichts zu suchen. Es geht dabei nur um die Regulierung der Marktzugangs zu sozialen Netzwerken. Das ist eine typische "Denkzettel"-Regel einiger EU-Politiker und Datenschützer, denen Facebook ein Dorn im Auge ist, deren Auswirkung aber niemand versteht und deren Kosten schon gar nicht. Wir sollten nicht den Fehler machen, solche Dinge in unser Recht zu übernehmen; dies ist überdies ein massiver Eingriff in die Wirtschaftsfreiheit. Falls sich die Datenportabilität auf EU-Ebene tatsächlich durchsetzen sollte, würden die Schweizer Kunden bei solchen Diensten ohnehin automatisch mitprofitieren.

8. Ausländische Gerichts- und Behördenverfahren als Rechtfertigungsgrund für Exporte

Die geforderte Ausdehnung des Rechtfertigungsgrunds bei Datenexporten von Gerichten auf Behörden ist sachgerecht. Ein Unternehmen darf heute Unterlagen liefern, wenn es im Ausland angeklagt worden ist oder selbst gegen jemanden klagt, und sei es wegen einer belanglosen Sache (Art. 6 Abs. 2 Bst. d DSG). Es darf aber keine Unterlagen liefern, wenn dies im Rahmen eines vorgerichtlichen, aber ebenso regulierten Behördenverfahrens erforderlich ist, zum Beispiel die eigene Unschuld zu beweisen. Diese Unterscheidung ist nicht nachvollziehbar. Ein Unternehmen wird heute dadurch gezwungen, entweder das DSG zu verletzen oder bei einer Behördenuntersuchung die Kooperation zu verweigern und es zu einer Anklage vor Gericht – mit potenziell katastrophalen Folgen für alle Beteiligten – kommen zu lassen, da erst dann nach

DSG geliefert werden darf. Das macht keinen Sinn. Die Regelung ist daher auf Behördenverfahren auszudehnen.

9. Zertifizierungspflicht

Die Zertifizierungspflicht im Bereich der Krankenversicherung ist letztlich ein Kompromiss im Streit um die Einführung der Fallpauschalen; sie kann und sollte keineswegs als Vorbild für weitere Zertifizierungspflichten für andere Bereiche dienen. Die Zertifizierungen und damit verbundenen Aufwände kosteten den Prämienzahler bereits Millionen, ohne, dass sie wirklich einen Zusatznutzen bringen. Eine Zertifizierung belegt einzig, dass ein Datenschutzmanagementsystem existiert, also entsprechende Prozesse und Dokumentationen vorhanden sind, es belegt aber in keiner Weise, ob der Datenschutz wirklich eingehalten wird. Datenschutzverstösse verhindert auch ein DSMS nicht. Es gibt einen guten Grund, warum sich Unternehmen nicht für Zertifizierungen nach Art. 11 DSG interessieren. Solange sie freiwillig sind, schaden sie nichts. Wird die Zertifizierungspflicht aber ausgedehnt, dient dies vor allem der Zertifizierungsbranche. Soll in gewissen Branchen der Datenschutz verstärkt werden, sind Kontrollen und Untersuchungen, wie sie bisher praktiziert wurden, wesentlich wirksamer und nachhaltiger.

10. Rechtfertigungsmöglichkeit auch bei Verletzung der Datenschutzgrundsätze

Es wurde angeregt, dass Art. 12 Abs. 2 Bst. a DSG entgegen dem Vorschlag im Normenkonzept so belassen wird, wie er heute im Gesetz ist. Dies ist abzulehnen. Der EDÖB hatte dies im Fall Logistep so vertreten, aber das Bundesgericht hat festgestellt, dass es sich um ein Versehen handelte (wie in der Lehre mit Verweis auf die Sitzungsprotokolle nachgewiesen wurde; das Parlament ging damals von einer falschen Annahme aus). Es hielt fest, dass auch Verletzungen der Bearbeitungsgrundsätze gerechtfertigt werden können. Dies entspricht auch einem Grundprinzip des Persönlichkeitsschutzrechts entspricht. Der Fall, in welchem der Entscheid zustande kam, war jedoch ein sehr schlechter Fall und das Bundesgericht wurde für seine Interessenabwägung zugunsten des Datenschutzes massiv kritisiert. Aus der Not gebar es die Formel, dass eine Rechtfertigung eben nur mit grosser Zurückhaltung zulässig sei. Diese Formel wird inzwischen vom EDÖB und auch den Gerichten gebetsmühlenmässig wiederholt wird. Das Bundesgericht hält sich selbst allerdings nicht (mehr) daran, sondern praktiziert die Interessenabwägung so, wie eine Interessenabwägung überall im Schweizer Recht vorzunehmen ist: Durch schlichtes Abwägen aller auf dem Spiel stehenden Interessen. So gilt es heute auch. Bereits im Fall Google Street View wurde die Interessenabwägung wieder wie vor der letzten Revision durchgeführt. Die Sache sollte im Normenkonzept korrekterweise ausdrücklich beim Namen genannt werden, nämlich dass es sich bei der heutigen Formulierung um ein Versehen handelte. Das gesetzgeberische Versehen sollte definitiv korrigiert werden.

11. Verfügungskompetenz des EDÖB, kollektive Klageinstrumente

Wie eingangs erwähnt ist es wenig sinnvoll, den EDÖB durch Verfügungskompetenzen verfahrensmässig unnötig zu belasten. Er wird mehr Ressourcen benötigen, und die wenigen zusätzlichen Ressourcen, die er erhalten wird, werden für die Wahrung der nötigen Verfahrensvorschriften und -garantien verbraucht werden. Damit ist dem Datenschutz nicht gedient, und inzwischen scheint diese Erkenntnis verschiedenenorts zu reifen.

Wenn nun stattdessen auf Instrumente wie Verbands- oder Sammelklagen ausgewichen werden soll, wird dies den Datenschutz zusätzlich schwächen. Die Datenschutzverbandsklage gibt es seit Jahren und sie ist toter Buchstabe. Die Sammelklage wird in Datenschutzbelangen ebenfalls toter Buchstabe (was die Stärkung des Datenschutzes betrifft) bleiben, birgt aber einiges an Missbrauchspotenzial. Der Datenschutz eignet sich schlicht nicht für Sammelklagen. Und dort, wo es darum geht, gegen eine bestimmte Art der Datenbearbeitung einer bestimmten Person an sich vorzugehen, haben wir bereits das Verfahren nach Art. 29 DSG, das ausgezeichnet funktioniert und erprobt ist. Es ist zugleich das volkswirtschaftlich günstigste Instrument.

Google Street View oder Moneyhouse sind Paradebeispiele, dass das Verfahren nach Art. 29 DSG, in welchem der EDÖB quasi stellvertretend für die betroffenen Personen gegen eine Datenbearbeitung in grundsätzlicher Art und Weise vorgeht, funktioniert und zielführend ist. Kein Verein hätte eine solche Klage gegen Google Street View oder Moneyhouse geführt, eine Sammelklage wäre nie in Frage gekommen. Soll der EDÖB allerdings Verfügungskompetenz erhalten, wird er zwangsläufig wesentlich weniger frei in der Wahl seiner Fälle sein. Auch das ist ein Grund, am bisherigen System festzuhalten.

12. Prozessuale Instrumente

Die Beweislastumkehr läuft, wie entsprechende Kommentatoren festgestellt haben, auf eine Vermutung der "Schuld" hinaus. Hier möchten wir nochmals zu bedenken geben, dass eine Beweislastumkehr in der Praxis unnötig ist. Der Schutz des Einzelnen scheitert in Datenschutzfällen nie am Problem der Beweislast, und es gibt auch keinerlei Belege für solche Fälle. In Tat und Wahrheit sieht das Schweizer Zivilprozessrecht schon heute weitgehende Mitwirkungspflichten seitens einer beklagten Person vor.

Es sei an dieser Stelle – wie schon in der Redaktionsgruppe – betont, dass es keinen Sinn macht, aus reiner Symbolik Dinge, die im Schweizer Zivilprozessrecht ausgiebig, gerecht und sachgerecht geregelt sind, für das Datenschutzrecht nochmals und zudem anders zu regeln. Es gibt keinen Grund, den Datenschutz anders zu behandeln. Auch für eine Kausalhaftung gibt es keinen Anlass. Sie belastet lediglich die Unternehmen, die solche Risiken in ihrer Kalkulation finanziell unterlegen und letztlich auf die Konsumenten überwälzen müssen, ohne, dass ihnen dies jedoch wirklich zu Gute kommt.

Die vorgeschlagenen Kostenerleichterungen braucht es in der Praxis nicht. Sie belasten nur die Staatskasse, werden aber den Rechtsschutz von Privatpersonen nicht stärken. Wenn überhaupt Kosten ein Hinderungsgrund für die Rechtsdurchsetzung sind, dann nicht die Gerichtskosten, sondern die Kosten für die anwaltliche Vertretung und die Pflicht, die gegnerischen Kosten im Falle eines Unterliegens tragen zu müssen.

Wenn aber aus politischen bzw. symbolischen Gründen eine Kostenerleichterung vorgesehen werden sollte, so hat sie für alle Verfahren von Konsumenten zu gelten, die dieselben Themenkomplexe betreffen, so namentlich UWG, DSG und ZGB 28. Andernfalls könnten die betreffenden Ansprüche aus prozessualen Gründen nicht mehr zusammen geltend gemacht werden, wie dies in der Praxis regelmässig geschieht; den betroffenen Personen wäre ein Bärendienst er-

wiesen. Im Grunde sollte es also gar keine Kostenerleichterung geben, und wenn doch, dann höchstens eine, die einer Klagehäufung nicht im Wege steht.

Der Hinweis, dass der Rechtfertigungsgrund von Daten juristischer Personen im Rahmen ihres Geschäftszwecks bzw. ihrer Geschäftstätigkeit auch auf Personengesellschaften und Einzelfirmen auszuweiten ist, erscheint an sich berechtigt; allerdings muss dies einhergehen mit der Definition des Begriffs der Personendaten (d.h. wenn im Rechtfertigungsgrund auch Einzelfirmen berücksichtigt werden, dann sollte auch der Begriff des Personendatums Daten von Einzelfirmen umfassen, was nicht der Fall ist, da sich sonst das Problem gar nicht stellt, weil deren Daten nicht vom DSG erfasst sind).

C. Abschliessende Bemerkung

Die Bemerkungen sind aufgrund sprachlicher Hindernisse (französische Teile des Normenkonzepts) nicht als abschliessende Stellungnahme bzw. Zustimmung zu allen anderen Teilen des Normenkonzepts zu verstehen.