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

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.

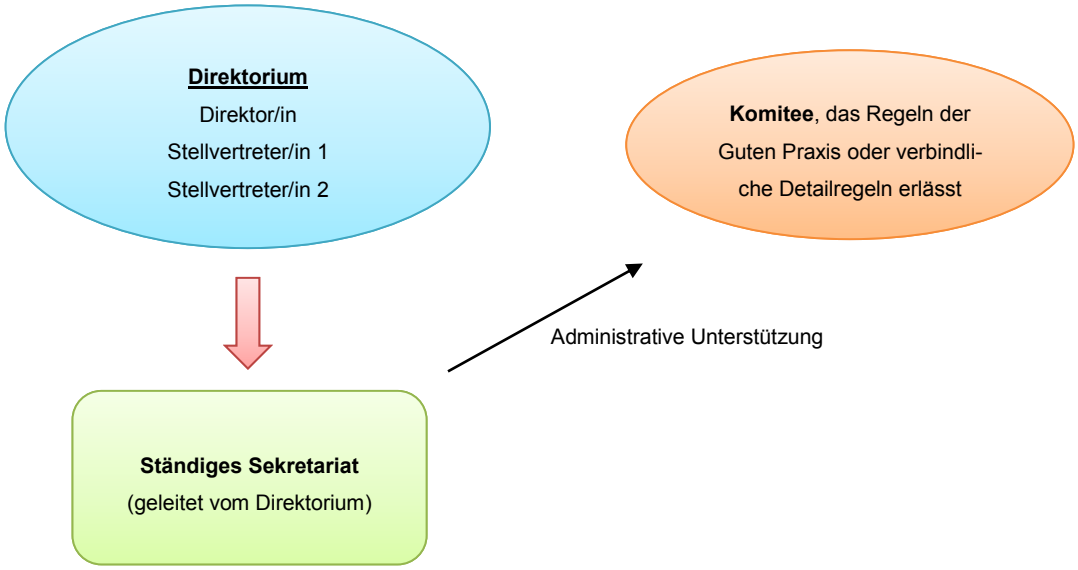
Die Aufgaben und Kompetenzen der Aufsichtsbehörde im Bereich des Datenschutzes und im Bereich des Öffentlichkeitsprinzips werden sich künftig womöglich noch stärker unterscheiden (Aufsicht mit Verfügungsbefugnis [DSG] gegenüber Schlichtungsbefugnis [Art. 13 ff. BGÖ]). Um nicht der bereits heute teilweise 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

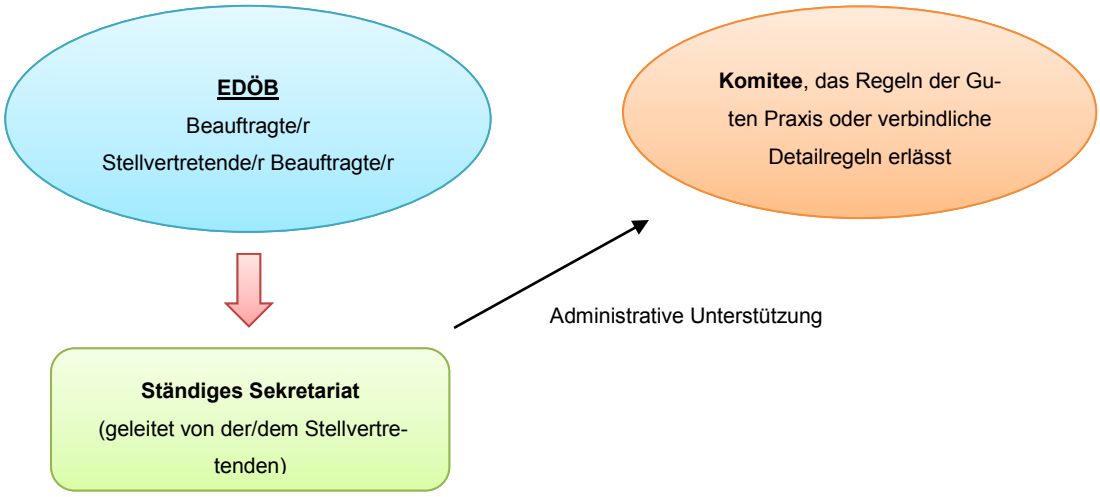
Wie bereits erwähnt, lehnt es eine *Minderheit der Begleitgruppe* ab, ein spezialisiertes Komitee einzusetzen, welches Regeln der Guten Praxis bzw. verbindliche Detailregeln zuhanden der Datenbearbeitenden erlässt oder genehmigt (siehe Ziff. 4.1.2 lit. b und Ziff. 4.10.2 lit. c). Diese Minderheit stellt 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»).

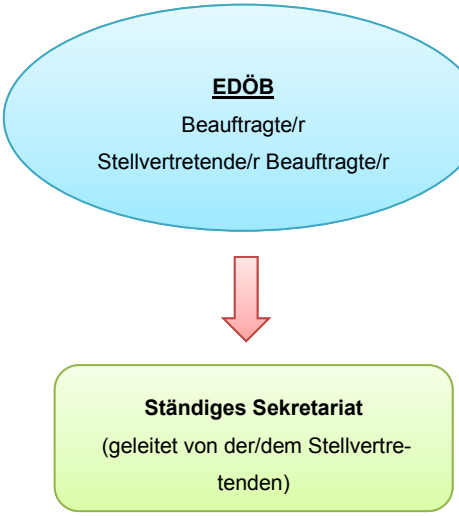
Um die Unabhängigkeit der Aufsichtsbehörde zu stärken, wird vorgeschlagen, dass die/der stellvertretende Beauftragte ebenso wie die/der Beauftragte vom Bundesrat gewählt wird, wobei die Wahl durch die Bundesversammlung zu genehmigen ist.

[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.

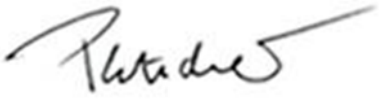
<u>Anpassung an internationale Bestrebungen (EU/Europarat) nur sofern für Marktzugang zwingend</u>

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.