Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

17.059

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz

vom 15. September 2017

Sehr geehrter Herr Nationalratspräsident
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf des Bundesgesetzes über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz sowie den Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.

Gleichzeitig beantragen wir Ihnen, die folgenden parlamentarischen Vorstösse abzuschreiben:

- Postulat Hodgers 10.3383 «Anpassung des Datenschutzgesetzes an die neuen Technologien»;
- Postulat Graber 10.3651 «Angriff auf die Privatsphäre und indirekte Bedrohungen der persönlichen Freiheit»;
- Postulat Schwaab 12.3152 «Recht auf Vergessen im Internet»;
- Postulat Recordon 13.3989 «Verletzungen der Persönlichkeitsrechte im Zuge des Fortschritts der Informations- und Kommunikationstechnik»;
- Motion Comte 14.3288 «Identitätsmissbrauch. Eine strafbare Handlung für sich»;
- Postulat Derder 14.3655 «Die digitale Identität definieren und Lösungen für ihren Schutz finden»;
- Postulat Schwaab 14.3739 «Control by Design. Die Rechte auf Eigentum im Falle von unerwünschten Verbindungen verstärken»;

– Postulat FDP-Liberale Fraktion 14.4137 «Videoaufnahmen durch Private. Die Privatsphäre besser schützen»;
– Postulat Comte 14.4284 «Videoaufnahmen durch Private. Die Privatsphäre besser schützen»;
– Postulat Béglé 16.3383 «Elektronische Daten. Information der Geschädigten im Falle eines Hackerangriffs»;
– Postulat Béglé 16.3384 «Elektronische medizinische Daten. Eine geschützte, transparente und zielgerichtete Datenerhebung im revidierten Bundesgesetz über den Datenschutz sicherstellen».

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

15. September 2017

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Doris Leuthard
Der Bundeskanzler: Walter Thurnherr

Übersicht

Der vorliegende Gesetzesentwurf hat zum Ziel, den Datenschutz zu stärken, indem die Transparenz der Bearbeitung von Daten und die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten verbessert werden. Zugleich soll das Verantwortungsbewusstsein der für die Bearbeitung Verantwortlichen erhöht werden, beispielsweise indem sie dazu verpflichtet werden, bereits bei der Planung neuer Datenbearbeitungen die Einhaltung der Datenschutzvorschriften zu berücksichtigen. Auch die Aufsicht über die Anwendung und die Einhaltung der eidgenössischen Datenschutznormen soll verbessert werden. Schliesslich soll die Wettbewerbsfähigkeit der Schweiz aufrechterhalten und verbessert werden, namentlich indem die Bekanntgabe von Daten ins Ausland erleichtert und die Entwicklung neuer Wirtschaftszweige im Bereich der Digitalisierung der Gesellschaft gefördert wird, und zwar auf der Basis eines hohen, international anerkannten Schutzstandards.

Ausgangslage und Ziele der Vorlage

Mit dem vorliegenden Gesetzesentwurf sollen hauptsächlich zwei Zielsetzungen verwirklicht werden: Einerseits sollen die Schwächen des Datenschutzgesetzes behoben werden, die aufgrund der rasanten technologischen Entwicklung entstanden sind. Andererseits soll die Revision den Entwicklungen auf der Ebene des Europarats und der Europäischen Union Rechnung tragen. Der Vorentwurf war vom 21. Dezember 2016 bis am 4. April 2017 in der Vernehmlassung.

Die Europäische Union hat am 27. April 2016 ihre Datenschutzgesetzgebung revidiert. Diese umfasst zwei Rechtsakte, zum einen die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum anderen die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts. Nur die Richtlinie ist Teil des Schengen-Acquis. Der Europarat wiederum sieht ein Protokoll zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vor, das vom Ministerkomitee noch verabschiedet werden muss.

Die Vorlage soll sicherstellen, dass die Gesetzgebung auf Bundesebene mit dem revidierten Übereinkommen SEV 108 vereinbar ist, damit die Schweiz das revidierte Übereinkommen so rasch als möglich unterzeichnen kann. Darüber hinaus soll sie die Anforderungen der Richtlinie (EU) 2016/680 übernehmen, damit die Schweiz ihren Schengen-Verpflichtungen nachkommen kann. Sie setzt auch die Empfehlungen um, welche die Europäische Union im Rahmen der Schengen-Evaluation betreffend die Schweiz abgegeben hat. Dabei wurde insbesondere empfohlen, die Kompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) auszubauen. Schliesslich soll die Vorlage die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Aus Sicht des Bundesrates bildet diese Annäherung zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbe-

schluss weiterhin bestätigt, dass das schweizerische Datenschutzniveau angemessen ist. Dieser Angemessenheits-beschluss ist insbesondere für die Schweizer Wirtschaft von zentraler Bedeutung.

Die Verabschiedung der Botschaft zur Vorlage ist in den Zielen des Bundesrates für das Jahr 2017 und in der Legislaturplanung 2015–2019 enthalten. Die Revision des Datenschutzes war in den vergangenen Jahren auch Gegenstand zahlreicher parlamentarischer Vorstösse. Dies verdeutlicht, dass der politische Wille besteht, die Bundesgesetzgebung in diesem Bereich zu stärken.

Inhalt der Vorlage

Die Vorlage umfasst in erster Linie die Totalrevision des Bundesgesetzes über den Datenschutz.

Im Einklang mit den europäischen Normen und der Mehrheit der ausländischen Rechtsordnungen wird im Datenschutzgesetz auf den Schutz der Daten juristischer Personen verzichtet und der Geltungsbereich des Gesetzes entsprechend angepasst. Dies erleichtert auch die Bekanntgabe von Daten ins Ausland.

Generell wird die Transparenz der Bearbeitung verbessert. Die Informationspflicht bei der Datenbeschaffung gilt nunmehr für alle Bearbeitungen durch private Verantwortliche, aber es sind einzelne Ausnahmen vorgesehen. Die Information kann in einfacher, standardisierter Weise erfolgen. Darüber hinaus muss die betroffene Person spezifisch über Entscheidungen informiert werden, die auf einer rein automatisierten Datenbearbeitung beruhen. Auch muss sie unter bestimmten Voraussetzungen die Gelegenheit erhalten, ihren Standpunkt darzulegen und zu verlangen, dass die Entscheidung von einer natürlichen Person überprüft wird. Erweitert werden auch die Informationen, die der betroffenen Person mitzuteilen sind, wenn sie ihr Auskunftsrecht geltend macht.

Die Revision soll die Selbstregulierung bei den Verantwortlichen fördern. Dies erfolgt über Verhaltenskodizes, welche die Tätigkeit der Verantwortlichen erleichtern und die Einhaltung des Gesetzes verbessern sollen. Diese Kodizes werden von den Branchen erarbeitet und können dem Beauftragten vorgelegt werden.

Die Unabhängigkeit und die Position des Beauftragten werden gestärkt. In der Revision ist vorgesehen, dass dieser, analog zu seinen europäischen Amtskollegen, von Amtes wegen oder auf Anzeige hin eine Untersuchung gegenüber den Verantwortlichen und Auftragsbearbeitern eröffnen und beim Abschluss der Untersuchung eine Verfügung erlassen kann.

Schliesslich werden auch die Strafbestimmungen des Gesetzes in verschiedener Hinsicht verschärft. Dies erfolgt insbesondere, weil der Beauftragte, anders als seine europäischen Amtskollegen, keine Verwaltungssanktionen auferlegen darf.

Neben der Totalrevision des Datenschutzgesetzes umfasst die Vorlage eine Teilrevision weiterer Bundesgesetze. Damit sollen namentlich die Anforderungen der Richtlinie (EU) 2016/680 umgesetzt werden. Betroffen sind insbesondere das Strafgesetzbuch, die Strafprozessordnung und das Rechtshilfegesetz sowie das Schengen-Informationsaustauschgesetz.

Inhaltsverzeichnis

Botschaft

1 Grundzüge der Vorlage

1.1 Ausgangslage auf nationaler Ebene

1.1.1 Geltendes Recht

Auf Bundesebene ist der Datenschutz gegenwärtig primär im Bundesgesetz vom 19. Juni 1992[1] über den Datenschutz (DSG) geregelt, das am 1. Juli 1993 in Kraft getreten ist.

Das DSG regelt die Bearbeitung von Daten natürlicher und juristischer Personen durch private Personen und durch Bundesorgane (Art. 2 Abs. 1). Nicht anwendbar ist es indessen auf Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt (Abs. 2 Bst. a), auf Beratungen in den eidgenössischen Räten und parlamentarischen Kommissionen (Abs. 2 Bst. b), auf hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren (Abs. 2 Bst. c), auf öffentliche Register des Privatrechtsverkehrs (Abs. 2 Bst. d) und schliesslich auf Personendaten, die das Internationale Komitee vom Roten Kreuz (IKRK) bearbeitet (Abs. 2 Bst. e).

Das DSG enthält Grundsätze, die beim Bearbeiten von Daten zu befolgen sind. So schreibt es vor, dass Personendaten nur rechtmässig bearbeitet werden dürfen (Art. 4 Abs. 1) und dass ihre Bearbeitung nach Treu und Glauben zu erfolgen hat sowie verhältnismässig sein muss (Art. 4 Abs. 2). Ebenfalls dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, gesetzlich vorgesehen oder aus den Umständen ersichtlich ist (Art. 4 Abs. 3). Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein (Art. 4 Abs. 4). Artikel 4 Absatz 5 regelt die Voraussetzungen für die Einwilligung der betroffenen Person. Privatpersonen oder Bundesorgane, die Personendaten bearbeiten, haben sich zudem über deren Richtigkeit zu vergewissern (Art. 5).

Das DSG enthält sodann Vorschriften über die Bekanntgabe von Personendaten ins Ausland (Art. 6) und das Auskunftsrecht (Art. 8–10). In Artikel 10*a* ist die Bearbeitung von Daten durch Dritte geregelt. Gemäss Artikel 11*a* ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (Beauftragter) verpflichtet, ein der Öffentlichkeit zugängliches Online-Verzeichnis der Datensammlungen zu führen. Von einigen Ausnahmen abgesehen, müssen die Inhaber von Datensammlungen diese melden.

Der dritte Abschnitt des DSG enthält spezifische Normen für die Datenbearbeitung durch Private. So dürfen private Personen, die Personendaten bearbeiten, die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen (Art. 12 Abs. 1). Insbesondere dürfen sie ohne Rechtfertigungsgrund keine Personendaten gegen den

[1] SR **235.1**

ausdrücklichen Willen der betroffenen Person bearbeiten (Art. 12 Abs. 2 Bst. b und Art. 13). Nach Artikel 14 sind private Personen unter Vorbehalt von Ausnahmen verpflichtet, die betroffene Person über die Beschaffung von besonders schützenswerten Daten oder Persönlichkeitsprofilen zu informieren. Schliesslich regelt dieser Abschnitt auch die zivilrechtlichen Ansprüche, die Geschädigte geltend machen können, und das entsprechende Verfahren (Art. 15).

In den Artikeln 16–25 DSG ist die Bearbeitung von Personendaten durch Bundesorgane geregelt. Organe des Bundes dürfen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Art. 17 Abs. 1). Für die Bearbeitung besonders schützenswerter Daten oder von Persönlichkeitsprofilen ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich (Art. 17 Abs. 2). Gemäss Artikel 18*a* sind Bundesorgane verpflichtet, die betroffene Person über die Beschaffung von Personendaten zu informieren; vorbehalten sind einige Ausnahmen (Art. 18*b*). Grundsätzlich dürfen Bundesorgane Personendaten nur dann an Dritte bekannt geben, wenn dafür eine Rechtsgrundlage besteht (Art. 19 Abs. 1). Auch dürfen Personendaten nur dann durch ein Abrufverfahren zugänglich gemacht werden, wenn dies ausdrücklich im Gesetz vorgesehen ist (Art. 19 Abs. 3). Für besonders schützenswerte Daten oder Persönlichkeitsprofile gelten noch strengere Anforderungen: Sie dürfen nur dann durch ein Abrufverfahren zugänglich gemacht werden, wenn ein Gesetz im formellen Sinn dies explizit vorsieht (Art. 19 Abs. 3). Artikel 25 regelt schliesslich die Rechtsansprüche, die betroffene Personen gegenüber einem für die Bearbeitung von Personendaten verantwortlichen Bundesorgan geltend machen können.

In den Artikeln 26 und 26*a* regelt das DSG die Wahl, die Stellung, die Wiederwahl und die Beendigung der Amtsdauer der oder des Beauftragten. In den Artikeln 27–33 sind die Aufgaben und Zuständigkeiten des Beauftragten festgelegt. Dieser überwacht die Einhaltung des Gesetzes durch die Bundesorgane und berät private Personen in Fragen des Datenschutzes. Er kann Abklärungen durchführen und Empfehlungen abgeben. Hält sich eine private Person nicht an eine Empfehlung, kann der Beauftragte die Angelegenheit dem Bundesverwaltungsgericht unterbreiten, und ist berechtigt, gegen diesen Entscheid Beschwerde zu führen (Art. 29 Abs. 4). Befolgt hingegen ein Bundesorgan eine Empfehlung nicht, kann er die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorlegen (Art. 27 Abs. 5). Der Beauftragte kann gegen den Entscheid der vorgesetzten Behörde und gegen den Entscheid der Beschwerdebehörde Beschwerde führen (Art. 27 Abs. 6).

Schliesslich enthält das DSG in den Artikeln 34 und 35 Strafbestimmungen bei Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten sowie bei Verletzung der beruflichen Schweigepflicht.

Vorbehaltlich von Artikel 37 DSG und Bestimmungen in Spezialgesetzen des Bundes werden Datenbearbeitungen kantonaler (und kommunaler) Organe durch das kantonale Recht geregelt. Dies gilt auch, wenn die betreffenden Organe Bundesrecht vollziehen oder die Daten über einen Online-Zugriff auf eine Datenbank des Bundes beschafft haben.

Neben dem DSG gelten in vielen Bereichen Spezialgesetze, die ebenfalls datenschutzrechtliche Bestimmungen enthalten (bereichsspezifische Datenschutznormen).

1.1.2 Vorarbeiten und Konzept

In den Jahren 2010 und 2011 wurde das DSG einer Evaluation[2] unterzogen. Diese hat ergeben, dass durch die technologischen und gesellschaftlichen Entwicklungen seit dem Inkrafttreten des DSG neue Bedrohungen für den Datenschutz entstanden sind und dass das DSG zum Teil nicht mehr ausreicht, um einen genügenden Schutz zu gewährleisten. Ausgehend von den Schlussfolgerungen der Evaluation und von seinem Bericht vom 9. Dezember 2011[3] beauftragte der Bundesrat das Eidgenössische Justiz- und Polizeidepartement (EJPD), gesetzgeberische Massnahmen zur Stärkung des Datenschutzes zu prüfen, mit denen den neuen Gefahren für die Privatsphäre Rechnung getragen werden kann.

Zur Umsetzung des Auftrags des Bundesrates vom 9. Dezember 2011 bildete das Bundesamt für Justiz (BJ) eine Arbeitsgruppe, um die Arbeiten zur Revision des DSG zu begleiten. Diese Arbeitsgruppe setzte sich aus Vertreterinnen und Vertretern der Bundesverwaltung[4], der Kantone[5], der Wirtschaft[6], der Konsumentenschutzorganisationen[7] sowie aus Expertinnen und Experten zusammen. Die Begleitgruppe präsentierte ihre Überlegungen im Bericht vom 29. Oktober 2014[8] mit dem Titel «Normkonzept zur Revision des Datenschutzgesetzes».

Am 1. April 2015 nahm der Bundesrat vom Bericht der Begleitgruppe Kenntnis und beauftragte das EJPD, zusammen mit dem Beauftragten, dem Eidgenössischen Departement für Wirtschaft, Bildung und Forschung (WBF), dem Eidgenössischen Finanzdepartement (EFD) und dem Eidgenössischen Departement des Innern (EDI) einen Vorentwurf für das Gesetz zu erarbeiten und dabei die Schlussfolgerungen des Berichts und die Entwicklungen im Europarat und in der Europäischen Union zu berücksichtigen.

Der Vorentwurf wurde am 21. Dezember 2016 in die Vernehmlassung geschickt. Die Vernehmlassung betraf drei Erlasse. Erstens einen Vorentwurf zu einem Gesetz – den Mantelerlass mit dem Titel «Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz». Darin waren die Totalrevision des DSG (VE-DSG) sowie die Teilrevision weiterer gleich-

2 Büro Vatter / Institut für Europarecht, Evaluation des Bundesgesetzes über den Datenschutz – Schlussbericht, Bern 10. März 2011, www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf.

3 Bericht des Bundesrates vom 9. Dezember 2011 über die Evaluation des Bundesgesetzes über den Datenschutz, BBl **2012** 335.

4 In der Arbeitsgruppe waren die folgenden Bundesbehörden vertreten: das Bundesamt für Justiz (BJ, Leitung), der Beauftragte, die Bundeskanzlei (BK), das Bundesamt für Kommunikation (BAKOM), das Schweizerische Bundesarchiv (BAR), das Eidgenössische Büro für Konsumentenfragen (BFK) und das Generalsekretariat des Eidgenössischen Justiz- und Polizeidepartements (GS-EJPD).

5 Die Kantone waren durch die Vereinigung der schweizerischen Datenschutzbeauftragten (PRIVATIM) vertreten.

6 Die Wirtschaft war durch economiesuisse und den Schweizerischen Gewerbeverband (SGV) vertreten.

7 Die Konsumentenschutzorganisationen waren durch die Fédération romande des consommateurs vertreten.

8 www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf.

rangiger Erlasse zusammengefasst. Zweitens den Entwurf des Bundesbeschlusses über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union (EU) betreffend die Übernahme der Richtlinie (EU) 2016/680. Drittens den Entwurf zur Revision des Übereinkommens des Europarates SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (E-SEV 108).

Ziel des Vorentwurfs war insbesondere:

- die Anforderungen der Richtlinie (EU) 2016/680[9] umzusetzen (vgl. Ziff. 2);
- die Empfehlungen im Rahmen der Schengen-Evaluation des Jahres 2014 umzusetzen (vgl. Ziff. 1.2.2.3);
- das DSG an die Anforderungen der Verordnung (EU) 2016/679[10] anzunähern (vgl. Ziff. 4);
- die Anforderungen des E-SEV 108 zu übernehmen (vgl. Ziff. 3).

Die Vernehmlassung ist am 4. April 2017 abgeschlossen worden.

Der Bundesrat hat auf Grundlage der Ergebnisse des Vernehmlassungsverfahrens einen Gesetzesentwurf erarbeitet. In der Form entspricht er dem Vorentwurf. Es handelt sich folglich um einen dem fakultativen Referendum unterstehenden Mantelerlass (Entwurf zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz; im Folgenden «Gesetzesentwurf»). Der Mantelerlass besteht aus einer Ziffer I, welche die Totalrevision des DSG (E-DSG) und in dessen Anhang die dadurch notwendigen Anpassungen weiterer Bundesgesetze beinhaltet. Ziffer II des Mantelerlasses enthält die Änderungen von Bundesgesetzen, die sich aus der Umsetzung der Richtlinie (EU) 2016/680 im Rahmen des Abkommens vom 26. Oktober 2004[11] zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (Schengen-Assoziierungsabkommen), ergeben. In der vorliegenden Botschaft werden die zu ändernden Erlasse jeweils mit «E» bezeichnet, gefolgt von der Abkürzung des betreffenden Gesetzes.

9 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2000/383/JI des Rates, ABl. L 119 vom 4.5.2016, S. 89.

10 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Ersetzung von Richtlinie 95/46/EC (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1.

11 SR **0.362.31**

1.1.3 Strategie «Digitale Schweiz»

Am 20. April 2016[12] hat der Bundesrat die Strategie «Digitale Schweiz» verabschiedet. Diese löste die Strategie für eine Informationsgesellschaft in der Schweiz vom 9. März 2012 ab.

Die neue Strategie hat zum Ziel, dass die Schweiz die zunehmende Digitalisierung noch konsequenter nutzt und sich als innovative Volkswirtschaft noch dynamischer entwickelt. In diesem Rahmen soll insbesondere eine kohärente und zukunftsorientierte Datenpolitik entwickelt werden. Diese soll der Schweiz erlauben, das Potenzial auszuschöpfen, das mit der zunehmenden Beschaffung und Bearbeitung von Daten verbunden ist. Gleichzeitig soll die Kontrolle über diese Daten erhalten bleiben. Die neue Strategie «Digitale Schweiz» versteht sich als übergreifende Strategie, unter deren Dach die zahlreichen Aktivitäten und die Expertengruppen aufeinander abgestimmt werden sollen. Diese Koordination wird durch das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) gewährleistet. Für die Verwirklichung der Strategie wurde ein Aktionsplan[13] erarbeitet, der alle Massnahmen umfasst, die von der Bundesverwaltung umzusetzen sind. Der Gesetzesentwurf ist eine dieser Massnahmen (Ziff. 1.2 und 1.7 des Aktionsplans).

Im Rahmen der Datenpolitik, die der Bundesrat entwickeln will, hat er das EJPD beauftragt, verschiedene juristische Fragen im Zusammenhang mit der Wiederverwendung digitaler Daten zu klären. Bei dieser Gelegenheit wird das EJPD unter anderem prüfen, ob in der schweizerischen Rechtsordnung ein Recht auf Portabilität der Personendaten eingeführt werden soll. Es wird ausserdem eine Studie darüber erstellen, welche Möglichkeiten der Bund gestützt auf die geltenden Gesetze und die laufenden Gesetzgebungsprojekte hat, um Personendaten im öffentlichen Interesse (z. B. für die öffentliche Statistik) wiederzuverwenden. Das EJPD muss dem Bundesrat die Ergebnisse seiner Arbeit Ende 2017 unterbreiten.

Bei der Erarbeitung dieser Strategie liess das Bundesamt für Kommunikation (BAKOM) von der Berner Fachhochschule eine Studie zur Problematik von *Big Data* (sehr grossen Datenmengen) erstellen: «Big Data: Chancen, Risiken und Handlungsbedarf des Bundes»[14]. Diese Studie gelangte teilweise zu den gleichen Schlussfolgerungen wie die Evaluation des DSG. Demnach besteht gesetzgeberischer Handlungsbedarf. Auch müsse die Funktionsweise des Marktes verbessert werden, indem die Nutzerinnen und Nutzer mehr Befugnisse erhalten sowie die Regulierung und Kontrolle der privaten Akteure durch den Staat ausgebaut werden. Die im Gesetzesentwurf vorgesehenen Massnahmen gehen in diese Richtung.

12 Die Strategie «Digitale Schweiz» ist abrufbar unter: www.bakom.admin.ch > Digitale Schweiz und Internet > Strategie «Digitale Schweiz».

13 www bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/strategie/aktionsplan_digitale_schweiz.pdf.download.pdf/aktionsplan_digitale_schweiz_DE.pdf.

14 «Big Data: Chancen, Risiken und Handlungsbedarf des Bundes», verfügbar (ausschliesslich auf Deutsch) unter: www.bakom.admin.ch/bakom/de/home/digital-und-internet/big-data.html.

1.1.4 Weitere Arbeiten der Bundesverwaltung im Zusammenhang mit dem Datenschutz

Innerhalb der Bundesverwaltung hängen zahlreiche Arbeiten mit dem Datenschutz zusammen. Nachfolgend sind die wichtigsten laufenden Projekte aufgeführt:

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken vom 27. Juni 2012[15] *(NCS):* Bei dieser Strategie geht es darum, Infrastrukturen, die Informations- und Kommunikationstechnologien nutzen, vor Cyber-Risiken zu schützen. Die Strategie ist darauf ausgerichtet, Bedrohungen und Gefahren im Cyber-Bereich frühzeitig zu erkennen, die Widerstandsfähigkeit kritischer Infrastrukturen zu erhöhen sowie Cyber-Risiken – insbesondere die Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage – wirksam zu reduzieren. Für die Umsetzung dieser Strategie ist das EFD zuständig. Die Umsetzung der Strategie wird dieses Jahr plangemäss abgeschlossen. Gemäss dem am 26. April 2017[16] vom Bundesrat verabschiedeten Jahresbericht 2016 zum Stand der Umsetzung der NCS sind 15 der 16 vorgesehenen Massnahmen bereits realisiert worden. Aufgrund der gestiegenen Cyberrisiken hat der Bundesrat beschlossen, eine zweite Strategie für die Jahre 2018–2023 erarbeiten zu lassen, die den gegenwärtigen Bedrohungen gerecht wird und die Ergebnisse der Überprüfung der Wirksamkeit der NCS berücksichtigt.

Open Government Data Strategie Schweiz vom 16. April 2014[17]*:* Mit dieser Strategie soll die Publikation von Daten, die von der Verwaltung als *Open Government Data* (OGD), also als frei weiterverwendbare Behördendaten, beschafft werden, gefördert werden. Obwohl bei OGD-Projekten typischerweise aggregierte und anonymisierte Daten für die Weiterverwendung bereitgestellt werden, muss den Datenschutzgrundsätzen Rechnung getragen werden.

Nationales Forschungsprogramm 75 «Big Data»[18] *(NFP 75):* Dieses Programm mit einem Finanzrahmen von 25 Millionen Franken wurde vom Bundesrat im Jahr 2015 lanciert. Es soll die wissenschaftlichen Grundlagen für einen wirksamen und angemessenen Einsatz grosser Datenmengen liefern. Das Programm ist in drei Bereiche gegliedert: ein Modul zu den Informationstechnologien, den Datenmanagementdiensten und zu Fragen im Zusammenhang mit der Sicherheit, der Auskunft, der Aufsicht und dem Vertrauen; ein Modul zu den gesellschaftlichen Herausforderungen von Big Data sowie ein Modul zur Entwicklung von Big-Data-Applikationen in verschiedenen Gesellschaftsbereichen. Seit Anfang 2017 sind 35 Forschungsprojekte lanciert worden. Jedes dauert 24 bis 48 Monate. Die ersten Ergebnisse werden ab 2019 vorliegen. Bis im Jahr 2022 werden in diesem Programm zahlreiche Aktivitäten zum Wissenstransfer durchgeführt werden.

Expertenkommission «Zukunft der Datenbearbeitung und Datensicherheit»: Diese Expertengruppe wurde nach der Annahme der Motion Rechsteiner 13.3841 «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit» vom EFD

15 www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html
16 www.newsd.admin.ch/newsd/message/attachments/48041.pdf
17 www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn004-open_government_data_strategie_schweiz.html
18 www.nfp75.ch/de

gebildet. Die Arbeiten der Expertenkommission werden möglicherweise zu zusätzlichen Reformen im Bereich des Datenschutzes führen. Allerdings ist der Handlungsspielraum des schweizerischen Gesetzgebers aufgrund des europäischen Umfelds begrenzt. Soweit sich ein Bedarf nach zusätzlichen Reformen ergibt, können diese in einer nächsten Etappe umgesetzt werden. Zudem ist nicht auszuschliessen, dass auch in anderen Bereichen als dem Datenschutz (beispielsweise im Obligationenrecht[19] [OR], im Immaterialgüterrecht, bei der Objektsicherheit, im Wettbewerbsrecht) ein entsprechender Reformbedarf besteht. Die Arbeiten der Kommission werden voraussichtlich nicht vor Mitte 2018 abgeschlossen sein.

Jugend und Medien – Schutz von Kindern und Jugendlichen vor den digitalen Medien: Am 13. Mai 2015 hat der Bundesrat den Bericht «Jugend und Medien. Zukünftige Ausgestaltung des Kinder- und Jugendmedienschutzes der Schweiz» verabschiedet und damit beschlossen, die im Rahmen des nationalen Programms «Jugend und Medien»[20] lancierten Aktivitäten weiterzuführen. Dieses Programm wurde von 2011 bis 2015 umgesetzt. Das EDI (Bundesamt für Sozialversicherungen, BSV) hat den Auftrag, erzieherische und regulierende Massnahmen umzusetzen und zu koordinieren. Der Datenschutz gehört zu den Themen, die im Rahmen des erzieherischen Teils behandelt werden.

Bericht des Bundesrates vom 11. Januar 2017[21] *über die zentralen Rahmenbedingungen für die digitale Wirtschaft:* Der Bericht setzt sich mit den Bereichen auseinander, welche für die digitale Wirtschaft von zentraler Bedeutung sind. Es sind fünf Bereiche überprüft worden: Arbeitsmarkt, Forschung und Entwicklung, Sharing Economy, Digital Finance und Wettbewerbspolitik. Der Bundesrat hat das Staatssekretariat für Wirtschaft (SECO) beauftragt, gestützt auf Umfragen bei den Verbänden, Sozialpartnern sowie ausgewählten Unternehmen eine Analyse der digitalen Tauglichkeit bestehender, wirtschaftspolitisch relevanter Gesetze vorzulegen und allfälligen Revisionsbedarf aufzuzeigen («Digitaler Test»). Im Zentrum steht die Identifikation von Bestimmungen, welche aufgrund der technologischen Entwicklung ihren Nutzen weitgehend eingebüsst haben.

Nationale Forschungsprogramme (NFP) zum Thema «Digitaler Wandel von Wirtschaft und Gesellschaft»[22]: Am 5. Juli 2017 hat der Bundesrat das Eidgenössische Departement für Wirtschaft, Bildung und Forschung bzw. das Staatssekretariat für Bildung, Forschung und Innovation beauftragt, eine NFP-Serie zum Thema «Digitaler Wandel von Wirtschaft und Gesellschaft» zu prüfen. Unter Einbezug der Kantone soll geprüft werden, welche Auswirkungen die Digitalisierung im Bildungsbereich hat und welche Konsequenzen daraus allenfalls zu ziehen sind. Darüber hinaus ist zu untersuchen, inwiefern für die Bewältigung der digitalen Transformation Forschungslücken an den Hochschulen behoben werden müssen. Besonderes Augenmerk ist darauf zu richten, in welcher Breite Forschungskapazitäten in der

19 SR **210**
20 www.jeunesetmedias.ch/de/accueil.html
21 www.seco.admin.ch/seco/de/home/wirtschaftslage---wirtschaftspolitik/wirschaftspolitik/digitalisierung.html
22 Vgl. www.sbfi.admin.ch/sbfi/de/home/themen/forschung-und-innovation-in-der-schweiz/foerderinstrumente/nationale-forschungsprogramme-nfp.html

Schweiz vorhanden sein müssen, um den Wissens- und Technologietransfer in die Wirtschaft und den sicheren Betrieb kritischer Infrastrukturen zu gewährleisten.

1.1.5 Parlamentarische Vorstösse

Seit einigen Jahren ist der Datenschutz Gegenstand zahlreicher parlamentarischer Vorstösse. Nachfolgend werden lediglich die wichtigsten Vorstösse aufgezählt:

- Parlamentarische Initiative Vischer 14.413 «Grundrecht auf informationelle Selbstbestimmung»: Gemäss dem Urheber der Initiative schützt Artikel 13 Absatz 2 der Bundesverfassung[23] (BV) jede Person ausschliesslich vor dem «Missbrauch ihrer persönlichen Daten». Damit liege die Beweislast für den Missbrauch nicht beim Staat oder beim Internetbetreiber, sondern bei den Bürgerinnen und Bürgern. Mit der Initiative soll der Wortlaut von Artikel 13 Absatz 2 BV so geändert werden, dass die Garantie nicht nur einen Anspruch auf Schutz vor Missbrauch gewährt, sondern ein Grundrecht auf informationelle Selbstbestimmung. Die Staatspolitische Kommission des Nationalrates hat die Initiative am 29. August 2014 angenommen, diejenige des Ständerates am 20. August 2015.
- Parlamentarische Initiative Derder 14.434 «Schutz der digitalen Identität von Bürgerinnen und Bürgern»: Mit dieser Initiative soll Artikel 13 BV wie folgt geändert werden: «Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung, ihres Brief-, Post- und Fernmeldeverkehrs sowie all ihrer eigenen Daten» (Abs. 1) und «Die Daten sind Eigentum der betreffenden Person; diese ist davor zu schützen, dass die Daten missbräuchlich verwendet werden» (Abs. 2). Die Staatspolitische Kommission des Nationalrates hat die Initiative am 16. Januar 2015 angenommen, diejenige des Ständerates am 20. August 2015.
- Postulat Hodgers 10.3383 «Anpassung des Datenschutzgesetzes an die neuen Technologien»: Dieser Vorstoss wurde vom Nationalrat am 1. Oktober 2010 verabschiedet. Mit dem Postulat wird der Bundesrat beauftragt, zu untersuchen, ob der Datenschutz und das Recht auf Schutz des Privatlebens gestärkt werden können, indem das DSG revidiert und an die neuen Technologien angepasst wird. Dieses Postulat wurde durch den Bericht des Bundesrates vom 9. Dezember 2011[24] über die Evaluation des Bundesgesetzes über den Datenschutz bereits teilweise erfüllt.
- Postulat Graber 10.3651 «Angriff auf die Privatsphäre und indirekte Bedrohungen der persönlichen Freiheit»: Der Nationalrat hat diesen Vorstoss am 17. Dezember 2010 angenommen. Der Urheber des Postulats verlangt vom Bundesrat, in einem Bericht zu den folgenden Fragen Stellung zu nehmen: Risiken für die Privatsphäre durch Technologien zur Überwachung und Informationserfassung; Ziehen von Grenzen zum Schutz der Privatsphäre, gegebenenfalls durch das Festlegen eines unverletzbaren und unantastbaren

23 SR **101**
24 BBl **2012** 335 350

Kerngehalts der Privatsphäre; Sinn einer Verschärfung der Gesetzgebung zum Schutz der Privatsphäre und persönlicher Daten. Auch dieses Postulat wurde durch den Bericht des Bundesrates vom 9. Dezember 2011 teilweise erfüllt.

– Postulat Schwaab 12.3152 «Recht auf Vergessen im Internet»: Diesem Vorstoss hat der Nationalrat am 15. Juni 2012 zugestimmt. Mit dem Postulat wurde der Bundesrat beauftragt, zu prüfen, ob es zweckmässig ist, ein «Recht auf Vergessen im Internet» in die Gesetzgebung aufzunehmen und dieses Recht zu präzisieren. Zudem soll untersucht werden, wie die Nutzerinnen und Nutzer dieses Recht besser geltend machen können.

– Motion Rechsteiner 13.3841 «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit: Mit dieser Motion wird der Bundesrat beauftragt, eine interdisziplinäre Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit einzusetzen. Dieser Vorstoss wurde vom Ständerat am 3. Dezember 2013 und vom Nationalrat am 13. März 2014 angenommen. Die Tragweite der damit verbundenen Arbeiten, mit denen das EFD beauftragt wurde, geht über den Rahmen der vorliegenden Vorlage hinaus (vgl. Ziff. 1.1.3). Das EFD sieht jedoch eine Reihe von Massnahmen vor, die mit der Umsetzung dieser Motion zusammenhängen.

– Postulat Recordon 13.3989 «Verletzungen der Persönlichkeitsrechte im Zuge des Fortschritts der Informations- und Kommunikationstechnik»: Der Ständerat hat den Vorstoss am 11. Dezember 2013 angenommen. Mit diesem Postulat wird der Bundesrat gebeten, einen Bericht darüber vorzulegen, welche Risiken die Fortschritte der Informations- und Kommunikationstechnik für die Persönlichkeitsrechte darstellen und welche Lösungen dafür denkbar sind.

– Motion Comte 14.3288 «Identitätsmissbrauch. Eine strafbare Handlung für sich»: Diesen Vorstoss haben die eidgenössischen Räte am 12. Juni bzw. 24. November 2014 angenommen. Er verlangt vom Bundesrat, einen Entwurf zur Änderung des Strafrechts auszuarbeiten, damit der Missbrauch einer Identität eine eigenständige Straftat wird.

– Postulat Derder 14.3655 «Die digitale Identität definieren und Lösungen für ihren Schutz finden»: Diesem Vorstoss hat der Nationalrat am 26. September 2014 zugestimmt. Mit dem Postulat wird der Bundesrat beauftragt, dem Parlament einen Bericht vorzulegen, in dem die digitale Identität der Bürgerinnen und Bürger definiert und in ihre gegenwärtige Rechtspersönlichkeit integriert wird. Der Bericht soll ebenfalls auf die digitalen Spuren von potenziell öffentlich zugänglichen Daten sowie auf die Bedrohung der Privatsphäre eingehen und aufzeigen, wie diese vor den Aktivitäten schweizerischer oder ausländischer Unternehmen oder Nachrichtendienste geschützt werden kann.

– Postulat Schwaab 14.3739 «Control by Design. Die Rechte auf Eigentum im Falle von unerwünschten Verbindungen verstärken»: Der Nationalrat hat diesen Vorstoss am 29. Oktober 2014 angenommen. Der Urheber des Postulats verlangt vom Bundesrat, zu prüfen, ob die «Kontrolle ab der Herstel-

lung» (Control by Design) in die Gesetzgebung eingeführt werden soll, sodass die Person, die im Besitz oder Eigentum einer Sache ist, das Recht hat, die Verbindung dieser Sache mit irgendeinem Netzwerk zu unterbinden. Der Bundesrat soll insbesondere evaluieren, ob in Bezug auf die Eigentums- und Besitzübertragung sowie den Datenschutz die Gesetzgebung anzupassen ist.

– Postulat Schwaab 14.3782 «Richtlinien für den ‹digitalen Tod›»: Der Vorstoss wurde am 12. Dezember 2014 vom Nationalrat angenommen. Er beauftragt den Bundesrat zu prüfen, ob das Erbrecht ergänzt werden muss, um die Rechte der Erbinnen und Erben auf Personendaten und digitale Zugänge der verstorbenen Person sowie die Auswirkungen des Todes auf deren virtuelle Präsenz zu regeln.

– Postulat FDP-Liberale Fraktion 14.4137 «Videoaufnahmen durch Private. Die Privatsphäre besser schützen»: Mit dem Postulat wird der Bundesrat beauftragt, einen Bericht auszuarbeiten, der sich schwerpunktmässig mit den Risiken der Nutzung privater Kameras in Drohnen und Datenbrillen befasst. Diesen Vorstoss hat der Nationalrat am 20. März 2015 angenommen.

– Postulat Comte 14.4284 «Videoaufnahmen durch Private. Die Privatsphäre besser schützen»: Es hat denselben Wortlaut wie das oben genannte Postulat 14.4137. Diesen Vorstoss hat der Ständerat am 19. März 2015 angenommen.

– Postulat Derder 15.4045 «Recht auf Nutzung der persönlichen Daten. Recht auf Kopie»: Das Postulat verlangt vom Bundesrat, zu prüfen und darüber Bericht zu erstatten, inwiefern der Einzelne und die Volkswirtschaft von der Weiterverwendung personenbezogener Daten profitieren könnten. Der Bundesrat soll insbesondere ein Recht auf Kopie für den Einzelnen untersuchen. Der Nationalrat hat diesen Vorstoss am 18. Dezember 2015 angenommen.

– Postulat Béglé 16.3383 «Elektronische Daten: Information der Geschädigten im Falle eines Hackerangriffs»: Mit diesem Postulat wird der Bundesrat beauftragt, zu prüfen, ob und wie Organisationen, die Opfer eines Hackerangriffs wurden, durch den Dritte Zugang zu elektronischen Daten erhielten, für deren Sicherheit die Organisationen verantwortlich waren, verpflichtet werden können, die geschädigten Personen zu informieren, damit diese Massnahmen zur Schadensbegrenzung treffen können. Der Nationalrat hat diesem Vorstoss am 30. September 2016 zugestimmt.

– Postulat Béglé 16.3384 «Elektronische medizinische Daten. Eine geschützte, transparente und zielgerichtete Datenerhebung im revidierten Bundesgesetz über den Datenschutz sicherstellen»: Der Bundesrat wird beauftragt, zu prüfen, wie die folgenden Punkte in das revidierte Datenschutzgesetz integriert werden können, damit medizinische Daten so gut wie möglich geschützt werden: strenge und einheitliche Bestimmungen betreffend die Sicherheit, Speicherung und Übermittlung sowie den Zugriff auf die Daten für alle Beteiligten; Einführung des Prinzips der «tatsächlichen Einwilligung» der Patientin oder des Patienten; Grundsätze Privacy by Default und Privacy by Design; Sensibilisierung der betroffenen Personen für die Gefahren im Zusammenhang mit der Übertragung gewisser persönlicher Daten. Der Nationalrat hat dieses Postulat am 30. September 2016 angenommen.

- Postulat Béglé 16.3386 «Kontrolle über persönliche Daten. Informationelle Selbstbestimmung fördern»: Mit diesem Postulat wird der Bundesrat gebeten, zu prüfen, wie am besten dazu beigetragen werden kann, dass die Bürgerinnen und Bürger die Kontrolle über ihre persönlichen Daten wiedererlangen. Der Nationalrat hat diesem Vorstoss am 30. September 2016 zugestimmt.
- Postulat Schwaab 16.3682 «Die Tätigkeiten von Wirtschaftsauskunfteien einschränken»: Der Bundesrat wird mit dem Postulat beauftragt zu prüfen, ob es nicht notwendig wäre, die Praktiken der Wirtschaftsauskunfteien stärker zu regeln, namentlich ob nicht im Bereich der Methoden, die zur Beschaffung von Informationen über Privatpersonen und Unternehmen verwendet werden können, klarere Grenzen eingeführt werden sollten. Der Nationalrat hat das Postulat am 16. Dezember 2016 wie vom Bundesrat beantragt angenommen.
- Parlamentarische Initiative Leutenegger Oberholzer 16.409 «Wahlverfahren für den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten oder die -beauftragte»: Die parlamentarische Initiative verlangt, dass der Beauftragte von der Bundesversammlung gewählt wird. Die Staatspolitische Kommission des Nationalrats hat der Initiative am 20. Januar 2017 Folge gegeben. Ihre Schwesterkommission hat sich diesem Entscheid am 31. März 2017 angeschlossen.

1.2 Ausgangslage auf internationaler Ebene

1.2.1 Allgemeine Bemerkungen zum Schutz der Privatsphäre auf internationaler Ebene

Die damalige UN-Hochkommissarin für Menschenrechte, Navi Pillay, hat am 16. Juli 2014 ihren Bericht zum Schutz der Privatsphäre im digitalen Zeitalter (A/HRC/27/37) präsentiert (vgl. Ziff. 1.2.4). Dieser Bericht gibt einen konzisen Überblick über den menschenrechtlichen Rahmen zum Schutz der Privatsphäre im digitalen Zeitalter und zieht eine ernüchternde Bilanz der gegenwärtigen Rechtswirklichkeit.

Auf internationaler Ebene ist zunehmend anerkannt, dass jede Bearbeitung von Personendaten grundsätzlich die Privatsphäre berührt und weitere Menschenrechte beeinträchtigen kann. Um die Privatsphäre wirksam zu schützen, sind hinreichende gesetzliche Regelungen zu schaffen, die solche Eingriffe rechtfertigen. Rechte, die offline gelten, sind auch online geschützt. Neben dem Recht auf Privatsphäre, das nicht nur in Artikel 13 der Bundesverfassung, sondern auch in verschiedenen völkerrechtlich verbindlichen Abkommen garantiert wird (Übereinkommen vom 28. Januar 1981[25] zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Übereinkommen SEV 108]; Art. 8 der Konvention vom 4. November 1950[26] zum Schutze der Menschenrechte und Grundfreiheiten

25 SR **0.235.1**
26 SR **0.101**

[EMRK], Art. 17 des Internationalen Pakts vom 16. Dezember 1966[27] über bürgerliche und politische Rechte [UNO-Pakt II]), können auch weitere Grund- und Menschenrechte betroffen sein. Dazu gehören namentlich die Meinungs- und Informationsfreiheit (Art. 16 BV, Art. 10 EMRK, Art. 19 UNO-Pakt II), das Recht, sich friedlich zu versammeln (Art. 22 BV, Art. 11 EMRK, Art. 21 UNO-Pakt II) und sich zu Vereinigungen zusammenzuschliessen (Art. 23 und 28 BV, Art. 11 EMRK, Art. 22 UNO-Pakt II).

Für Einschränkungen des Schutzes der Privatsphäre sei insbesondere auf die Anforderungen an einen rechtmässigen Eingriff gemäss Artikel 8 Absatz 2 EMRK verwiesen (gesetzliche Grundlage, Rechtfertigung aus einem der in Art. 8 Abs. 2 EMRK explizit aufgeführten Gründe sowie Verhältnismässigkeit). Diese Anforderungen sind eng auszulegen. Der Europäische Gerichtshof für Menschenrechte (EGMR) räumt den Vertragsstaaten zwar regelmässig einen weiten Gestaltungsspielraum hinsichtlich der Legitimität des verfolgten Zwecks ein.[28] Hingegen stellt er an die Ausgestaltung der gesetzlichen Grundlage recht hohe Anforderungen. So muss das den Eingriff erlaubende Gesetz hinreichend bestimmt sein, grundsätzlich Vorkehrungen gegen Datenmissbrauch enthalten sowie den Betroffenen die Möglichkeit geben, Auskunft betreffend die über sie gesammelten Daten zu erhalten. Auch hat das Gesetz zu bestimmen, wer welche Daten zu welchem Zweck bearbeiten darf, wie lange die Daten aufbewahrt werden dürfen und auf welche Weise die Einhaltung der Vorgaben kontrolliert wird. Bei sensiblen Daten werden erhöhte Anforderungen gestellt.

1.2.2 Europäische Union

1.2.2.1 Einschlägige Regelung

Die Europäische Union hat in den letzten Jahrzehnten mehrere Erlasse zum Schutz von Personendaten verabschiedet. Der wichtigste ist die Richtlinie 95/46/EG vom 24. Oktober 1995[29] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Richtlinie 95/46/EG). Diese Richtlinie wurde ergänzt durch den Rahmenbeschluss 2008/977/JI vom 27. November 2008[30] über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (Rahmenbeschluss 2008/977/JI).

Im Rahmen des Stockholmer Programms[31] erklärte die Europäische Union, sie wolle eine neue einheitliche Gesetzgebung im Bereich des Datenschutzes schaffen. Damit soll insbesondere das Grundrecht auf Schutz personenbezogener Daten gewährleistet werden. Ausserdem soll dies die Entwicklung der digitalen Wirtschaft und eine wirksamere Bekämpfung der Kriminalität und des Terrorismus erlauben. Der Euro-

27 SR **0.103.2**
28 Vgl. hierzu z.B. EGMR 59842/00 (Vetter v. France) vom 31.8.2005; EGMR 44647/98 (Peck v. UK) vom 28.1.2003; EGMR 27798/95 (Amann v. Switzerland) vom 16.2.2000.
29 ABl. L 281 vom 23.11.1995, S. 31.
30 ABl. L 350 vom 30.12.2008, S. 60.
31 ABl. C 115 vom 4.5.2010, S. 1.

päische Rat hat die Europäische Kommission gebeten, die Funktionsweise der Richtlinie 95/46/EG und des Rahmenbeschlusses 2008/977/JI zu evaluieren und ihm gegebenenfalls neue Initiativen im Bereich des Datenschutzes vorzulegen. In ihrer Mitteilung vom 4. November 2010[32] mit dem Titel «Gesamtkonzept für den Datenschutz in der Europäischen Union» kam die Europäische Kommission zum Schluss, dass die Europäische Union eine allgemeinere und kohärentere Politik im Zusammenhang mit dem Grundrecht auf Schutz personenbezogener Daten benötigt.

Am 27. April 2016 haben das Europäische Parlament und der Rat der Europäischen Union eine Reform der Datenschutzgesetzgebung verabschiedet, die zwei Erlasse umfasst. Dabei handelt es sich erstens um die Verordnung (EU) 2016/679, welche die Richtlinie 95/46/EG ersetzen wird (vgl. Ziff. 4). Der zweite verabschiedete Erlass ist die Richtlinie (EU) 2016/680, die den Rahmenbeschluss 2008/977 /JI ersetzen wird (vgl. Ziff. 2).

Für die Schweiz ist die Richtlinie (EU) 2016/680 Bestandteil des Schengen-Acquis. Aufgrund des Schengen-Assoziierungsabkommens muss die Schweiz die Richtlinie umsetzen. Hingegen ist sie nicht verpflichtet, die Verordnung (EU) 2016/679 zu übernehmen, da es sich gemäss der Europäischen Union dabei nicht um eine Weiterentwicklung des Schengen-Acquis handelt.

Im Rahmen der Strategie zum digitalen Binnenmarkt in Europa hat die Europäische Kommission am 10. Januar 2017 einen Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation vorgelegt. Diese Vorlage soll die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2001[33] über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation ersetzen. Die Verordnung wäre ein Spezialgesetz zur Verordnung (EU) 2016/679, indem sie letztere in Bezug auf die elektronische Kommunikation präzisiert und ergänzt.[34] Es handelt sich hierbei nicht um eine Schengen-Weiterentwicklung.

1.2.2.2 Angemessenheitsbeschluss

In den Bereichen, die nicht der Schengen-Zusammenarbeit unterstehen, gilt die Schweiz als Drittstaat. Zwischen einem Drittstaat und den Mitgliedstaaten der Europäischen Union dürfen Daten nur ausgetauscht werden, wenn der Drittstaat ein angemessenes Schutzniveau gemäss der Richtlinie 95/46/EG gewährleistet. Dieses Schutzniveau wird durch die Europäische Kommission periodisch überprüft und in einem Angemessenheitsbeschluss festgehalten. Ein solcher Beschluss kann jederzeit widerrufen werden.

32 COM (2010) 609 final.
33 ABl. L 201, 31.7.2002, S. 37–47.
34 Ziff. 1.2 des Explanatory memorandum zum Vorschlag.

Die Europäische Kommission hat in einem Angemessenheitsbeschluss vom 26. Juli 2000 bestätigt, dass die Schweiz über ein angemessenes Datenschutzniveau verfügt.[35] Diese Entscheidung beruht jedoch auf dem in der Richtlinie 95/46/EG festgelegten Schutzniveau.

Mit Schreiben vom 25. Januar 2017 hat die Europäische Kommission die Mission der Schweiz bei der Europäischen Union nach einem Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015 (Rechtssache «Schrems») darüber informiert, dass sie das von den Drittländern mit einem Angemessenheitsbeschluss gewährleistete angemessene Datenschutzniveau regelmässig überprüfen muss. Die Europäische Kommission hat die Schweiz deshalb darum ersucht, ihr einen Bericht zukommen zu lassen, in dem die rechtliche Ausgangslage im Bereich Datenschutz sowie die hauptsächlichen Gesetzesänderungen seit 2000 dargelegt werden. Der Bericht wird der Europäischen Kommission vor Ende 2017 übermittelt werden.

Künftig wird die schweizerische Gesetzgebung anhand der in der Verordnung (EU) 2016/679 enthaltenen Anforderungen überprüft. Falls die Schweiz den Angemessenheitsbeschluss beibehalten bzw. im Falle eines Widerrufs erneut eine Bestätigung über das angemessene Datenschutzniveau erhalten möchte, ist es insbesondere für die Wirtschaft von zentraler Bedeutung, dass die schweizerische Gesetzgebung einen den Anforderungen dieser Verordnung entsprechenden Schutz gewährleistet.

1.2.2.3 Empfehlungen im Zusammenhang mit den Schengener Abkommen

Mit der Schengen- und Dublin-Assoziierung hat die Schweiz sich verpflichtet, dass die Bearbeitung von Personendaten bei der Schengen-Zusammenarbeit dem geltenden Gemeinschaftsrecht im Bereich des Datenschutzes, insbesondere der Richtlinie 95/46/EG und dem Rahmenbeschluss 2008/977/JI, entspricht.

Im Rahmen der Schengen-Evaluation überprüft die Europäische Union regelmässig, ob die Schengen-Staaten und damit auch die Schweiz ihren Verpflichtungen nachkommen. Die letzte Schengen-Evaluation der Schweiz fand im ersten Halbjahr 2014 statt.

Am 11. September 2014 hat der Rat der Europäischen Union den Bericht des Evaluationsausschusses zum Datenschutz in der Schweiz im Bereich der Schengen-Zusammenarbeit genehmigt. Demnach erfüllt die schweizerische Gesetzgebung im Bereich des Datenschutzes die Anforderungen des Schengen-Besitzstands. Im Evaluationsbericht wird der Schweiz indessen nahegelegt, die Befugnisse des Beauftragten auszubauen, indem ihm Entscheidungskompetenzen eingeräumt werden. Auch ein Ausbau der Sanktionsbefugnisse des Beauftragten wäre zu begrüssen. Bei der nächsten Evaluation, die 2018 durchgeführt wird, muss die Schweiz darüber Bericht erstatten, wie sie die Empfehlungen der Expertinnen und Experten umgesetzt hat.

35 Entscheidung der Kommission vom 26. Juli 2000 gemäss der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, ABl. L 215 vom 25.8.2000, S. 1.

Der E-DSG kommt den Empfehlungen des Rates der Europäischen Union insoweit nach, als der Beauftragte Verfügungskompetenzen erhält (siehe Art. 44 und 45 E-DSG). Hingegen wäre es nach Ansicht des Bundesrates nicht angemessen, dem Beauftragten die Befugnis einzuräumen, Verwaltungssanktionen gegen Bundesorgane zu verhängen. Diese in anderen Ländern bestehende Möglichkeit widerspricht nach Meinung des Bundesrates der schweizerischen Rechtstradition. Die Möglichkeit des Beauftragten, eine von einem Bundesorgan durchgeführte Datenbearbeitung zu untersagen oder auszusetzen, sowie die Stärkung der strafrechtlichen Bestimmungen des DSG sind nach Auffassung des Bundesrates wirksam genug.

1.2.3 Europarat (Übereinkommen SEV 108)

Am 28. Januar 1981 hat der Europarat den ersten völkerrechtlichen Vertrag im Bereich des Datenschutzes verabschiedet: das Übereinkommen SEV 108, das von der Schweiz am 2. Oktober 1997 ratifiziert wurde. Dieses Übereinkommen wurde durch das Zusatzprotokoll vom 8. November 2001[36] zum Übereinkommen SEV 108 bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung (SEV 181, im Folgenden «Zusatzprotokoll») ergänzt. Das Zusatzprotokoll wurde von der Schweiz am 20. Dezember 2007 ratifiziert. Das Übereinkommen SEV 108 wurde inzwischen auch von Staaten ratifiziert, die nicht Mitglieder des Europarats sind (vgl. Ziff. 3.1).

Im Jahr 2011 leitete der Europarat ein Verfahren zur Revision des Übereinkommens SEV 108 und seines Zusatzprotokolls ein. Damit sollen die Herausforderungen für den Schutz der Privatsphäre und der Grundrechte der betroffenen Personen, welche die Globalisierung, die technologischen Entwicklungen und die Zunahme des grenzüberschreitenden Datenverkehrs mit sich bringen, besser bewältigt werden können. Unter schweizerischer Leitung hat der beratende Ausschuss des Übereinkommens SEV 108 einen Entwurf zu dessen Revision erarbeitet. Die Arbeiten des vom Ministerkomitee eingesetzten Ad-hoc-Komitees (CAHDATA) wurden im Juni 2016 abgeschlossen. Das Änderungsprotokoll zum Übereinkommen SEV 108 muss vom Ministerkomitee noch verabschiedet werden (vgl. Ziff. 3.2). Die vorliegende Botschaft beruht auf dem Entwurf zur Revision des Übereinkommens (in der Fassung vom September 2016[37]), der voraussichtlich keine substanziellen Änderungen mehr erfahren wird.

Der E-SEV 108 ist inhaltlich sehr ähnlich wie die Richtlinie (EU) 2016/680 und die Verordnung (EU) 2016/679. Er ist jedoch weniger detailliert. Die Europäische Kommission, welche die Mitgliedstaaten der Europäischen Union bei den Verhandlungen vertrat, hat darauf geachtet, dass der Inhalt des E-SEV 108 mit dem neuen Recht der Europäischen Union vereinbar ist.

36 SR **0.235.11**
37 Die französische Fassung kann unter folgender Adresse eingesehen werden: rm.coe.int/16806b6f7b.

1.2.4 Vereinte Nationen

Seit der Snowden-Affäre ist das Recht auf Privatsphäre für mehrere UNO-Institutionen ein vorrangiges Thema. So hat die UNO-Generalversammlung im Dezember 2013 eine Resolution[38] verabschiedet. Sie ruft alle Staaten auf, ihre Gesetzgebung zum Schutz des Rechts auf Privatsphäre zu überarbeiten. Darüber hinaus wird das UNO-Hochkommissariat für Menschenrechte (UNHCHR) ersucht, einen Bericht über «die Förderung des Rechts auf Privatsphäre im Kontext des innerstaatlichen und extraterritorialen Überwachens und/oder Abfangens von digitaler Kommunikation und des Sammelns personenbezogener Daten, namentlich in massivem Umfang» zu erarbeiten. Dieser Bericht wurde im Juli 2014 vorgelegt.[39] Im Weiteren hat der Menschenrechtsrat im März 2015 für einen Zeitraum von drei Jahren einen Sonderberichterstatter für das Recht auf Privatsphäre eingesetzt. Dieser hat den Auftrag, zu analysieren, welche Herausforderungen die rasante technologische Entwicklung und die daraus resultierenden neuen Möglichkeiten für die Überwachung der privaten Kommunikation für den Schutz des Rechts auf Privatsphäre mit sich bringen. Die Schweiz hat diese beiden Initiativen unterstützt und sich aktiv daran beteiligt.

Der Sonderberichterstatter hat bisher zwei Berichte vorgelegt, einen am 8. März 2016[40] und den anderen am 27. Februar 2017[41].

Im ersten Bericht legt er eine Bestandesaufnahme im Bereich des Schutzes der Privatsphäre zu Beginn des Jahres 2016 sowie einen Aktionsplan für die drei ersten Jahre seines Mandats vor. Er hebt insbesondere hervor, dass das Fehlen einer universell verbindlichen Definition von «Privatsphäre» eines der Haupthindernisse für deren umfassenden rechtlichen Schutz darstellt. Er stellt insgesamt auch fest, dass die ursprünglich gegenüber den Staaten bestehende Befürchtung, dass Personendaten missbräuchlich verwendet werden, nun gegenüber den Unternehmen geäussert wird. Er erachtet daher einen internationalen Dialog über das Sammeln von bzw. den Umgang mit Personendaten durch Unternehmen sowie deren Weitergabe an staatliche Stellen als notwendig.[42] Ferner beobachtet der Sonderberichterstatter bei Konsumentinnen und Konsumenten ein zunehmendes Bewusstsein für die Risiken betreffend das Recht auf Privatsphäre; dies äussere sich beispielsweise im sich rasch entwickelnden Markt für «privatsphärefreundliche» Produkte und Dienstleistungen.[43] Schliesslich anerkennt er die Bedeutung der sich rasch entwickelnden Industrie von biometrisch geschützten Produkten und beabsichtigt mit der Forschung, den Strafverfolgungsbehörden und Nachrichtendiensten sowie mit der Zivilgesellschaft zusammenzuarbeiten, um geeignete faktische und rechtliche Schutzmechanismen zu identifizieren[44].

38 Resolution 68/167 vom 18. Dezember 2013, unter dem folgenden Link auf Französisch verfügbar: www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167.
39 UNHCHR «Das Recht auf Privatheit im digitalen Zeitalter», 2014.
40 A/HRC/31/64.
41 A/HRC/34/60.
42 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9 und Ziff. 46(f).
43 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 50.
44 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 15 und Ziff. 46(e).

Der zweite Bericht konzentriert sich auf die nationalen und internationalen Massnahmen zur staatlichen Überwachung. Er beschreibt die jüngsten Entwicklungen und Tendenzen und skizziert eine Reihe von Möglichkeiten zur Kontrolle der Überwachung. Er schlägt insbesondere die Schaffung eines internationalen Instruments zum Schutz der Privatsphäre im Cyberspace vor. Der Sonderberichterstatter betrachtet seine Forderungen als Ergänzung zu den bestehenden Instrumenten (wie z. B. dem Übereinkommen vom 13. November 2001[45] über die Cyberkriminalität) und den verschiedenen Vorstössen auf internationaler Ebene[46].

Die Schweiz verfolgt diese Entwicklungen aufmerksam.

1.2.5 OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten

Der wirtschaftlichen Ausrichtung der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) entsprechend dienen die ursprünglich aus dem Jahr 1980 stammenden und im Jahr 2013 revidierten Datenschutz-Richtlinien[47] primär der Harmonisierung der unterschiedlichen nationalen Datenschutzniveaus. Die Richtlinien sollen – unter Wahrung der Menschenrechte – eine Basis für die Regulierung des internationalen Datenaustauschs schaffen, um wirtschaftliche Handelshemmnisse zu vermeiden und den freien globalen Datenaustausch und Informationsfluss zu gewährleisten. Obwohl den Datenschutz-Richtlinien blosser Empfehlungscharakter zukommt und sie rechtlich nicht verbindlich sind, hatten sie nachhaltigen Einfluss auf die Entwicklung des Datenschutzrechts auf internationaler und nationaler Ebene.

Der Anwendungsbereich der Datenschutz-Richtlinie erstreckt sich auf alle Daten aus dem öffentlichen und privaten Sektor, die aufgrund der Art ihrer Verarbeitung, ihrer Natur oder der Umstände, unter denen sie genutzt werden, eine Gefahr für die Privatsphäre und andere individuelle Freiheiten bedeuten. Mit acht datenschutzrechtlichen Grundprinzipien, die als Minimalstandards konzipiert sind, soll ein Gleichgewicht zwischen den beiden konkurrierenden Konzepten der Privatsphäre und des freien Informationsflusses hergestellt werden (d. h. begrenzte Datenerhebung, Datenqualität, Zweckbestimmung, Nutzungsbegrenzung, Datensicherheit, Transparenz, Mitspracherecht der Betroffenen und Verantwortlichkeit).[48] Die revidierten Datenschutz-Richtlinien traten im Juli 2013 in Kraft und enthalten, unter Beibehaltung dieser acht datenschutzrechtlichen Grundprinzipien, verschiedene Präzisierungen

45 SR **0.311.43,** von der Schweiz ratifiziert am 21. September 2011.
46 Siehe zum Beispiel das «MAPPING-project»; www.mappingtheinternet.eu/.
47 OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten, 1980, online abrufbar unter: www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten, 2013, online abrufbar unter: www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.
48 OECD, Datenschutz-Richtlinien 1980, Grundsätze 6–14; OECD, Privacy Framework 2013, S. 22 und S. 47 f.

und Erweiterungen; so wurden u. a. die Kriterien für Datenübermittlungen ins Ausland präziser definiert und die internationale Zusammenarbeit verstärkt.[49] Die revidierten Datenschutz-Richtlinien sehen neu explizit vor, dass Datenhauptverantwortliche stets für die unter ihrer Kontrolle stehenden Personendaten verantwortlich sind, dies ungeachtet des Standorts der Daten.[50] Ferner soll der grenzüberschreitende Datenaustausch zwischen Teilnehmerstaaten und anderen Staaten nicht beschränkt werden, wenn letztere die Datenschutz-Richtlinien befolgen oder wenn ausreichende Garantien vorhanden sind, die das von den Datenschutz-Richtlinien verlangte Schutzniveau gewährleisten.

1.3 Ziele der Vorlage

Die Vorlage beruht auf dem Auftrag des Bundesrates an das EJPD, unter Berücksichtigung der Schlussfolgerungen des Berichts vom 29. Oktober 2014 mit dem Titel «Normkonzept zur Revision des Datenschutzgesetzes» sowie der Reformen des Europarats und der Europäischen Union einen Vorentwurf für das DSG zu erarbeiten. Darüber hinaus gehört die Verabschiedung der Botschaft zu den Zielen des Bundesrates für das Jahr 2017 und ist Teil der Legislaturplanung 2015–2019 (vgl. Ziff. 12.1). Sie setzt eine grosse Zahl der parlamentarischen Vorstösse um, die unter Ziffer 1.1.4 aufgeführt sind.

Mit dem Gesetzesentwurf werden verschiedene Ziele verfolgt, die sich gegenseitig ergänzen.

Zunächst dient die Vorlage der Anpassung des schweizerischen Rechts an die rasante technologische Entwicklung, die erhebliche Auswirkungen auf den Datenschutz hat. Dabei soll erstens den betroffenen Personen ermöglicht werden, die Kontrolle über ihre Daten wiederzuerlangen. Diese werden im Zusammenhang mit der Entwicklung der digitalen Gesellschaft in sehr grosser Zahl beschafft («Big Data»). Zudem wird deren Bearbeitung immer intransparenter (z. B. Profiling auf der Basis von Algorithmen). Zweitens soll die Eigenverantwortung der Verantwortlichen gefördert werden. Insbesondere sollen sie die Datenschutzvorschriften bei neuen Datenbearbeitungen bereits bei der Planung berücksichtigen und standardmässig diejenige Lösung vorsehen, die am datenschutzfreundlichsten ist. Schliesslich geht es drittens darum, die Wettbewerbsfähigkeit der Schweiz zu erhalten und zu stärken, indem ein günstiges Umfeld geschaffen wird, mit dem der grenzüberschreitende Datenverkehr erleichtert und die Attraktivität unseres Landes für neue Aktivitäten im Zusammenhang mit der digitalen Gesellschaft gesteigert werden können. Dies lässt sich nur mit einem hohen, auf internationaler Ebene anerkannten Schutzniveau verwirklichen.

Weitere Zielsetzungen der Revision ergeben sich aus den Entwicklungen des Rechts der Europäischen Union. Diesen kommt im Bereich des Datenschutzes eine grosse Bedeutung zu, weil der grenzüberschreitende Datenverkehr alltäglich ist. Zum einen gehört die Richtlinie (EU) 2016/680 zum Schengen-Acquis, und die Schweiz ist

49 OECD, Datenschutz-Richtlinien 2013, Grundsätze 16–18, 19 Bst. g und 20–23.
50 OECD, Datenschutz-Richtlinien 2013, Grundsatz 16.

verpflichtet, ihre Gesetzgebung entsprechend anzupassen. Ebenfalls müssen mit der Vorlage die Empfehlungen umgesetzt werden, welche die Europäische Union im Jahr 2014 nach der Evaluation der Schweiz im Rahmen der Schengen-Assoziierungsabkommen abgegeben hat (vgl. Ziff. 1.2.2.3). Die europäischen Expertinnen und Experten haben der Schweiz namentlich empfohlen, dem Beauftragten Verfügungskompetenzen zu übertragen. Zum anderen soll die Schweiz weiterhin von einem Angemessenheitsbeschluss der Europäischen Kommission profitieren, mit dem ein angemessenes Datenschutzniveau anerkannt wird (vgl. Ziff. 1.2.2.2). Zu diesem Zweck soll die schweizerische Gesetzgebung an die Verordnung (EU) 2016/679 angenähert werden, ohne dass diese jedoch vollständig umgesetzt wird.

Im Rahmen der Revision soll schliesslich die schweizerische Gesetzgebung an den E-SEV 108 angepasst werden, denn es liegt im Interesse der Schweiz, das revidierte Übereinkommen zu ratifizieren, sobald es zur Unterzeichnung durch die Vertragsstaaten aufliegt. Dies gilt nicht zuletzt auch mit Blick auf den Angemessenheitsbeschluss der Europäischen Kommission, für den die Unterzeichnung des revidierten Übereinkommens von grosser Bedeutung ist. Da der Wortlaut dieses Abkommens grundsätzlich feststeht und sein Inhalt zu einem grossen Teil dem Inhalt der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 entspricht – wobei er weniger detailliert ist –, hat der Bundesrat beschlossen, die sich darauf beziehenden Erläuterungen vorwegzunehmen und in die vorliegende Botschaft zu integrieren.

Zusammenfassend soll durch die Verwirklichung dieser verschiedenen Ziele die schweizerische Gesetzgebung einerseits der aktuellen technischen Entwicklung angepasst werden. Andererseits soll sichergestellt werden, dass die Schweiz ihren Verpflichtungen durch das Schengen-Assoziierungsübereinkommen nachkommt, dass sie das revidierte Übereinkommen SEV 108 ratifizieren kann und dass die Europäische Kommission ihr in einem Angemessenheitsbeschluss erneut bescheinigt, dass sie zu den Drittstaaten mit einem angemessen Schutzniveau gehört. An diesem Beschluss hat insbesondere die Schweizer Wirtschaft ein erhebliches Interesse.

Die Vorlage führt damit zu einer Totalrevision des DSG (einschliesslich der Revision weiterer bereichsspezifischer Datenschutznormen) und einer Teilrevision der bereichsspezifischen Datenschutznormen, die für die polizeiliche und justizielle Zusammenarbeit im Rahmen der Schengen-Abkommen gelten.

1.4 Darstellung des E-DSG

1.4.1 Leitlinien der Revision

Die Revision orientiert sich an sieben Leitlinien, auf denen die verschiedenen Neuerungen beruhen.

Eine erste Leitlinie der Revision bildet der risikobasierte Ansatz. Der Revisionsentwurf orientiert sich konsequent an den potenziellen Risiken für die betroffenen Personen, denn die Gefahren für die Privatsphäre der betroffenen Personen hängen weitgehend von den Aktivitäten der verschiedenen Verantwortlichen und Auftragsbearbeiter ab. Dementsprechend sind beispielsweise die Pflichten von Verantwortlichen, deren Aktivitäten mit einem erhöhten Risiko verbunden sind (z. B. Unterneh-

men, deren Haupttätigkeit in der Datenbearbeitung besteht), strenger als jene von Verantwortlichen, deren Aktivitäten ein geringeres Risiko darstellen (z. B. Datenbearbeitungen, die auf eine Kundendatei ohne besonders schützenswerte Daten beschränkt sind).

Eine zweite Leitlinie ist der technologieneutrale Charakter der Revisionsvorlage. Wie das derzeit geltende Gesetz soll auch der E-DSG so weit wie möglich alle Technologien gleichberechtigt behandeln. Dadurch bleibt das Gesetz offen für weitere technologische Entwicklungen und verhindert keine Innovationen.

Die dritte Leitlinie besteht in der Modernisierung der Terminologie, insbesondere um die Vereinbarkeit mit dem Recht der Europäischen Union zu verbessern. So werden gewisse Begriffe aus dem europäischen Recht übernommen. Der Begriff «Inhaber der Datensammlung» wird durch den Begriff «Verantwortlicher» ersetzt. Der Begriff «Persönlichkeitsprofil», der eine schweizerische Besonderheit darstellt, wird durch den Begriff «Profiling» abgelöst. Der Begriff «besonders schützenswerte Personendaten» umfasst neu auch genetische und biometrische Daten.

Als vierte Leitlinie ist die Verbesserung des grenzüberschreitenden Datenverkehrs zu nennen. So wird die geltende Regelung für die grenzüberschreitende Bekanntgabe von Daten teilweise ausgebaut. Der Grundsatz, wonach Personendaten nicht ins Ausland bekannt gegeben werden dürfen, wenn kein angemessener Schutz gewährleitet ist, wird aufgrund der damit verbundenen Rechtsunsicherheit aufgehoben. Daten dürfen ins Ausland übermittelt werden, wenn der Bundesrat per Verordnung festgestellt hat, dass das empfangende Land oder internationale Organ einen angemessenen Datenschutz gewährleistet. Liegt kein solcher Beschluss vor, sieht der E-DSG verschiedene Möglichkeiten vor, mit denen ein geeigneter Schutz gewährleistet werden kann, sodass die Bekanntgabe ins Ausland dennoch möglich ist.

Eine fünfte, besonders bedeutsame Leitlinie der Revision ist die Stärkung der Rechte der betroffenen Personen. Diese erfolgt über verschiedene Instrumente, die den Betroffenen insgesamt erlauben sollen, ihre Daten besser zu kontrollieren und besser darüber bestimmen zu können. Genauer festgelegt werden insbesondere die Voraussetzungen für die gültige Einwilligung der betroffenen Person.

Eng mit der fünften verbunden ist die sechste Leitlinie, wonach die Pflichten der Verantwortlichen präzisiert und stärker auf den Schutz der betroffenen Person ausgerichtet werden. Die Informationspflicht ist im Entwurf umfassender ausgestaltet. Die Verantwortlichen werden auch dazu verpflichtet, bei gewissen Arten von Bearbeitungen eine Datenschutz-Folgenabschätzung durchzuführen. Technische Vorkehren sollen für eine datenschutzfreundliche Ausgestaltung von Systemen sorgen. Diese Pflichten werden indessen durch gewisse Erleichterungen ausgeglichen. So soll die im privaten Sektor geltende Verpflichtung, dem Beauftragten die Datensammlungen zu melden, aufgehoben werden, was den Aufwand für die Verantwortlichen reduziert.

Die siebte Leitlinie ist die Stärkung der Kontrolle. So werden einerseits Stellung und Unabhängigkeit des Beauftragten gestärkt. Die Befugnisse des Beauftragten werden künftig mit den Befugnissen der entsprechenden ausländischen Kontrollbehörden vergleichbar sein. Anders als die meisten seiner Kolleginnen und Kollegen im europäischen Ausland wird er jedoch nicht befugt sein, Verwaltungssanktionen

auszusprechen. Dies wird ausgeglichen, indem andererseits mit dem E-DSG der strafrechtliche Teil ausgebaut wird.

1.4.2 Hauptsächliche Neuerungen

1.4.2.1 Änderung des Geltungsbereichs des künftigen DSG

Mit dem E-DSG wird vorgeschlagen, auf den Schutz der Daten juristischer Personen zu verzichten. In den datenschutzrechtlichen Bestimmungen der Europäischen Union und des Europarates sowie der meisten ausländischen Rechtsordnungen ist kein solcher Schutz vorgesehen. Der Schutz von Daten juristischer Personen ist nur von geringer praktischer Bedeutung. Wenn er aufgehoben wird, sollte dies keine negativen Auswirkungen haben, insbesondere mit Blick auf den Schutz, der durch andere spezifische Gesetze gewährleistet wird (Persönlichkeitsschutz, unlauterer Wettbewerb, Urheberrecht). Durch diese Änderung sollte die Bekanntgabe von Daten an ausländische Staaten, deren Gesetzgebung keinen Schutz von Daten juristischer Personen vorsieht, erleichtert werden.

Im Bereich der Datenbearbeitung durch Bundesorgane hätte die Aufhebung des Schutzes von Daten juristischer Personen zur Folge, dass die bundesrechtlichen Gesetzesgrundlagen, mit denen die Bundesorgane zur Bearbeitung von Personendaten ermächtigt werden, nicht mehr anwendbar wären, wenn diese Daten juristischer Personen bearbeiten. Nach Artikel 5 BV ist die Grundlage staatlichen Handelns jedoch das Recht. Des Weiteren unterstehen auch juristische Personen dem Schutz der Privatsphäre, selbst wenn sie nicht Trägerinnen sämtlicher Schutzgehalte gemäss Artikel 13 BV sind.[51] Der Bundesrat schlägt deshalb vor, für Bundesorgane im Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997[52] (RVOG) eine Reihe von Bestimmungen zu schaffen, die deren Umgang mit Daten juristischer Personen regeln (vgl. Ziff. 9.2.8). Ausserdem soll eine Übergangsbestimmung während fünf Jahren mögliche Rechtslücken verhindern (vgl. Art. 66 E-DSG sowie die Erläuterungen unter Ziff. 9.1.11).

1.4.2.2 Erhöhte Transparenz von Datenbearbeitungen und verstärkte Kontrolle durch die betroffenen Personen

Die Transparenz von Datenbearbeitungen soll erhöht werden. So wird die Informationspflicht bei der Datenbeschaffung auf alle Datenbearbeitungen durch private Verantwortliche ausgeweitet. Sie kann auf standardisierte Weise erfüllt werden, zudem sind Ausnahmen vorgesehen. Darüber hinaus führt die Vorlage eine Informationspflicht bei vollständig automatisierten Einzelentscheidungen ein sowie das Recht der betroffenen Person, in diesem Fall unter bestimmten Voraussetzungen ihren Standpunkt geltend zu machen und zu verlangen, dass eine natürliche Person die Entscheidung überprüft. Gemäss dem Gesetzesentwurf müssen der betroffenen

51 BGE **137** II 371 E. 6.
52 SR **172.010**

Person auch mehr Informationen vorgelegt werden, wenn diese ihr Auskunftsrecht geltend macht.

Die Rechte der betroffenen Personen werden in verschiedenen Punkten klarer definiert. Unter anderem ist im E-DSG ausdrücklich das Recht auf Löschung der Daten festgehalten, während dies im DSG nur implizit erwähnt ist. Ausserdem wird der gerichtliche Zugang erleichtert, indem Verfahren gegenüber privaten Verantwortlichen von den Gerichtskosten befreit werden.

In Berücksichtigung der Ergebnisse der Vernehmlassung sind die verschiedenen Pflichten der Verantwortlichen und die Rechte der betroffenen Personen überarbeitet worden, damit nicht strengere Anforderungen als im europäischen Recht gestellt werden.

1.4.2.3 Förderung der Selbstregulierung

Die Revision soll die Entwicklung der Selbstregulierung und die Eigenverantwortung der Verantwortlichen fördern. Angesichts der Vernehmlassungsergebnisse ist das System überarbeitet worden. Es ist nun vorgesehen, dass Berufs- und Wirtschaftsverbände, die Verhaltenskodizes erarbeiten, diese dem Beauftragten vorlegen können. Dieser nimmt dazu Stellung und veröffentlicht seine Stellungnahmen.

Mit den von den Branchen erarbeiteten Verhaltenskodizes können bestimmte Begriffe sowie die Modalitäten einiger Rechte und Pflichten präzisiert werden.

Diese Verhaltenskodizes entfalten keinen bindenden Charakter.

1.4.2.4 Stärkung der Stellung und Ausbau der Befugnisse und Aufgaben des Beauftragten

Die Stellung und die Unabhängigkeit des Beauftragten werden gestärkt. Diese oder dieser kann zwei Mal wiedergewählt werden. Sie oder er darf nur unter ganz bestimmten Bedingungen einer Nebenbeschäftigung nachgehen. Im Weiteren sieht der E-DSG vor, dass der Beauftragte – wie seine Kolleginnen und Kollegen in den anderen europäischen Ländern – nach Abschluss einer Untersuchung, die von Amtes wegen oder auf Anzeige hin eingeleitet wurde, Verfügungen erlassen kann, die für die Verantwortlichen und die Auftragsbearbeiter verbindlich sind. Nur das Bundesorgan bzw. die private Person, gegen das bzw. die die Untersuchung eingeleitet wurde sind in einem Untersuchungsverfahren Partei.

1.4.2.5 Ausbau der strafrechtlichen Sanktionen

Der strafrechtliche Teil des DSG wird in mehrfacher Hinsicht ausgebaut. Damit wird insbesondere der Umstand kompensiert, dass der Beauftragte im Gegensatz zu praktisch allen Datenschutzaufsichtsbehörden im europäischen Ausland nicht befugt ist, Verwaltungssanktionen zu verhängen. Der Höchstbetrag der Bussen wird auf

250 000 Franken erhöht; die Liste der strafbaren Verhaltensweisen wird an die neuen Pflichten der Verantwortlichen angepasst; es wird eine Übertretung bei Missachten von Verfügungen des Beauftragten oder Entscheiden der Rechtsmittelinstanzen eingeführt; der Beauftragte kann in Strafverfahren die Rechte einer Privatklägerschaft wahrnehmen; und die Verfolgungsverjährungsfrist bei Übertretungen wird verlängert. Bei Übertretungen, die in einem Unternehmen begangen werden, können die Strafverfolgungsbehörden unter bestimmten Voraussetzungen darauf verzichten, die Verantwortlichen strafrechtlich zu belangen. Stattdessen wird das Unternehmen zur Bezahlung der Busse verurteilt.

In das Strafgesetzbuch[53] (StGB) wird im Übrigen ein Artikel 179decies aufgenommen, der den Identitätsmissbrauch mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bedroht.

Das bereits im Vorentwurf vorgesehene Sanktionssystem (Art. 50 ff.) war in der Vernehmlassung Gegenstand zahlreicher Bemerkungen. Die Hauptkritik betrifft die Tatsache, dass die Strafbestimmungen in erster Linie die natürlichen Personen erfassen, während gemäss den Vernehmlassungsteilnehmern ausschliesslich die Unternehmen über Verwaltungssanktionen des Beauftragten (oder einer zu diesem Zweck geschaffenen Kommission) sanktioniert werden sollten. Es wird befürchtet, dass einfache Angestellte ohne Entscheidungsbefugnisse verurteilt werden. Ebenfalls von vielen Seiten kritisiert wurden die Strenge der Sanktionen, insbesondere die Höhe der Bussen, die mangelnde Präzisierung bestimmter Straftatbestände und der Katalog der strafbaren Handlungen sowie die Tatsache, dass fahrlässiges Handeln ebenfalls unter Strafe steht.

In der Vorlage wird diese Kritik aufgenommen, indem der Katalog der strafbaren Handlungen und die Höhe der Bussen gegenüber dem Vorentwurf reduziert werden und fahrlässiges Handeln nicht mehr bestraft wird.

Der Bundesrat verzichtet hingegen darauf, dass Unternehmen direkt durch Verwaltungssanktionen bestraft werden können. Er ist der Ansicht, dass die Einführung solcher Sanktionen im DSG nicht angemessen ist, denn Verwaltungsstrafen, die Sanktionscharakter haben, müssen die Ausnahme und auf Sektoren beschränkt bleiben, in denen die Zielgruppe beschränkt ist (namentlich Kartelle, Geldspiele). Mangels spezifisch auf solche Sanktionen anwendbarer Verfahrensgrundsätze besteht die Gefahr, dass die Verfahrensgarantien zum Schutz der fehlbaren Personen verletzt werden.

Es besteht kein Grund zur Befürchtung, dass jede Angestellte oder jeder Angestellte eines Unternehmens, das Personendaten bearbeitet, bestraft werden könnte. Die Mehrheit der strafbaren Verhaltensweisen betreffen den Verantwortlichen. Handelt es sich dabei um eine juristische Person, wird die Straftat gemäss Artikel 29 StGB der Vertreterin oder dem Vertreter des Geschäftsorgans zugerechnet. Dies gilt insbesondere betreffend die Missachtung einer Verfügung des Beauftragten: in diesem Fall macht sich diejenige Person strafbar, die innerhalb des Unternehmens hätte dafür sorgen müssen, dass der Verfügung des Beauftragten Folge geleistet werde. Der Entwurf stärkt zudem die Verantwortung der leitenden Organe, indem Artikel 6

53 SR **311.0**

des Bundesgesetzes vom 22. März 1974[54] über das Verwaltungsstrafrecht (VStrR) für anwendbar erklärt wird (Widerhandlungen in Geschäftsbetrieben). Schliesslich sieht der Entwurf vor, dass der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden kann, wenn diese sich auf nicht mehr als 50 000 Franken beläuft und die Ermittlung der strafbaren Personen Untersuchungsmassnahmen bedingen würden, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.

1.5 Darstellung der Revision anderer Bundesgesetze

In den bereichsspezifischen Datenschutznormen für die polizeiliche und justizielle Zusammenarbeit im Rahmen der Schengen-Abkommen wird im Gesetzesentwurf neu unter anderem die Pflicht der zuständigen Behörde vorgesehen, nach Möglichkeit zwischen verschiedenen Kategorien von betroffenen Personen zu unterscheiden. Ebenfalls sind Daten, die auf Tatsachen aufbauen, von solchen abzugrenzen, die auf persönlichen Einschätzungen beruhen. Gestärkt werden auch die Rechte der betroffenen Personen. Diese können unter bestimmten Voraussetzungen vom Beauftragten verlangen, dass er die Rechtmässigkeit der Bearbeitung von Daten über sie prüft. Bei unrechtmässigen Bearbeitungen ihrer Daten können sie vom Beauftragten überdies die Einleitung einer Untersuchung fordern, die gegebenenfalls zu einer einsprachefähigen Verfügung führt. Schliesslich regelt der Gesetzesentwurf den Datenschutz bei der Bekanntgabe von Daten zwischen Schengen-Staaten oder zwischen einer schweizerischen Behörde und einem Drittstaat im Rahmen der justiziellen und polizeilichen Schengen-Zusammenarbeit.

1.6 Beurteilung der gewählten Lösung

1.6.1 Beurteilung der Vernehmlassungsergebnisse

Insgesamt sind im Rahmen der Vernehmlassung 222 Stellungnahmen eingegangen.[55] Von den offiziell zur Vernehmlassung eingeladenen Teilnehmern haben drei der eidgenössischen Gerichte, alle Kantone, sieben politische Parteien, der Städteverband und 11 Organisationen eine Stellungnahme eingereicht. Im Übrigen haben sich 178 Teilnehmer der interessierten Kreise zum Vernehmlassungsentwurf geäussert.

Es ist kein Vernehmlassungsteilnehmer grundsätzlich gegen eine neue Regelung des Datenschutzes. Eine Mehrheit der Teilnehmer heisst die Regelung ausdrücklich gut. Die Übernahme der Richtlinie (EU) 2016/680 und der Anforderungen des E-SEV 108 ist unbestritten.

Praktisch alle Teilnehmer haben Bemerkungen angebracht. Sie betreffen fast ausschliesslich den VE-DSG. Es lassen sich zwei grobe Tendenzen ableiten. Für die Mehrheit führt der Vorentwurf zu einem zu hohen Verwaltungsaufwand und geht in

54 SR **313.0**

55 Der Bericht über die Vernehmlassungsergebnisse kann auf der Webseite des BJ eingesehen werden: www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html.

einigen Punkten, hauptsächlich in Bezug auf die Pflichten der Verantwortlichen, unnötigerweise über die europäischen Anforderungen hinaus. Andere wiederum sind der Ansicht, dass die Vorlage nicht weit genug geht und zusätzliche Massnahmen zur Verstärkung des Schutzes der betroffenen Personen umfassen sollte.

Die wesentlichen Bemerkungen lauten wie folgt:

- Terminologie: Im VE-DSG sollte die Rechtsterminologie modernisiert werden, indem bestimmte europäische Begriffe übernommen werden. Von einer Mehrheit der Teilnehmer besonders begrüsst werden die Aufhebung des Begriffs des Persönlichkeitsprofils und die Einführung des Begriffs «Profiling». Die meisten vertreten jedoch die Meinung, dass dessen Definition (Art. 3 Bst. f VE-DSG) zu weit gefasst ist und an das europäische Recht angelehnt werden sollte.
- Pflichten der Verantwortlichen und Rechte der betroffenen Personen: Die verschiedenen Pflichten der Verantwortlichen, insbesondere die Pflicht zur Meldung an den Beauftragten, werden von vielen Teilnehmern aus der Wirtschaft als zu bürokratisch eingestuft. Für die kleinen und mittleren Unternehmen sei es schwierig, den Pflichten nachzukommen, da sie keinen angemessenen Rechtsdienst und keine Mittel dafür hätten. Das betrifft im Wesentlichen die Bekanntgabe ins Ausland (Art. 5 und 6 VE-DSG), die Informationspflichten (Art. 13, 14 und 15 VE-DSG) und die Datenschutz-Folgenabschätzung (Art. 16 VE-DSG). In einigen Punkten gehe der VE-DSG im Übrigen ohne Grund weiter als die Anforderungen im europäischen Recht.
- Selbstregulierung: Die Absicht des Bundesrates, die Selbstregulierung zu fördern, wird unterstützt. Das System der Empfehlungen der guten Praxis nach den Artikeln 8 und 9 VE-DSG überzeugt hingegen nicht. Breite Kreise der Wirtschaft lehnen es ab, dass der Beauftragte selbst die Initiative ergreifen kann, um solche Empfehlungen zu erlassen. Sie sind der Auffassung, dass dies ausschliesslich den Branchen obliegen sollte, da diese die Eigenheiten ihres Sektors besser kennen. Da die Behörden die Empfehlungen des Beauftragten in der Praxis befolgten, erhalte dieser ausserdem praktisch den Status eines Gesetzgebers, ohne jedoch demokratisch legitimiert zu sein. Ebenfalls kritisiert wird die Genehmigung der Empfehlungen der Branchen durch den Beauftragten. Dies namentlich deshalb, weil keine Rechtsmittel ergriffen werden können. Gemäss einigen Teilnehmern wird das Instrument der Empfehlungen der guten Praxis nichts nützen, da es nicht verbindlich sei. Andere schliesslich äussern die Meinung, dass der Beauftragte in der Praxis gar nicht die Ressourcen habe, um wirksame Empfehlungen zu erarbeiten. So würden die Artikel 8 und 9 VE-DSG zum Papiertiger.

  Eine Reihe von Vernehmlassungsteilnehmern bedauert es, dass die Möglichkeit, Datenschutzberaterinnen und Datenschutzberater zu ernennen, im VE-DSG nicht mehr erwähnt wird. Die Wirtschaftskreise wünschen diesbezüglich, dass die Verantwortlichen, die eine solche Stelle geschaffen haben, von administrativen Erleichterungen profitieren.

– Stellung und Ernennung der oder des Beauftragten: Einige Teilnehmer lehnen das Ernennungsverfahren ab und fordern, dass die oder der Beauftragte unmittelbar und ausschliesslich vom Parlament ernannt wird. Einige Kantone wünschen darüber hinaus, dass sie oder er über ein eigenes Budget verfügt. Die Beschränkung der Amtsdauer der oder des Beauftragten sowie das Verbot, in einem Kanton oder einer Gemeinde einer Nebenbeschäftigung nachzugehen, werden vor allem von einigen Kantonen in Frage gestellt. Schliesslich sind viele Teilnehmer aus den Wirtschaftskreisen gegen die stille Wiederernennung der oder des Beauftragten, die allerdings bereits im geltenden Recht so vorgesehen ist.

– Strafregime: Die Strafbestimmungen des VE-DSG (Art. 50 ff.) waren im Vernehmlassungsverfahren Gegenstand umfassender Kritik. Viele Teilnehmer verlangen, dass das vorgesehene System komplett überarbeitet wird. Die Hauptkritik richtet sich dagegen, dass die strafrechtlichen Sanktionen in erster Linie die natürlichen Personen erfassen, während sie gemäss den Teilnehmern administrativen Charakter haben und vom Beauftragten (oder von einer eigens geschaffenen Kommission) direkt gegenüber den Unternehmen verhängt werden können sollten. Es wird befürchtet, dass einfache Angestellte ohne Entscheidungsbefugnis verurteilt werden.

  Die Kantone sind zudem mehrheitlich dagegen, dass die Kantone weiterhin die Kompetenz haben, die Straftaten zu verfolgen und zu beurteilen. Sie befürchten, dass die Anzahl der Verfahren aufgrund der zahlreichen strafbaren Handlungen und der strengeren Sanktionen steigen wird und dass dafür zusätzliches Fachpersonal eingestellt werden muss.

  Die Strenge der Sanktionen, insbesondere die Höhe der Bussen, die mangelnde Präzisierung bestimmter Tatbestände und der Katalog der strafbaren Handlungen waren ebenfalls Gegenstand breiter Kritik.

  Verschiedene Teilnehmer der Wirtschaftskreise schlagen eine Änderung vor. Sie basiert im Wesentlichen auf einem System von Verwaltungssanktionen gegenüber Unternehmen, die von einer «Datenschutzkommission» verhängt werden. Die Kommission könnte dem EDI oder dem EJPD angegliedert werden. Der Katalog der Sanktionen sollte sich so weit wie möglich an jenen der Verordnung (EU) 2016/679 anlehnen, aber nicht darüber hinausgehen. Abweichend von der Verordnung, in der Bussen bis zu mehreren Millionen Euro vorgesehen sind, sollte die Höhe der Bussen gemäss dem Vorentwurf auf maximal 500 000 Franken beschränkt sein.

1.6.2 Wesentliche Änderungen gegenüber dem Vorentwurf

1.6.2.1 Wesentliche Änderungen in Bezug auf den E-DSG

Nach der Vernehmlassung ist der E-DSG hauptsächlich in folgenden Punkten angepasst worden:

- Die Systematik des Gesetzes wurde aufgrund der Vernehmlassungsergebnisse in verschiedener Hinsicht überarbeitet.
- Einige Ausnahmen vom Geltungsbereich des E-DSG wurden angepasst. Die Ausnahme betreffend die Bearbeitung im Rahmen der Verfahren vor den eidgenössischen Gerichten oder anderen eidgenössischen Justizbehörden wurden ebenfalls überarbeitet. Im E-DSG werden ferner die Bundesbehörden aufgeführt, die von der Aufsicht des Beauftragten ausgenommen sind. An der Aufhebung der Ausnahme betreffend die öffentlichen Register des Privatrechtsverkehrs hingegen wurde festgehalten. Gemäss dem E-DSG werden allerdings der Zugang zu diesen Registern und die Rechte der betroffenen Personen neu durch die Spezialbestimmungen des anwendbaren Bundesrechts geregelt.
- Die Definition des Profiling wird an das europäische Recht angepasst. Weiter wird eine Definition für die Verletzung der Datensicherheit eingefügt, weil dieser Begriff sich in der Vernehmlassung als sehr unklar erwies.
- Die Bestimmung zur Datensicherheit wird präzisiert, weil ihr Anwendungsbereich sehr unklar schien. Auch die Norm betreffend Meldungen von Verletzungen der Datensicherheit wird angepasst. Es sind nun verschiedene Ausnahmen vorgesehen und es ist sichergestellt, dass die Norm nicht gegen das Verbot verstösst, sich selbst belasten zu müssen.
- Aufgrund der Vernehmlassung wird eine Bestimmung zur Datenschutzberaterin bzw. zum Datenschutzberater eingefügt und unter bestimmten Voraussetzungen eine Erleichterung von der Meldepflicht für Datenschutz-Folgenabschätzungen vorgesehen.
- Zur Berücksichtigung der Kritik in der Vernehmlassung wurden die Empfehlungen der guten Praxis durch Verhaltenskodizes ersetzt, die ausschliesslich von den Berufs- und Wirtschaftsverbänden sowie den Bundesorganen erarbeitet werden können. Diese können sie dem Beauftragten vorlegen, der dazu Stellung nimmt und die Stellungnahme veröffentlicht. Im Rahmen seiner Beratungstätigkeit kann der Beauftragte weiterhin wie heute Leitfäden und andere Hilfs- oder Arbeitsinstrumente erarbeiten.
- Anstelle einer allgemeinen Dokumentationspflicht wurde eine Bestimmung über ein Verzeichnis der Bearbeitungstätigkeiten eingefügt. Die Vernehmlassung hat ergeben, dass eine allgemeine Dokumentationspflicht zu wenig definiert ist.
- Die Regelung zur Bekanntgabe von Personendaten wurde unter Berücksichtigung der Vernehmlassungsergebnisse zum Teil überarbeitet. Der Grundsatz, wonach Personendaten nicht ins Ausland bekannt gegeben werden dür-

fen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, wurde aufgehoben, da er in systematischer Hinsicht zu Rechtsunsicherheit führt. Die Terminologie im Zusammenhang mit der Bekanntgabe von Daten ins Ausland vorbehaltlich geeigneter Garantien wurde an jene in der Verordnung (EU) 2016/679 angepasst. Die Ausnahmen bezüglich der Bekanntgabe von Personendaten in einen Staat, dessen Gesetzgebung keinen angemessenen Datenschutz gewährleistet, wurden ausserdem leicht gelockert. Schliesslich wurden lediglich die gemäss dem E-SEV 108 geforderten Pflichten, den Beauftragten zu informieren oder dessen Genehmigung einzuholen, beibehalten.

– Die Bestimmung betreffend die Daten einer verstorbenen Person wurde aufgrund der Vernehmlassung wesentlich neu formuliert. Sie erlaubt nun eine umfassende Interessenabwägung, und ein allfälliges Amts- und Berufsgeheimnis ist zu berücksichtigen. Aufgrund der Vernehmlassung wurde zudem der Willensvollstrecker eingefügt.

– Die Bestimmungen zur Informationspflicht und die Ausnahmen wurden präzisiert. Auch die spezifische Informationspflicht bei automatisierten Einzelentscheidungen ist verständlicher formuliert und es wurden drei Ausnahmen eingefügt.

– Die Schwelle für die Erstellung einer Datenschutz-Folgenabschätzung wurde angehoben und es sind Ausnahmen vorgesehen. Aufgrund der Vernehmlassung wurde die Reaktionsfrist des Beauftragten gekürzt.

– Die Bestimmungen zum Auskunftsrecht wurden aufgrund der Vernehmlassung leicht angepasst. Die Ausnahmen sind nun ohne inhaltliche Änderung explizit aufgeführt.

– Die Fälle, in denen für die Bearbeitung von Personendaten durch die Bundesorgane eine formell-gesetzliche Grundlage erforderlich ist, wurden angepasst. Abweichend vom Vorentwurf ist gemäss dem E-DSG eine Grundlage in einem Gesetz im formellen Sinn erforderlich, wenn der Zweck oder die Art und Weise der Bearbeitung einen schwerwiegenden Eingriff in die Grundrechte der betroffenen Person mit sich bringen kann. Die Anforderung einer formell-gesetzlichen Grundlage ist im ersten Fall (Bearbeitungszweck) nötig aufgrund der Aufhebung des Begriffs «Persönlichkeitsprofil» und demzufolge auch der Aufhebung der Anforderung einer formell-gesetzlichen Grundlage für diese Art von Bearbeitung. Ein schwerwiegender Eingriff in die Grundrechte der betroffenen Person kann auch durch die Art und Weise der Bearbeitung entstehen, beispielsweise durch gewisse automatisierte Einzelentscheidungen. Folglich sieht der Entwurf in diesem Fall die Anforderung einer formell-gesetzlichen Grundlage vor. Die Anforderungen an die Normstufe bleiben für die Bearbeitung von besonders schützenswerten Personendaten und das Profiling hingegen unverändert im Vergleich zum Vorentwurf.

– Das Recht der betroffenen Person, von einem Bundesorgan die Einschränkung der Bearbeitung von Personendaten über sie zu verlangen, wurde gestrichen. Gemäss dem E-DSG ist die Einschränkung der Bearbeitung für das

Bundesorgan unter bestimmten Voraussetzungen eine Alternative zur Löschung oder Vernichtung der Daten.

– Anders als im VE-DSG, wonach der Beauftragte entscheiden konnte, ob er eine Untersuchung einleitet oder nicht, ist er gemäss dem E-DSG nun dazu verpflichtet. Er kann nur dann von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist.

– Der Katalog der Verwaltungsmassnahmen, die der Beauftragte anordnen kann, wurde ergänzt. Die Verfügungskompetenzen des Beauftragten werden durch diese Änderung nicht erweitert. Es wird lediglich präzisiert, dass der Beauftragte verfügen kann, dass der Verantwortliche bestimmte Pflichten wie die Informations- oder Meldepflichten beachtet. Schliesslich erhält der Beauftragte im Vergleich zum VE-DSG neu die Kompetenz, unter bestimmten Voraussetzungen eine Verwarnung auszusprechen.

– Anders als der VE-DSG sieht der E-DSG nicht mehr vor, dass Beschwerden gegen vorsorgliche Massnahmen des Beauftragten keine aufschiebende Wirkung zukommt. Es gelten nun die allgemeinen Bestimmungen des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968[56] (VwVG).

– Die Regelung der Amtshilfe zwischen dem Beauftragten und den ausländischen Behörden, die für den Datenschutz zuständig sind, wurde verschärft.

– Gemäss dem E-DSG ist der Beauftragte neu verpflichtet, gegenüber privaten Personen für bestimmte gesetzliche Aufgaben Gebühren zu erheben.

– Das System der strafrechtlichen Sanktionen wurde auf Grundlage der Stellungnahmen in der Vernehmlassung überarbeitet. Die Bussenobergrenze wurde auf 250 000 Franken gesenkt. Die Liste der strafbaren Verhaltensweisen wurde gekürzt und konzentriert sich nun auf die Verletzung wesentlicher Pflichten des Verantwortlichen. Die Verletzung der beruflichen Schweigepflicht ist wieder eine Übertretung und die Bekanntgabe von Daten, die zu kommerziellen Zwecken bearbeitet wurden, ist nicht mehr erfasst. Um der fehlenden direkten Strafbarkeit des Unternehmens entgegenzuwirken, sieht der Bundesrat vor, die strafrechtliche Verantwortlichkeit der leitenden Organe durch die Anwendung von Artikel 6 VStrR zusätzlich zu Artikel 29 StGB zu verschärfen. Zudem sieht er die Einführung einer Strafe wegen Missachtens von Verfügungen des Beauftragten vor, welche es erleichtert, die leitende Person innerhalb des Unternehmens zu identifizieren und zu verurteilen, die für die Einhaltung der Verfügung verantwortlich war. Zusammen mit der bereits im Vorentwurf enthaltenen Möglichkeit, auf die Verfolgung der verantwortlichen natürlichen Personen zu verzichten und stattdessen direkt das Unternehmen zu belangen, wenn die Busse 50 000 Franken nicht übersteigt und die Untersuchungsmassnahmen im Hinblick auf die verwirkte Strafe unverhältnismässig wären, können zwar nicht die Unternehmen selbst stärker zur Verantwortung gezogen werden, dafür aber deren leitende Personen.

56 SR **172.021**

– Die Übergangsregelung betreffend die Pflichten der Verantwortlichen wurde auf weitere Pflichten ausgedehnt.

1.6.2.2 Wesentliche Änderungen in Bezug auf die anderen Bundesgesetze

Die Bundesgesetze im Anhang des E-DSG wurden hauptsächlich in folgenden Punkten angepasst:

– Die Gesetzesgrundlagen für die Bearbeitung von Persönlichkeitsprofilen durch Bundesorgane wurden aufgehoben oder geändert.

– Abweichend vom Vorentwurf wurden im Gesetzesentwurf die Spezialbestimmungen zur Bekanntgabe von Personendaten ins Ausland an die Artikel 13 und 14 E-DSG angepasst, damit eine einheitliche bundesrechtliche Regelung gewährleistet ist.

– Der Gesetzesentwurf führt im RVOG eine Reihe von Gesetzesbestimmungen ein, welche für Bundesorgane den Umgang mit Daten juristischer Personen regeln. Denn aufgrund der Aufhebung des Schutzes der Daten juristischer Personen im E-DSG sind die bundesrechtlichen Gesetzesgrundlagen für die Bearbeitung von Personendaten durch Bundesorgane nicht mehr anwendbar, wenn diese Daten juristischer Personen bearbeiten. So werden die Artikel 5, 13 Absatz 2 und 36 BV gewahrt.

1.6.2.3 Wesentliche Änderungen in Bezug auf die Bundesgesetze zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680

Das neue Kapitel zum Schutz von Personendaten im Rechtshilfegesetz vom 20. März 1981[57] (IRSG) wird zum Teil angepasst. Im Vergleich mit dem in der Vernehmlassung unterbreiteten Vorentwurf wird die Informationspflicht gestrichen, da die Transparenz der Bearbeitung von Personendaten durch das Gesetz gewährleistet wird. Die Rechte der betroffenen Personen hingegen werden neu geregelt – einerseits zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680, andererseits zur Berücksichtigung der Ausnahme in Artikel 2 Absatz 3 E-DSG.

1.6.3 Nicht berücksichtigte bedeutende Bemerkungen aus der Vernehmlassung

Einige Vernehmlassungsteilnehmer fordern, dass sich der Datenschutz in der Schweiz am Grundsatz des «opt-in» orientiert, d. h. dass die Bearbeitung von Personendaten nur dann erfolgen darf, wenn die betroffene Person ausdrücklich zustimmt.

57 SR **351.1**

Gemäss verschiedenen Teilnehmern ist es bedauernswert, dass der VE-DSG nicht wie die Verordnung (EU) 2016/679 ein Recht auf Datenportabilität umfasst. Dieses Recht gewährleistet, dass die betroffene Person die über sie bearbeiteten Daten in einem Standardformat zurückerhalten und an einen anderen Anbieter übertragen kann. Aus Sicht der Teilnehmer wäre dadurch eine bessere Kontrolle über die Daten sichergestellt. Zudem könnten die Wiederverwendung der Daten und die Entwicklung neuer Dienstleistungen gefördert werden. Andere Teilnehmer begrüssen den Entscheid des Bundesrates dagegen ausdrücklich, weil ein solches Recht nicht direkt auf den Persönlichkeitsschutz ausgerichtet ist und sehr kostenintensiv wäre.

Einige Teilnehmer wünschen, dass die Beweislast zugunsten der betroffenen Person umgekehrt wird, sodass in Gerichtsverfahren der Verantwortliche nachweisen muss, dass er die Daten rechtmässig bearbeitet. Einzelne Teilnehmer begrüssen es demgegenüber explizit, dass die Beweislast nicht umgekehrt worden ist.

Verschiedene Teilnehmer bedauern, dass im VE-DSG keine Instrumente vorgesehen sind, mit denen die betroffenen Personen ihre Rechte kollektiv durchsetzen können. Andere Teilnehmer begrüssen diese Lösung hingegen ausdrücklich.

Einzelne Teilnehmer fordern, dass Bonitätsdatensammlungen verboten werden. Solche Datensammlungen, die Informationen über die Bonität privater Personen enthalten, könnten das Privatleben dieser Personen stark beeinträchtigen. Die Informationen in diesen Datensammlungen seien oft falsch, und das Verfahren zur Beantragung der Löschung und Vernichtung der Daten sei oft intransparent oder gar nicht vorhanden. Gemäss anderen Teilnehmern sollte zumindest überprüft werden, ob nicht eine Verschärfung des Gesetzes gegenüber Unternehmen, die Bonitätsdatensammlungen bearbeiten, angemessen wäre. Vgl. hierzu das Postulat Schwaab 16.3682 «Die Tätigkeiten von Wirtschaftsauskunfteien einschränken», in dessen Rahmen der Bundesrat zu prüfen beabsichtigt, ob eine spezifische Regelung der Tätigkeiten der Wirtschaftsauskunfteien zweckmässig ist und welche rechtlichen Lösungen in Frage kämen.

Einige Teilnehmer sind der Ansicht, dass das DSG auch für Unternehmen gelten sollte, die ihren Sitz nicht in der Schweiz haben, die aber Datenbearbeitungen mit Auswirkungen in der Schweiz vornehmen. Diese Unternehmen sollten namentlich eine Vertretung in der Schweiz haben.

Diverse Teilnehmer sind der Meinung, dass ein Recht auf Vergessen vorgesehen werden sollte. Dabei handelt es sich um einen wichtigen Aspekt des europäischen Rechts, der im VE-DSG nicht enthalten ist. Andere Teilnehmer heissen es demgegenüber gut, dass dieses Recht im VE-DSG nicht ausdrücklich erwähnt wird, da es bereits aus der geltenden Regelung abgeleitet werden kann.

1.6.4 Bewertung des Gesetzesentwurfs

Die Vorlage löst das DSG von 1992 ab. Sie soll einerseits eine bessere Antwort auf die Herausforderungen aufgrund der neuen Technologien bieten und andererseits den Anforderungen des europäischen Rechts Rechnung tragen. Die bewährten Regelungen und Grundsätze werden so weit wie möglich übernommen. Der Bund

erhält keine neuen Kompetenzen, sodass die Kantone in Bezug auf die Datenbearbeitung durch kantonale Organe unter Vorbehalt der europäischen Anforderungen und der materiellen bereichsspezifischen Datenschutzbestimmungen des Bundesrechts weiterhin souverän sind. Die Vorlage aktualisiert die Terminologie, fördert die Selbstregulierung, verschärft die Pflichten der Verantwortlichen und stärkt die Rechte der betroffenen Personen; sie verleiht dem Beauftragten neue Befugnisse und baut den strafrechtlichen Teil des Gesetzes aus. Die Änderungen schaffen einen klareren rechtlichen Rahmen, der mit dem Innovationsbedarf vereinbar ist und die internationale Wettbewerbsfähigkeit der Schweiz wahrt.

Durch die Vorlage werden zum Teil auch die spezifischen Gesetze zur Schengen-Zusammenarbeit revidiert. Für die Schweiz geht es dabei darum, ihre Verpflichtungen gegenüber der Europäischen Union einzuhalten.

Der Entscheid für eine umfassende Vorlage, die eine Totalrevision des DSG und Änderungen in zahlreichen anderen Gesetzen beinhaltet, hat sich aufgedrängt, da es sehr kompliziert gewesen wäre, bestimmte Anforderungen der Richtlinie (EU) 2016/680 ausschliesslich für bestimmte Datenbearbeitungen umzusetzen (z. B. Verfügungskompetenzen des Beauftragten). Dank dieser Lösung kann eine kohärente Gesetzgebung geschaffen werden, die einen klaren allgemeinen Rahmen für den Datenschutz bildet und so breit wie möglich anwendbar ist.

1.7 Weitere geprüfte Massnahmen

Im Rahmen seiner Arbeiten hat der Bundesrat weitere Massnahmen geprüft, aber schliesslich beschlossen, diese nicht in die Vorlage aufzunehmen. Einige dieser Massnahmen sind auch in der Vernehmlassung vorgeschlagen worden (vgl. Ziff. 1.6.1). Dabei handelt es sich namentlich um die folgenden Massnahmen.

1.7.1 Erlass verbindlicher Datenschutzvorschriften durch den Beauftragten

Die Möglichkeit, den Beauftragten zum Erlass verbindlicher Datenschutzvorschriften zu ermächtigen, wurde im Stadium des Vorentwurfs fallen gelassen. Diese Lösung hätte zwar den Vorteil gehabt, dass der Beauftragte seine Adressaten direkt verpflichten könnte. Doch sie hätte zu zahlreichen Problemen im Zusammenhang mit dem Legalitätsprinzip geführt (Delegation von Kompetenzen an den Beauftragten, Regelungsdichte). Im Vergleich mit der Lösung, die mit dem Vorentwurf in der Vernehmlassung unterbreitet worden ist, d. h. den Empfehlungen der guten Praxis, wäre das Verfahren zum Erlass solcher Normen auch langsamer gewesen, da jeweils das Verfahren zum Erlass von Verordnungen der Bundesverwaltung hätte durchlaufen werden müssen. Im Übrigen hätte diese Möglichkeit den betroffenen Kreisen nur einen geringen Spielraum gelassen, was sich negativ auf die Einhaltung der fraglichen Vorschriften auswirken könnte.

1.7.2 Beweislastumkehr

Auf eine Beweislastumkehr nach dem Beispiel von Artikel 13*a* des Bundesgesetzes vom 19. Dezember 1986[58] über den unlauteren Wettbewerb (UWG) hat der Bundesrat verzichtet. Nach einer solchen Bestimmung könnte das Gericht von den Datenbearbeitenden im Einzelfall den Nachweis einer datenschutzkonformen Bearbeitung verlangen, wenn dies unter Berücksichtigung der berechtigten Interessen der am Verfahren beteiligten Parteien angemessen erscheint. Bereits heute sind die Zivilgerichte in der Lage, im Rahmen der freien Beweiswürdigung und der Mitwirkungsobliegenheiten der Parteien mit Beweisproblemen umzugehen. Ausserdem hat die Vernehmlassung zum FIDLEG[59] gezeigt, dass Vorschläge zur Beweislastumkehr auf starken Widerstand stossen. Der Beautragte hätte es jedoch vorgezogen, wenn eine Beweislastumkehr vorgesehen worden wäre.

1.7.3 Kollektive Rechtsdurchsetzung

Zur Umsetzung der Motion 13.3931 Birrer-Heimo erarbeitet der Bundesrat zurzeit einen Vorentwurf zu einem Gesetz, das die kollektive Rechtsdurchsetzung erleichtern soll. Der Vorentwurf wird für den privaten Bereich allgemein und folglich auch für den Datenschutz gelten. Der Bundesrat erachtet es hingegen nicht als opportun, im DSG eine besondere Regelung zur kollektiven Rechtsdurchsetzung einzuführen (wie beispielsweise eine Erweiterung des Verbandsklagerechts und die Einführung einer Sammelklage bzw. eines Sammelvergleichs[60]).

1.7.4 Recht auf Datenportabilität

Es wurde die Frage geprüft, ob ein Recht auf Datenportabilität der betroffenen Personen eingeführt werden soll, wie es in Artikel 20 der Verordnung (EU) 2016/679 vorgesehen ist. Das Recht auf Datenportabilität gibt der betroffenen Person die Möglichkeit, ihre Daten von einem System zur automatisierten Datenbearbeitung auf ein anderes System zu übertragen. Dieses Recht setzt voraus, dass die betroffene Person Daten, die sie einem Verantwortlichen zur Verfügung gestellt hat, in einem strukturierten, gebräuchlichen und maschinenlesbaren Format erhält. Doch nach Auffassung des Bundesrates ist dieses Recht mehr darauf ausgerichtet, den betroffenen Personen die Wiederverwendung ihrer Daten zu ermöglichen, um den Wettbewerb spielen zu lassen, als ihre Persönlichkeit zu schützen. Es scheint daher problematisch, eine entsprechende gesetzliche Regelungen zu erlassen. Ausserdem könnte die Umsetzung dieses Rechts schwierig sein, da es die gegenseitige Abstimmung unter den Verantwortlichen und zweifellos eine – zumindest implizite – Einigung über die verwendeten Datenträger und Informatikstandards voraussetzt. Die Regulierungsfolgenabschätzung hat zudem gezeigt, dass sich die Einführung eines

58 SR **241**
59 Vgl. die Botschaft des Bundesrates vom 4. November 2015 zum Finanzdienstleistungsgesetz (FIDLEG) und zum Finanzinstitutsgesetz (FINIG; BBl **2015** 8901).
60 Siehe Art. 101 ff. des Vorentwurfs zum FIDLEG.

Rechts auf Datenportabilität als sehr kostenintensiv erweisen könnte. Dies gilt insbesondere für Unternehmen mit über fünfzig Angestellten, die für die Anwendung dieses Rechts zusätzliches Personal anstellen müssten.

Der Bundesrat zieht es vor, die Ergebnisse der Erfahrungen innerhalb der Europäischen Union abzuwarten, bevor die Einführung eines Rechts auf Datenportabilität in Betracht gezogen wird. Die Frage wird jedoch im Rahmen der Strategie «Digitale Schweiz» weiter geprüft. Der Beauftragte hätte es vorgezogen, wenn das Recht auf Datenportabilität in die Gesetzesvorlage aufgenommen worden wäre.

1.7.5 Ausserparlamentarische Kommission für die Erarbeitung und Genehmigung von Empfehlungen der guten Praxis

Es wurde in Betracht gezogen, eine ausserparlamentarische Kommission mit der Erarbeitung und Genehmigung von Empfehlungen der guten Praxis zu beauftragen. Diese Lösung ist im Stadium des Vorentwurfs verworfen worden, da sie einen zusätzlichen Verwaltungsaufwand und weitere Kosten verursachen würde und bürokratischer wäre.

1.7.6 Änderung der Organisation der Aufsichtsbehörde

Es wurde in Betracht gezogen, die Funktion des Beauftragten als Kollegialbehörde auszugestalten. Schliesslich wurde jedoch beschlossen, die gegenwärtige Struktur beizubehalten. Diese ist unbürokratisch, einfach und gewährleistet eine rasche Entscheidfindung sowie einen guten Informationsfluss. Ausserdem ist sie in den Kantonen und in zahlreichen europäischen Ländern (Deutschland, Spanien, Polen) gut etabliert.

1.7.7 Einrichtung spezieller Konfliktlösungsmechanismen

Der Bundesrat hat die Möglichkeit geprüft, ein Organ zu schaffen, das für die aussergerichtliche Beilegung von Konflikten im Zusammenhang mit dem Datenschutz zuständig wäre. Schliesslich hat er jedoch darauf verzichtet, da ein solcher Mechanismus bereits in zahlreichen Bereichen besteht (Ombudscom, Ombudsman der Banken, Ombudsman der Privatversicherung und der SUVA usw.) und zu Kompetenzkonflikten führen würde. Ausserdem würde die Schaffung eines dem Beauftragten angegliederten Organs erhebliche Kosten verursachen.

1.8 Regulierungsfolgenabschätzung

Die Regulierungsfolgenabschätzung (RFA) ist ein Instrument zur Untersuchung und Darstellung der volkswirtschaftlichen Auswirkungen von Vorlagen des Bundes. Dieses Instrument ist obligatorisch und vor allem bei Botschaften, erläuternden Berichten und Anträgen an den Bundesrat von Bedeutung. Die rechtlichen Grundlagen der RFA sind in Artikel 170 BV und Artikel 141 Absatz 2 des Bundesgesetzes vom 13. Dezember 2002[61] über die Bundesversammlung (ParlG) festgelegt.

Das BJ und das Staatssekretariat für Wirtschaft (SECO) haben das Unternehmen PwC mit der Durchführung einer RFA[62] zum Vorentwurf beauftragt. Sie sollte als Grundlage für dessen Beurteilung dienen. Da im Entwurf die meisten geprüften Massnahmen übernommen werden, können die Schlussfolgerungen zum Vorentwurf auf den Entwurf übertragen werden. Die Regulierungsfolgenabschätzung beruht im Wesentlichen auf den Ergebnissen einer Online-Unternehmensbefragung sowie auf Gesprächen mit Datenschutzfachleuten. In der RFA wurde der Vorentwurf insgesamt positiv beurteilt.

Die RFA umfasst fünf Prüfpunkte: die Notwendigkeit und Möglichkeit staatlichen Handelns, die Auswirkungen auf die einzelnen gesellschaftlichen Gruppen, die Auswirkungen auf die Gesamtwirtschaft, die alternativen Regelungen und die Zweckmässigkeit im Vollzug.

1.8.1 Notwendigkeit und Möglichkeit staatlichen Handelns

Die Notwendigkeit zum Erlass gesetzlicher Regelungen hängt zum einen mit den bedeutenden technologischen und gesellschaftlichen Entwicklungen während der letzten Jahre zusammen. Diese lösen in der Bevölkerung Ängste aus und haben zu neuen Datenschutzrisiken geführt. Der Vorentwurf war hauptsächlich darauf ausgerichtet, die Kontrolle und Verfügungsfähigkeit über Daten zu verbessern sowie die Transparenz von Datenbearbeitungen zu erhöhen. Dies trifft auch auf den Entwurf zu. Zum anderen muss der Bund auch aufgrund der Entwicklungen im Bereich des internationalen Rechts tätig werden. Dies gilt insbesondere für den E-SEV 108 sowie, aufgrund der Schengen-Zusammenarbeit, für die Richtlinie (EU) 2016/680; zu berücksichtigen ist aber auch die Verordnung (EU) 2016/679.

1.8.2 Auswirkungen auf die einzelnen gesellschaftlichen Gruppen

Von den im Vorentwurf vorgesehenen Änderungen waren alle in der Schweiz tätigen Unternehmen betroffen. PwC hat die Unternehmen, unter Berücksichtigung ihrer Branche und Grösse, entsprechend ihrer «datenschutzrechtlichen Exponierung» unterteilt. Es wurden die folgenden Segmente gebildet:

61 SR **171.10**
62 Die RFA ist auf der Website des BJ abrufbar: www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html.

- Segment A: Unternehmen mit geringer datenschutzrechtlicher Exponierung
- Segment B: Unternehmen mit mittlerer bis grosser datenschutzrechtlicher Exponierung
- Segment C: Unternehmen mit starker und für sie essentieller datenschutzrechtlicher Exponierung.

Wird diese Segmentierung auf die ausgewählten Wirtschaftszweige in der Schweiz angewandt, beläuft sich die Zahl der Unternehmen im Segment A auf rund 335 000 Unternehmen (55,1 %), das Segment B umfasst ungefähr 265 000 Unternehmen (43,5 %) und das Segment C knapp 8000 Unternehmen (1,4 %).

Die Analyseergebnisse haben gezeigt, dass die Unternehmen des Segments A von den im Vorentwurf vorgesehenen Massnahmen generell nur geringfügig betroffen waren. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im Vorentwurf Massnahmen stärker betroffen als Grossunternehmen, da sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei. Die Unternehmen der Segmente B und C dagegen sind aufgrund ihrer Aktivitäten, ihrer Grösse und ihrer Öffnung gegenüber dem Ausland stärker betroffen.[63]

1.8.3 Auswirkungen auf die Gesamtwirtschaft

Die Auswirkungen auf die Wirtschaft sind von den Auswirkungen auf die Gesellschaft insgesamt zu unterscheiden. Aus wirtschaftlicher Perspektive konzentrierte sich die Diskussion über die vermuteten Effekte auf die Problematik des Wettbewerbs. Würde die Europäische Union die Schweiz nicht mehr als Land einstufen, das einen angemessenen Datenschutz gewährleistet, oder würde die Schweiz Regelungen erlassen, die nur im Inland gelten oder restriktiver sind als das Recht der Europäischen Union, wären für die Schweiz schwerwiegende Wettbewerbsnachteile gegenüber den Mitgliedstaaten der Europäischen Union zu erwarten.

Da alle Unternehmen eines bestimmten Segments innerhalb der Schweiz gleichermassen betroffen sind, werden die vorgesehenen Änderungen im Inland als mehrheitlich wettbewerbsneutral erachtet. Aufgrund der RFA stellt sich jedoch die Frage, in welchem Masse ein verstärkter Datenschutz zu einem Wettbewerbsvorteil auf internationaler Ebene führt.

Aus gesellschaftlicher Perspektive ist festzuhalten, dass grundsätzlich keine Pflichten der betroffenen Personen vorgesehen sind. Nach Auffassung der befragten Expertinnen und Experten sind die in der RFA geprüften Massnahmen geeignet, den betroffenen Personen die Ausübung ihrer Rechte zumindest formell zu erleichtern. Die Expertinnen und Experten beziehen sich hauptsächlich auf die Stärkung des Auskunftsrechts, die höhere Transparenz der Datenbearbeitung, Verbesserungen der

63 Für eine detaillierte Übersicht über die Auswirkungen der einzelnen Massnahmen siehe die Übersichtstabelle auf den Seiten 50 ff. des Berichts.

Rechte der betroffenen Personen sowie ein Recht auf Datenportabilität (vgl. Ziff. 1.7.4). In welchem Ausmass die betroffenen Personen von den geprüften Massnahmen konkret profitieren werden, hängt vor allem davon ab, welche Bedeutung diese Personen dem Schutz ihrer persönlichen Daten beimessen. In diesem Zusammenhang können sich datenschutzfreundliche Voreinstellungen (Privacy by Default) zu einem wesentlichen Instrument des Datenschutzes entwickeln.

1.8.4 Alternative Regelungen

Im Rahmen der Gespräche mit Expertinnen und Experten wurden auch andere Lösungen als die vorgesehenen Massnahmen erörtert, wie beispielsweise die Möglichkeit, Daten den Regeln für dingliche Verfügungs- und Nutzungsrechte zu unterstellen. Diese Lösungen wurden indessen in vielen Fällen als nicht umsetzbar beurteilt, da sie zu stark von den Entwicklungen auf internationaler Ebene abweichen (so sieht beispielsweise kein anderes europäisches Land Eigentumsrechte an Daten vor). Was den internationalen Wettbewerb anbelangt, wird nahegelegt, auf strengere Massnahmen als in den Ländern der Europäischen Union zu verzichten. Damit soll eine Überregulierung verhindert werden. Begrüsst wird die Möglichkeit der Einsetzung einer Expertenkommission, die den Auftrag hat, Empfehlungen der guten Praxis zu erarbeiten, weil diese eine rasche Anpassung an technologische Neuerungen ermöglichen. Der Bundesrat hat inzwischen auf diese Möglichkeit verzichtet (vgl. Ziff. 1.7.5).

1.8.5 Zweckmässigkeit im Vollzug

Zur Begrenzung der mit der Umsetzung der Massnahmen verbundenen Kosten empfiehlt eine Mehrheit der befragten Fachleute, den Unternehmen zu erlauben, ihren Informationspflichten pauschal nachzukommen. Dies könnte nach Auffassung der Expertinnen und Experten beispielsweise mit Erläuterungen zum Datenschutzrecht oder dadurch erfolgen, dass auf einer Website oder in allgemeinen Geschäftsbedingungen Piktogramme angebracht werden. Die Einführung von «individualisierten» Informationspflichten würde nach den Einschätzungen der Fachleute hingegen hohe Kosten nach sich ziehen.

Um die Rechtssicherheit und Transparenz zu gewährleisten, solle der Gesetzesentwurf klar definierte Begriffe (Legaldefinitionen) verwenden und die Umstände klar bestimmen, aus denen eine Pflicht resultiert. So müsse beispielsweise angegeben werden, in welchen Fällen eine Datenschutz-Folgenabschätzung vorzunehmen ist. Zur Sensibilisierung für die Probleme im Zusammenhang mit dem Datenschutz und zur Erleichterung der Umsetzung des Gesetzes sei eine zielgerichtete Kommunikation (beispielsweise mit Hinweisen, Broschüren) und die Entwicklung von Leitfäden erforderlich. Diese Massnahmen könnten insbesondere für Unternehmen mit geringer datenschutzrechtlicher Exponierung nützlich sein. Die Idee einer unabhängigen Expertenkommission wurde in diesem Zusammenhang von den meisten Expertinnen und Experten begrüsst.

2 Richtlinie (EU) 2016/680

2.1 Erläuterung der Richtlinie (EU) 2016/680

2.1.1 Verlauf der Verhandlungen

Die Beratungen der Mitgliedstaaten der Europäischen Union und der vier assoziierten Schengen-Mitglieder (Norwegen, Island, Schweiz und Liechtenstein im Rahmen ihrer Mitwirkungsrechte) fanden in den Jahren 2012 bis 2015 unter dem Vorsitz des Mitgliedslandes der Europäischen Union, das die Präsidentschaft innehatte, innerhalb der dafür zuständigen Arbeitsgruppen des Rates (gemischte Ausschüsse) statt. Im Rahmen dieser gemischten Ausschüsse beteiligten sich Vertreterinnen und Vertreter des Bundes und der Kantone an der Erarbeitung der Richtlinie (EU) 2016/680. Am 27. April 2016 haben das Europäische Parlament und der Rat der Europäischen Union die Richtlinie (EU) 2016/680 formell verabschiedet.

2.1.2 Kurzer Überblick

Die Richtlinie (EU) 2016/680 ist darauf ausgerichtet, personenbezogene Daten zu schützen, die zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, bearbeitet werden. Der Rechtsakt soll ein hohes Schutzniveau für personenbezogene Daten gewährleisten und gleichzeitig den Austausch dieser Daten zwischen den zuständigen Behörden der verschiedenen Schengen-Staaten erleichtern. Anders als der Rahmenbeschluss 2008/977/JAI gilt die Richtlinie (EU) 2016/680 sowohl für grenzüberschreitende Datenbearbeitungen als auch für Datenbearbeitungen, die von den Polizei- und Justizbehörden ausschliesslich auf innerstaatlicher Ebene durchgeführt werden. Der Wortlaut der Richtlinie ist auf die Verordnung (EU) 2016/679 (vgl. Ziff. 4) abgestimmt, damit in den Grundzügen die gleichen allgemeinen Grundsätze gelten. Allerdings soll durch gewisse Anpassungen ein angemessenes Gleichgewicht zwischen dem Recht der betroffenen Person auf Schutz ihrer Privatsphäre und den Bedürfnissen der Strafbehörden hergestellt werden. Nachfolgend werden die wesentlichen Neuerungen aufgeführt.

Die Richtlinie (EU) 2016/680 führt eine Verpflichtung zur Unterscheidung verschiedener Kategorien betroffener Personen (Art. 6) sowie Regeln zur Unterscheidung der Daten und zur Überprüfung der Qualität der Daten ein. Artikel 8 regelt die Rechtmässigkeit der Bearbeitung. Datenbearbeitungen müssen im Wesentlichen auf einer gesetzlichen Grundlage beruhen. Andere Rechtfertigungsgründe, wie beispielsweise die Einwilligung der betroffenen Person, gelten nicht für Datenbearbeitungen, die in den Geltungsbereich der Richtlinie (EU) 2016/680 fallen. In Artikel 11 ist der Grundsatz festgelegt, dass eine ausschliesslich auf einer automatischen Verarbeitung beruhende Entscheidung verboten ist, es sei denn, sie ist nach dem Recht des betreffenden Mitgliedstaats erlaubt und für die betroffene Person ist das Recht auf ein persönliches Eingreifen seitens des Verantwortlichen gewährleistet.

In Kapitel III sind die Rechte der betroffenen Person geregelt. Nach Artikel 16 Absatz 3 ist der Verantwortliche verpflichtet, die Verarbeitung einzuschränken, wenn die betroffene Person die Richtigkeit der Daten bestreitet und diese nicht festgestellt werden kann. Artikel 17 sieht vor, dass die betroffene Person im Fall einer Einschränkung die Möglichkeit haben muss, ihre Rechte über die Aufsichtsbehörde auszuüben. Ausserdem können die Schengen-Staaten gemäss Artikel 18 vorsehen, dass die Ausübung der Rechte nach den Artikeln 13, 14 und 16 im Einklang mit dem Verfahrensrecht des Schengen-Staates erfolgt, wenn es um Daten in einer gerichtlichen Entscheidung oder einer Verfahrensakte geht, die in strafrechtlichen Ermittlungen und in Strafverfahren verarbeitet werden.

Kapitel IV regelt die Pflichten des Verantwortlichen und des Auftragsverarbeiters. Es führt den Grundsatz des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ein (Art. 19 und 20). Artikel 24 sieht die Pflicht des Verantwortlichen und des Auftragsverarbeiters vor, ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die ihrer Zuständigkeit unterliegen. Ausserdem sind die Verantwortlichen verpflichtet, vor bestimmten Verarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen (Art. 27) und gegebenenfalls die Aufsichtsbehörde zu konsultieren (Art. 28). Die Artikel 30 und 31 verpflichten die Verantwortlichen, in gewissen Fällen der Aufsichtsbehörde eine Verletzung der Datensicherheit zu melden und gegebenenfalls die betroffene Person zu benachrichtigen.

Das Kapitel V regelt die Übermittlung von Daten an Drittländer oder internationale Organisationen. Die Europäische Kommission ist dafür zuständig, das Schutzniveau zu prüfen, das ein Drittland, ein Gebiet oder ein Verarbeitungssektor in einem Drittland bietet (Art. 36). Hat die Europäische Kommission die Angemessenheit des Schutzniveaus in einem Drittstaat nicht durch Beschluss festgestellt, darf die Datenübermittlung nur erfolgen, wenn geeignete Garantien bestehen (Art. 37) oder wenn in bestimmten Fällen eine Ausnahme vorliegt (Art. 38). Artikel 39 regelt die Übermittlung personenbezogener Daten an in Drittländern niedergelassene Empfänger, wenn Daten nicht durch die üblichen Kanäle der polizeilichen oder justiziellen Zusammenarbeit an die zuständigen Behörden übermittelt werden können.

Kapitel VI verpflichtet die Schengen-Staaten, im Bereich des Datenschutzes unabhängige Aufsichtsbehörden einzusetzen. Die Artikel 45–47 regeln die Zuständigkeiten, Aufgaben und Befugnisse der Aufsichtsbehörden. Gemäss Artikel 45 Absatz 2 sehen die Schengen-Staaten vor, dass die Aufsichtsbehörde nicht für die Aufsicht über jene Verarbeitungen zuständig ist, die Gerichte im Rahmen ihrer justiziellen Tätigkeit vornehmen. Nach Artikel 45 Absatz 2 können die Schengen-Staaten auch eine Ausnahme für jene Datenverarbeitungen vorsehen, die durch andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit erfolgen. Dabei kann es sich beispielsweise um Staatsanwaltschaften handeln. Artikel 47 Absatz 1 verpflichtet die Schengen-Staaten vorzusehen, dass die Aufsichtsbehörde über wirksame Untersuchungsbefugnisse verfügt, d. h. zumindest vom Verantwortlichen und vom Auftragsverarbeiter Zugang zu den verarbeiteten Daten und allen Informationen erhält, die zur Erfüllung ihrer Aufgaben notwendig sind. Gemäss Absatz 2 muss die Aufsichtsbehörde auch über wirksame Abhilfebefugnisse verfügen, wie beispielsweise über die Befugnis zur Verwarnung eines Verantwortlichen oder eines Auf-

tragsverarbeiters, zur Anordnung von vorschriftsgemässen Verarbeitungen, gegebenenfalls durch Berichtigung oder Löschung der Daten, sowie zur Verhängung einer vorübergehenden oder endgültigen Beschränkung der Verarbeitung, einschliesslich eines Verbots. Die Befugnisse der Aufsichtsbehörde dürfen jedoch weder die speziellen Vorschriften für Strafverfahren, einschliesslich der Ermittlung und Verfolgung von Straftaten, noch die Unabhängigkeit der Gerichte berühren.

Kapitel VIII bezieht sich auf die Rechtsbehelfe, die Haftung und die Sanktionen. Artikel 52 sieht vor, dass die betroffene Person das Recht auf Beschwerde bei der Aufsichtsbehörde hat. Nach Artikel 53 hat die betroffene Person auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden Entscheid der Aufsichtsbehörde. Zudem können sich die betroffenen Personen nach Artikel 55 unter bestimmten Umständen vertreten lassen.

2.2 Übernahme der Richtlinie (EU) 2016/680 als Schengen-Weiterentwicklung

Gemäss Artikel 2 Absatz 3 des Schengen-Assoziierungsabkommens hat sich die Schweiz grundsätzlich verpflichtet, jede Weiterentwicklung des Schengen-Besitzstands zu akzeptieren, umzusetzen und anzuwenden. Die Richtlinie (EU) 2016/680 entspricht einer Weiterentwicklung des Schengen-Besitzstands. Wie in Ziffer 2.4 ausgeführt, müssen im Zusammenhang mit der Übernahme der Richtlinie (EU) 2016/680 verschiedene gesetzgeberische Massnahmen auf Bundesebene getroffen werden, weil das geltende Recht nicht alle Anforderungen dieses Rechtsakts erfüllt.

Wird der Schweiz die Annahme eines Rechtsaktes als Schengen-Besitzstand notifiziert, muss sie gemäss dem Assoziierungsabkommen innert 30 Tagen nach Annahme des betreffenden Rechtsaktes entscheiden, ob sie dessen Inhalt akzeptiert und in ihre innerstaatliche Rechtsordnung umsetzt (Art. 7 Abs. 2 Bst. a des Schengen-Assozierungsabkommens).

Ist der fragliche Rechtsakt rechtlich verbindlich, erfolgen die Notifikation durch die Europäische Union und die Antwort der Schweiz im Rahmen eines Notenaustausches, der für die Schweiz einen völkerrechtlichen Vertrag darstellt. Dieser wird gemäss Verfassung entweder direkt durch den Bundesrat abgeschlossen oder der Abschluss bedarf der Zustimmung des Parlaments oder, im Falle eines Referendums, auch des Volkes.

Das Europäische Parlament und der Rat der Europäischen Union haben die Richtlinie (EU) 2016/680 am 27. April 2016 verabschiedet. Der Rechtsakt wurde der Schweiz indessen erst am 1. August 2016 notifiziert. Dadurch war es der Schweiz nicht möglich, dem Generalsekretariat des Rates ihre Antwortnote innert der durch das Assoziierungsabkommen vorgeschriebenen Frist zu übermitteln. Die Schweiz konnte ihre Antwortnote erst am 1. September 2016 überreichen.

Im vorliegenden Fall muss die Bundesversammlung dem Notenaustausch betreffend die Übernahme der Richtlinie (EU) 2016/680 zustimmen. Da die Richtlinie für die Schweiz erst nach Erfüllung ihrer verfassungsrechtlichen Voraussetzungen rechtsverbindlich ist, hat der Bundesrat die Europäische Union in seiner Antwortnote vom

1. September 2016 darüber unterrichtet (Art. 7 Abs. 2 Bst. b Schengen-Assoziierungsabkommen).

Die Schweiz muss innert zwei Jahren (einschliesslich eines allfälligen Referendums) ab dem Zeitpunkt der Notifikation den fraglichen Akt in ihre Rechtsordnung umsetzen. Sobald der innerstaatliche Anpassungsprozess abgeschlossen ist, muss die Schweiz unverzüglich schriftlich die zuständigen europäischen Institutionen darüber informieren, dass die verfassungsrechtlichen Voraussetzungen erfüllt sind. Dies entspricht einer Ratifizierung des Notenaustausches zwischen der Schweiz und der Europäischen Union. Der Notenaustausch betreffend die Richtlinie (EU) 2016/680 tritt im Zeitpunkt der Mitteilung durch die Schweiz in Kraft. Die Richtlinie (EU) 2016/680 wurde der Schweiz am 1. August 2016 notifiziert. Die Frist für die Übernahme des Rechtsaktes und dessen Umsetzung dauert daher bis zum 1. August 2018.

2.3 Regelungskonzept

Die Richtlinie (EU) 2016/680 ist sowohl für die EU-Mitgliedstaaten als auch für die Schweiz nicht direkt anwendbar und bedarf einer Umsetzung in das jeweilige nationale Recht. In der Schweiz braucht es zur Umsetzung der Richtlinie gewisse Anpassungen in verschiedenen Bundesgesetzen, da diese den Anforderungen der Richtlinie (EU) 2016/680 nicht gänzlich entsprechen.

Als Schengen-assoziierter Staat muss die Schweiz die Richtlinie (EU) 2016/680 grundsätzlich nur insoweit anwenden, als Datenbearbeitungen im Rahmen der Schengener Zusammenarbeit im Strafrechtsbereich vorgenommen werden. Eine auf diesen Bereich beschränkte Umsetzung wäre prinzipiell ausreichend. Da der Inhalt der Richtlinie (EU) 2016/680 jedoch zu einem grossen Teil dem Inhalt des E-SEV 108 entspricht – wobei die Richtlinie detaillierter ist –, schlägt der Bundesrat vor, die Anforderungen der Richtlinie (EU) 2016/680 entsprechend den nachfolgenden Kriterien umfassender umzusetzen:

- Bestimmungen der Richtlinie (EU) 2016/680, die den Anforderungen des E-SEV 108 entsprechen, werden in den E-DSG übernommen und gelten für alle Datenbearbeitungen durch private Personen und Bundesorgane.
- Anforderungen der Richtlinie (EU) 2016/680, die allgemeinen Datenschutzgrundsätzen entsprechen, aber im E-SEV 108 nicht vorgesehen sind, werden für alle Datenbearbeitungen durch Bundesorgane übernommen. Auf diese Weise sollen unterschiedliche Datenschutzniveaus im öffentlichen Sektor vermieden werden.
- Vorschriften der Richtlinie (EU) 2016/680 in Bezug auf die Aufsichtsbehörde im Bereich des Datenschutzes werden im E-DSG umgesetzt. Ein Teil dieser Anforderungen ist auch im E-SEV 108 vorgesehen. Auf Bundesebene ist der Beauftragte grundsätzlich die zuständige nationale Aufsichtsbehörde für alle bundesrechtlichen Datenschutzregelungen. Die für den Beauftragten geltende Regelung muss unabhängig vom jeweiligen Aufsichtsbereich einheitlich gestaltet werden.

– Die Anforderungen der Richtlinie (EU) 2016/680, die spezifischen Bestimmungen für die Schengener Zusammenarbeit im Strafrechtsbereich entsprechen, werden ausschliesslich in die für diese Bereiche geltenden Gesetze übernommen (vgl. Ziff. 9.3).

2.4 Hauptsächliche notwendige Gesetzesänderungen

Aufgrund der Übernahme der Richtlinie (EU) 2016/680 müssen nebst dem DSG weitere Bundesgesetze geändert werden: das StGB, die Strafprozessordnung vom 5. Oktober 2007[64] (StPO), das IRSG, das Bundesgesetz vom 22. Juni 2001[65] über die Zusammenarbeit mit dem Internationalen Strafgerichtshof, das Bundesgesetz vom 3. Oktober 1975[66] zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen, das Bundesgesetz vom 7. Oktober 1994[67] über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten, das Bundesgesetz vom 13. Juni 2008[68] über die polizeilichen Informationssysteme des Bundes (BPI) und das Schengen-Informationsaustausch-Gesetz vom 12. Juni 2009[69] (SIaG). Die Bestimmungen der Richtlinie (EU) 2016/680, die in den E-DSG und in die oben erwähnten bereichsspezifischen Datenschutznormen übernommen werden müssen, sind in den Erläuterungen zu den Gesetzesbestimmungen aufgeführt.

Es ist somit ersichtlich, dass viele Bundesgesetze im Polizeibereich Datenschutzbestimmungen enthalten. Es stellt sich die Frage, ob durch diese Verstreuung der Datenschutzbestimmungen die Rechtsanwendung nicht erschwert wird und ob nicht der Erlass eines Bundesgesetzes in Betracht gezogen werden sollte, das die Tätigkeiten im Polizeibereich gesamthaft regelt; zahlreiche Kantone haben diesen Weg gewählt.

3 E-SEV 108

3.1 Kurzer Überblick

Die Vertragsparteien müssen den Entwurf zur Revision des Übereinkommens SEV 108 auf alle Datenbearbeitungen in ihrer Rechtsordnung im öffentlichen und privaten Sektor anwenden. Nicht durch diesen Entwurf geregelt werden nur Datenbearbeitungen, die eine Person im Rahmen ihrer persönlichen Aktivitäten vornimmt (Art. 3).

Entsprechend dem E-SEV 108 müssen die Pflichten des für die Verarbeitung Verantwortlichen ausgeweitet werden. Dieser ist verpflichtet, der zuständigen Aufsichtsbehörde bestimmte Verstösse gegen den Datenschutz zu melden (Art. 7

64 SR **312**
65 SR **351.6**
66 SR **351.93**
67 SR **360**
68 SR **361**
69 SR **362.2**

Abs. 2). Die Verpflichtung des für die Verarbeitung Verantwortlichen, die betroffene Person zu informieren, muss überdies insbesondere auf die zu liefernden Informationen und die automatisierten Einzelentscheidungen ausgedehnt werden. Die Vertragsparteien müssen den für die Verarbeitung Verantwortlichen auch dazu verpflichten, im Vorfeld bestimmter Datenverarbeitungen eine Folgenabschätzung vorzunehmen und für den Datenschutz die Grundsätze «Privacy by Design» und «Privacy by Default» anzuwenden (Art. 8bis Abs. 2 und 3).

Die Vertragsparteien müssen der betroffenen Person das Recht einräumen, nicht einer Entscheidung unterworfen zu sein, die ausschliesslich auf der Grundlage einer automatisierten Verarbeitung ihrer Daten ergeht, ohne dass die betroffene Person ihren Standpunkt geltend machen kann (Art. 8 Bst. a). Auch das Auskunftsrecht der betroffenen Person muss ausgebaut werden (Art. 8 Bst. b), und die geltenden Bedingungen für die Einwilligung der betroffenen Person müssen erweitert werden.

Die Vertragsparteien sind verpflichtet, ein Sanktionensystem und ein Rechtsmittelsystem festzulegen (Art. 10).

Der Grundsatz, wonach Personendaten nur in einen Drittstaat übermittelt werden dürfen, wenn ein angemessener Schutz gewährleistet ist, bleibt im Vergleich zum gegenwärtigen Übereinkommen SEV 108 unverändert. Gemäss dem E-SEV 108 (Art. 12) kann ein angemessenes Datenschutzniveau durch Rechtsvorschriften des betreffenden Staates oder der empfangenden internationalen Organisation oder durch bestimmte Sicherheiten gewährleistet werden. Wenn kein angemessenes Schutzniveau garantiert ist, dürfen Daten an einen Drittstaat weitergegeben werden, wenn die betroffene Person gültig eingewilligt hat oder wenn ein bestimmter Ausnahmefall vorliegt. Schliesslich müssen die Vertragsparteien gemäss dem E-SEV 108 vorsehen, dass die Aufsichtsbehörde von der Person, welche die Daten weitergibt, den Nachweis über die Wirksamkeit der aufgestellten Sicherheiten verlangen und die Datenweitergabe gegebenenfalls verbieten oder aussetzen kann.

Die Vertragsparteien sind verpflichtet, eine unabhängige Aufsichtsbehörde zu schaffen, wie dies bereits im bestehenden Übereinkommen SEV 108 verlangt wird. Gemäss dem E-SEV 108 (Art. 12bis) müssen die Aufsichtsbehörden ermächtigt werden, verbindliche, anfechtbare Entscheidungen zu fällen und verwaltungsrechtliche Sanktionen zu verhängen. Von der Überwachung durch die Aufsichtsbehörde sind lediglich Datenverarbeitungen ausgenommen, die von Organen in Ausübung ihrer Rechtsprechungsbefugnisse ausgeführt werden. Der Aufsichtsbehörde muss auch der Auftrag erteilt werden, die Öffentlichkeit und die für die Verarbeitung Verantwortlichen für den Datenschutz zu sensibilisieren.

3.2 Ratifizierung des Änderungsprotokolls zum Übereinkommen SEV 108

Der E-SEV 108 soll zu einem universellen Instrument werden. Bereits das derzeitige Übereinkommen kann auch durch Staaten ratifiziert werden, die nicht Mitglied des Europarates sind. Rund fünfzig Staaten haben das gegenwärtige Übereinkommen ratifiziert, davon vier Länder, die dem Europarat nicht angehören (Uruguay, Tunesien, Mauritius und Senegal). Ausserdem sind mehrere Staaten, die nicht Mitglied des

Europarates sind, im Begriff, das Übereinkommen zu ratifizieren (Marokko, Kapverden, Burkina Faso, Argentinien). Das Interesse aussereuropäischer Staaten an einer Ratifizierung des Übereinkommens SEV 108 könnte weiter zunehmen, weil die Europäische Union dieses als entscheidendes Kriterium für einen Angemessenheitsbeschluss betrachtet.

Mit dem E-SEV 108 lässt sich der Datenschutz auf internationaler Ebene vereinheitlichen und verbessern. Dies verstärkt auch den Schutz der Schweizer Bürgerinnen und Bürger, wenn ihre Personendaten im Ausland bearbeitet werden. Der Entwurf trägt ebenfalls dazu bei, die Bekanntgabe von Daten zwischen den Vertragsparteien zu vereinfachen. Dadurch erhalten Schweizer Unternehmen einen besseren Zugang zu den Märkten dieser Länder. Die Ratifizierung des Änderungsprotokolls zum Übereinkommen SEV 108 dürfte zudem eine zentrale Voraussetzung sein, damit die Europäische Union der Schweiz erneut ein angemessenes Datenschutzniveau bestätigt. Nur dadurch bleibt der Zugang zum europäischen Markt weiterhin uneingeschränkt gewährleistet.

Ob zum Schutz der Menschenrechte oder aus wirtschaftlichen Gründen (Erleichterung der Bekanntgabe ins Ausland), die Schweiz tut mithin gut daran, das Änderungsprotokoll zum Übereinkommen SEV 108 rasch zu ratifizieren. In mehreren Antworten auf parlamentarische Vorstösse hat der Bundesrat zum Ausdruck gebracht, dass er den E-SEV 108 unterstützt. Ausserdem hat er dafür plädiert, den Datenschutz im Rahmen seiner Massnahmen für die Stärkung der Menschenrechte auszubauen.[70] Schliesslich ist darauf hinzuweisen, dass die im E-SEV 108 vorgesehenen Massnahmen mit den Zielen übereinstimmen, die der Bundesrat in seinem Beschluss vom 9. Dezember 2011[71] aufgrund der Evaluation des DSG festgehalten hat.

Gemäss Artikel 4 E-SEV 108 ist jede Vertragspartei verpflichtet, in ihrem innerstaatlichen Recht die erforderlichen Massnahmen zu ergreifen, um die Bestimmungen dieses Erlasses umzusetzen. Ausserdem müssen diese Massnahmen bei der Ratifizierung zum künftigen Übereinkommen SEV 108 in Kraft treten. Die Vertragsparteien können keine Vorbehalte anbringen (Art. 25).

Der Inhalt des E-DSG stimmt weitgehend mit den Anforderungen des Änderungsprotokolls überein, sodass zum gegebenen Zeitpunkt eine Ratifizierung möglich ist, ohne dass die Schweizer Gesetzgebung weiterer Anpassungen bedürfte.

70 Seine Unterstützung für die laufenden Arbeiten im Europarat hat der Bundesrat insbesondere in seinen Antworten auf die folgenden parlamentarischen Vorstösse zum Ausdruck gebracht: Interpellation Eichenberger 13.4209 («US-Swiss Safe Harbor Framework. Wiederherstellung des Vertrauens beim Datenaustausch mit den USA»); Anfrage Gross 13.1072 («Uno-Pakt über bürgerliche und politische Rechte. Integration des Datenschutzes»).

71 BBl **2012** 255

3.3 Hauptsächliche notwendige Gesetzesänderungen

Die Bestimmungen des E-SEV 108 sind nicht direkt anwendbar. Um das Änderungsprotokoll dieses Erlasses ratifizieren zu können, muss die Schweiz bestimmte bundesrechtliche Bestimmungen anpassen. Die Bestimmungen des E-SEV 108, die in den E-DSG übernommen werden müssen, sind in den Erläuterungen zu den Bestimmungen dieses Erlasses aufgeführt.

4 Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

4.1 Kurzer Überblick

Die Verordnung (EU) 2016/679 ist der grundlegende Datenschutzerlass auf Ebene der Europäischen Union; sie gehört nicht zum Schengen-Acquis. Die Richtlinie (EU) 2016/680 ist inhaltlich auf die Verordnung ausgerichtet, sodass die beiden Erlasse weitgehend übereinstimmende Regelungen vorsehen. Allerdings ist die Verordnung detaillierter, während einige Bestimmungen der Richtlinie auf die Bedürfnisse der Strafbehörden ausgerichtet sind.

Die Verordnung (EU) 2016/679 regelt hauptsächlich den Schutz von Daten, die im Rahmen des Binnenmarkts bearbeitet werden, doch sie gilt auch für den öffentlichen Sektor. Sie enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten (Art. 1).

In Kapitel III sind die Rechte der betroffenen Person geregelt. Im Vergleich zur Richtlinie 95/46/EG wurden diese Rechte ausgebaut. So gewährleistet die Verordnung (EU) 2016/679 den betroffenen Personen ein besseres Auskunftsrecht in Bezug auf sie betreffende Daten (Art. 12–15). Der Erlass sieht darüber hinaus für die betroffenen Personen ein Recht auf Berichtigung (Art. 16), ein Recht auf Löschung (Art. 17) – das auch als «Recht auf Vergessenwerden» bezeichnet wird – sowie ein Recht auf Einschränkung der Verarbeitung (Art. 18) vor. Die betroffenen Personen haben auch das Recht, die sie betreffenden Daten von einem Dienstleistungserbringer zu einem anderen zu übermitteln (Datenportabilität, Art. 20). Schliesslich haben die betroffenen Personen das Recht, Widerspruch gegen eine Datenverarbeitung einzulegen, insbesondere wenn diese dem Profiling dient (Art. 21), und sie haben Anspruch darauf, nicht einer auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden (Art. 22).

In Kapitel IV sind die Pflichten des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters geregelt. In diesem Kapitel wird der Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen festgehalten (Art. 25). Es definiert auch die Bedingungen für Auftragsverarbeiter (Art. 28 und 29). Die für die Verarbeitung Verantwortlichen sind in bestimmten Fällen verpflichtet, Verletzungen des Schutzes personenbezogener Daten der Aufsichtsbehörde und der betroffenen Person zu melden (Art. 33 und 34). Ausserdem müssen die für die Verarbeitung Verantwortlichen bei bestimmten Formen der Verarbeitung vorab eine Datenschutz-Folgenabschätzung durchführen (Art. 35) und

gegebenenfalls die Aufsichtsbehörde konsultieren (Art. 36). Im Weiteren müssen Behörden und öffentliche Stellen sowie Unternehmen, die Datenverarbeitungen mit besonderen Risiken durchführen, einen Datenschutzbeauftragten benennen (Art. 37–39). Schliesslich müssen die Mitgliedstaaten der Europäischen Union die Ausarbeitung von Verhaltensregeln fördern, die zur ordnungsgemässen Anwendung der Verordnung (EU) 2016/679 beitragen (Art. 40 und 41), und datenschutzspezifische Zertifizierungsverfahren einführen (Art. 42 und 43).

Kapitel V der Verordnung (EU) 2016/679 regelt die Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen. Die Kommission muss das Schutzniveau prüfen, das ein Gebiet oder ein Sektor in einem Drittland bietet (Art. 45). Liegt kein Beschluss der Kommission vor, wonach in einem Gebiet oder in einem Sektor ein angemessenes Schutzniveau gewährleistet ist, kann die Datenübermittlung trotzdem durchgeführt werden, sofern geeignete Garantien vorliegen (Art. 46), verbindliche interne Datenschutzvorschriften erlassen wurden (Art. 47) oder eine Ausnahme für einen bestimmten Fall anwendbar ist (Art. 49).

In Kapitel VI geht es um die unabhängigen Aufsichtsbehörden. Die Mitgliedstaaten können eine oder mehrere Aufsichtsbehörden einsetzen, die den Auftrag haben, die Anwendung der Verordnung (EU) 2016/679 und gegebenenfalls auch der Richtlinie (EU) 2016/680 zu überwachen. Für die Unabhängigkeit der Aufsichtsbehörde gelten in beiden Erlassen die gleichen Anforderungen. Jede Aufsichtsbehörde muss über bestimmte Untersuchungsbefugnisse verfügen (Art. 58 Abs. 1). Ausserdem stehen ihr sämtliche Abhilfebefugnisse zu, die in der Verordnung (EU) 2016/679 (Abs. 2) vorgesehen sind.

In Kapitel VII sind Verfahren vorgesehen, mit denen in der ganzen Europäischen Union eine kohärente Anwendung des DSG gewährleistet werden soll. Insbesondere bei grenzüberschreitenden Fällen, in die mehrere nationale Aufsichtsbehörden involviert sind, wird ein einziger Aufsichtsbeschluss getroffen. Dank diesem Grundsatz, der auch als «Verfahren der Zusammenarbeit und Kohärenz» bezeichnet wird, muss sich ein Unternehmen, das über Niederlassungen in mehreren Mitgliedstaaten verfügt, nur mit der Aufsichtsbehörde des Mitgliedstaates auseinandersetzen, in dem es seinen Hauptsitz hat. Diese Behörde wird mit dem Begriff «federführende Aufsichtsbehörde» bezeichnet (Art. 56). Die Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden ist in Artikel 60 geregelt. Diese bemühen sich, einen Konsens zum Beschlussentwurf zu erzielen, der von der federführenden Aufsichtsbehörde erarbeitet wird. In Kapitel VII sind auch die gegenseitige Amtshilfe zwischen den Aufsichtsbehörden (Art. 61) und gemeinsame Massnahmen der Aufsichtsbehörden (Art. 62) vorgesehen.

In Kapitel VIII geht es um Rechtsbehelfe, Haftung und Sanktionen. In Artikel 77 ist festgehalten, dass die betroffene Person das Recht auf Beschwerde bei einer Aufsichtsbehörde hat. Gemäss Artikel 78 hat die betroffene Person auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Entscheid einer Aufsichtsbehörde. In Artikel 80 ist das Recht der betroffenen Personen vorgesehen, sich unter bestimmten Bedingungen vertreten zu lassen. In Artikel 83 sind Voraussetzungen festgehalten, nach denen die Aufsichtsbehörde Geldbussen verhängen kann.

Kapitel IX enthält verschiedene Vorschriften für besondere Verarbeitungssituationen, insbesondere betreffend die Freiheit der Meinungsäusserung und die Informationsfreiheit (Art. 85), den Zugang der Öffentlichkeit zu amtlichen Dokumenten (Art. 86) sowie in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken (Art. 89).

4.2 Angleichung der schweizerischen Gesetzgebung

Innerhalb der Europäischen Union wird die Verordnung (EU) 2016/679 die Richtlinie 95/46/EG ersetzen. Für die Schweiz sind die Bestimmungen der Verordnung (EU) 2016/679 nicht verbindlich, da es sich dabei nicht um eine Weiterentwicklung des Schengen-Acquis handelt. Dies bedeutet jedoch nicht, dass sie keine Auswirkungen in den Bereichen haben, in denen die Schweiz als Drittstaat betrachtet wird (Bereich ausserhalb der Schengen-Zusammenarbeit). Insbesondere für den privaten Sektor ist die Verordnung bedeutsam. Wie in Ziffer 1.2.2.2 erläutert, besteht in der Schweiz gemäss Beschluss der Europäischen Kommission[72] ein angemessenes Datenschutzniveau. Dieser Beschluss kann jedoch jederzeit widerrufen werden. Überdies hat die Europäische Union infolge des Urteils Schrems beschlossen, einen dynamischeren Ansatz zu verfolgen und die Entwicklung der Gesetzgebung zum Schutz der Personendaten in den Drittstaaten mit einem Angemessenheitsbeschluss ständig zu überprüfen. Wenn die Schweiz den Angemessenheitsbeschluss der Europäischen Union beibehalten will, tut sie als Drittstaat gut daran, ihre Gesetzgebung an die europäischen Anforderungen anzupassen. Die in Artikel 45 der Verordnung (EU) 2016/679 festgelegten Kriterien werden künftig massgebend sein für die Beurteilung, ob die schweizerische Gesetzgebung einen angemessenen Datenschutz gewährleistet. Der E-DSG sollte ein angemessenes Schutzniveau im Sinn der Verordnung garantieren.

5 Swiss-US Privacy Shield

Die Vereinigten Staaten bieten keinen angemessenen Schutz von Personendaten. Für die freie Übermittlung von Personendaten aus der Schweiz in die USA war deshalb die Verabschiedung eines besonderen Rechtsrahmens, des «Swiss-US Safe Harbor»[73] erforderlich. Diese Regelung entsprach im Grossen und Ganzen jener zwischen der Europäischen Union und den USA, dem «US-EU Safe Harbor», die von der Europäischen Kommission im Jahr 2000[74] genehmigt wurde. Mit diesem Rechtsrahmen verpflichteten sich die Vereinigten Staaten, Grundsätze anzuwenden, die ein mit der Schweiz bzw. der Europäischen Union vergleichbares Datenschutzniveau gewährleisten.

72 ABl. L 215 vom 25.8.2000, S. 1.
73 In einem Schreiben vom 9. Dezember 2008 an das amerikanische Handelsministerium hat die Schweiz anerkannt, dass das Abkommen «Swiss-US Safe Harbor» einen angemessenen Datenschutz im Sinne von Artikel 6 Absatz 1 DSG bietet.
74 Entscheidung 2000/520/EG vom 26. Juli 2000.

Am 6. Oktober 2015 hat der Gerichtshof der Europäischen Union die Entscheidung der Europäischen Kommission zur Genehmigung der «US-EU Safe Harbor»-Regelung für ungültig erklärt.[75] Er befand, dass die Europäische Kommission nicht überprüft habe, ob die Vereinigten Staaten aufgrund ihrer Rechtsvorschriften ihren internationalen Verpflichtungen tatsächlich nachkämen, dass keine Regelung den amerikanischen Staat daran hindere, unbeschränkten Zugang zu den Personendaten der Staatsangehörigen der Europäischen Union zu erhalten und dass kein wirksamer Rechtsschutz gegen derartige Eingriffe bestehe. Im Februar 2016 haben die Vereinigten Staaten und die Europäische Union eine neue Regelung namens «EU-US Privacy Shield» vorgelegt, die von der Europäischen Kommission am 12. Juli 2016 verabschiedet wurde und von den USA seit dem 1. August 2016 angewandt wird.

Infolge des genannten Urteils des Gerichtshofs der Europäischen Union und des neuen EU-US Privacy Shield handelte der Bund (SECO) die Regelung für die Bekanntgabe von Personendaten aus der Schweiz an Unternehmen mit Sitz in den Vereinigten Staaten neu aus. Der Bundesrat hat die neue Regelung namens «Swiss-US Privacy Shield» (Privacy Shield) am 11. Januar 2017 zur Kenntnis genommen. Der neue Rahmen entspricht weitgehend der Lösung zwischen den Vereinigten Staaten und der Europäischen Union sowie dem Europäischen Wirtschaftsraum (EWR).

Mit dem Privacy Shield werden die Mechanismen zur Umsetzung der Vorschriften durch die amerikanischen Unternehmen durch eine Reihe von Massnahmen gestärkt. Vorgesehen sind neue Pflichten für die amerikanischen Unternehmen (Informationspflichten gegenüber den betroffenen Personen, Pflicht zur Veröffentlichung der Entscheide der Federal Trade Commission [FTC] oder der Gerichte, Pflicht zur Zusammenarbeit mit dem amerikanischen Department of Commerce [DOC] oder dem Beauftragten).

Das Privacy Shield erweitert auch die Verwaltungs- und Aufsichtsbefugnisse des DOC. Bevor es ein Unternehmen in die Privacy-Shield-Liste aufnimmt, überprüft es beispielsweise, ob das Unternehmen seine Tätigkeiten in Verbindung mit den in der Schweiz erhaltenen Daten gut beschrieben hat, ob es genau festhält, welche Informationen durch die Zertifizierung abgedeckt sind und wie es auf die Zertifizierung hinweist (Website mit Link auf das DOC oder anderes Mittel). Das DOC setzt sich auch dafür ein, falsche Angaben über die Beteiligung am Privacy Shield aufzudecken und rechtliche Schritte einzuleiten sowie das Dossier an das FTC, das Department of Transportation oder andere Vollzugsorgane weiterzuleiten, wenn das Unternehmen die falschen Angaben nicht löscht.

Es ist auch ein Schiedsorgan geschaffen worden, das die Fälle von Verletzung der Grundsätze des Privacy Shield durch Unternehmen mit Sitz in den Vereinigten Staaten behandelt, die nicht über andere Rechtsmittel geheilt werden konnten und in denen keine oder nur zum Teil Massnahmen ergriffen worden sind. Keinen Zugang zum Schiedsorgan erhalten Personen, deren Fall bereits Gegenstand eines verbindlichen Schiedsverfahrens oder eines Gerichtsverfahrens war oder deren Beschwerde bereits früher abschliessend behandelt worden ist. Schweizer Staatsangehörige können bei diesem Organ Beschwerde erheben und müssen keine Verfahrenskosten

75 Urteil EuGH vom 6. Oktober 2015, Rs. C-362/14, ECLI:EU:C:2015:650 (Schrems).

tragen. Das Schiedsorgan wird durch Beiträge der amerikanischen Unternehmen finanziert.

Um auf die in Europa herrschende Befürchtung einzugehen, dass Personendaten insbesondere von den Nachrichtendiensten der USA missbräuchlich verwendet werden, hat das Department of State die Stelle einer Ombudsperson geschaffen, die von den Nachrichtendiensten unabhängig und dafür zuständig ist, diese auf Ersuchen des Beauftragten zu kontaktieren. Die Ombudsperson erstattet direkt dem Secretary of State Bericht, welches dafür sorgen wird, dass die Ombudsperson ihre Funktion objektiv ausübt.

Für den Beauftragten zieht das Swiss-US Privacy Shield bestimmte Kooperationspflichten nach sich. Er leitet die Beschwerden der betroffenen Personen an die FTC, das DOC und an die Ombudsperson des Department of State weiter. Da in den Vereinigten Staaten immer mehr Datenbearbeitungen ausgelagert werden und weil in der Schweiz heute verbreitet Dienste amerikanischer Unternehmen wie Facebook, Google oder Apple in Anspruch genommen werden, ist davon auszugehen, dass die Anzahl der vom Beauftragten zu bearbeitenden Beschwerden stark zunehmen wird. Er muss ferner die zertifizierten Unternehmen bei der Lösung von Datenschutzproblemen unterstützen, wenn sich diese zur Zusammenarbeit mit ihm bereit erklärt haben. Der Beauftragte leitet ausserdem die Auskunftsgesuche an die Ombudsperson des Department of State weiter. Schliesslich muss er jährlich in Zusammenarbeit mit den zuständigen Bundesämtern (u. a. dem SECO) die Qualität der im Swiss-US Privacy Shield vereinbarten Massnahmen zum Schutz der Persönlichkeit der betroffenen Personen überprüfen und einen Bericht verfassen.

6 Vergleich mit der Gesetzgebung aussereuropäischer Staaten, die das Übereinkommen SEV 108 nicht ratifiziert haben

Das BJ hat dem Schweizerischen Institut für Rechtsvergleichung (SIR) ein Mandat erteilt, um zu erfahren, wie die Gesetzgebung in Staaten ausserhalb der Europäischen Union ausgestaltet ist, die das Übereinkommen SEV 108 nicht ratifiziert haben. In die entsprechende Untersuchung[76] sind hauptsächlich folgende Punkte einbezogen worden: die Befugnisse und die Unabhängigkeit der Aufsichtsbehörde, das Vorliegen einer guten Praxis, die Rechte der betroffenen Personen (z. B. Rechtsmittel, Schlichtungsverfahren), die Pflichten der Verantwortlichen (z. B. Dokumentationspflicht, Datenschutz-Folgenabschätzung), Vorliegen von Normen zu Big Data, zum Profiling, zum Internet der Dinge, zur Datenportabilität sowie zur Umsetzung der Grundsätze des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen.

Es ist festzustellen, dass die Verabschiedung von Datenschutzgesetzen nicht mehr eine Besonderheit der europäischen Staaten ist.

76 Die Angaben beruhen auf einem Rechtsgutachten des SIR vom 3. August 2016.

6.1 Argentinien

Die Dirección Nacional de Protección de Datos Personales (DNPDP, Nationale Direktion für den Schutz von Personendaten) ist die Aufsichtsbehörde in Argentinien. Ihre Aufgaben sind in Artikel 29 des Gesetzes 25.326 geregelt.[77] Sie hat eine Unterstützungs-, Beratungs- und Aufsichtsfunktion. Gemäss Artikel 29 des Dekrets 1558/2001[78] kann sie auch Verwaltungs- und Verfahrensvorschriften zum Register der Personendatenbanken (Registro) erlassen, dank dem Personendatenbanken eruiert und kontrolliert werden können. In diesem Artikel 29 ist auch vorgesehen, dass die DNPDP Klagen und Beschwerden behandeln kann, die gemäss dem Gesetz 25.326 eingereicht werden. Die DNPDP hat im Weiteren die Aufgabe, Verhaltenskodizes zu genehmigen, die von den Organisationen der Nutzerinnen und Nutzer oder von den Datenbankverantwortlichen verabschiedet werden (Art. 30 des Gesetzes 25.326).

In Artikel 14 des Gesetzes 25.326 ist ein Auskunftsrecht festgelegt. Gemäss diesem Artikel haben die betroffenen Personen das Recht, Informationen zu ihren Personendaten zu erhalten, die in privaten oder öffentlichen Datenbanken enthalten sind. Wenn ein entsprechendes Gesuch eingereicht wird, muss der Verantwortliche dieses innerhalb von zehn Tagen beantworten. Nach Ablauf dieser Frist können die interessierten Personen eine Beschwerde einreichen. Gemäss Artikel 16 können natürliche Personen die Berichtigung, Aktualisierung oder Löschung sie betreffender Daten verlangen. Der Datenbankverantwortliche muss ein entsprechendes Gesuch innerhalb von fünf Tagen beantworten. Zurückweisen kann er ein solches Gesuch nur aus Gründen des Staatsschutzes, der öffentlichen Ordnung oder der öffentlichen Sicherheit oder im Zusammenhang mit den Interessen von Dritten. Nach Ablauf der fünftägigen Frist oder bei einer abschlägigen Antwort kann die interessierte Person eine Beschwerde einreichen.

Die Verantwortlichen haben die folgenden Hauptaufgaben: Eintragung der Datenbanken im Registro, Gewährleistung der Sicherheit der gespeicherten Daten, Sicherstellung der Vertraulichkeit der Daten und Lieferung der von der DNPDP verlangten Unterlagen und Auskünfte.

Die Datenschutzgesetzgebung gilt auch für die Beschaffung von Big Data, sofern eine Person anhand aller erhobenen Daten identifiziert werden kann. In Bezug auf das Profiling enthält Artikel 27 des Dekrets 1558/2001 eine Vorschrift zum Profiling im Bereich der Werbung. Gemäss diesem Artikel dürfen Daten ohne Einwilligung der betroffenen Person erhoben, bearbeitet und übermittelt werden, wenn dies dazu dient, Profile zu erstellen, sowie um Präferenzen und Verhaltensweisen zu kategorisieren. In diesem Zusammenhang sind jedoch zwei Voraussetzungen zu beachten: Die betroffenen Personen dürfen nur anhand ihrer Zugehörigkeit zu einer bestimmten Gruppe identifiziert werden, und der Umfang der erhobenen Personendaten muss

77 Ley 25.326, Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Sancionada: Octubre 4 de 2000, verfügbar unter: www.jus.gob.ar/media/33481/ley_25326.pdf.

78 Decreto 1558/2001, Protección de los datos personales, verfügbar unter: www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf.

auf das absolut notwendige Minimum beschränkt werden. Ausserdem muss in jeder Mitteilung zu Werbezwecken darauf hingewiesen werden, dass der Dateninhaber den Rückzug oder die Sperrung der Daten verlangen kann.

Bezüglich der Umsetzung des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen hat die DNPDP einen «Leitfaden für Best Practices bei der Entwicklung von Softwareapplikationen» genehmigt, der sich an Anwendungsentwickler richtet. In erster Linie soll dieser Leitfaden die Entwickler daran erinnern, bei der Entwicklung von Applikationen von Anfang an die Privatsphäre der betroffenen Personen zu respektieren.

6.2 Neuseeland

In Neuseeland wird der Datenschutz hauptsächlich durch den «Privacy Act 1993»[79] geregelt. Dieses Gesetz wird gegenwärtig revidiert. Der Entwurf zu einem neuen «Privacy Act» soll dem Parlament im Jahr 2017 vorgelegt werden.

Die vorgesehene Revision bezieht sich hauptsächlich auf die Funktionen der Behörde, die mit der Aufsicht im Bereich des Datenschutzes beauftragt ist, den sogenannten «Privacy Commissionner» (PC). Die Aufgaben des PC, der bislang die Regeln der Best Practices genehmigte, werden ausgebaut. Es wird ein System für die obligatorische Meldung von Verletzungen des Datenschutzes eingeführt, das mit zwei Verbesserungen für den PC kombiniert wird: Künftig kann er dringende Anfragen stellen, um Informationen zu erhalten, die er als notwendig erachtet, und er kann Zulässigkeitserklärungen bei Verstössen gegen den «Privacy Act» abgeben.

Die Revision hat nicht den Zweck, die Rechte von Privatpersonen zu stärken, da jene gemäss dem «Privacy Act 1993» als ausreichend gelten. In Teil 2 dieses Gesetzes werden den Einzelpersonen mit den «Information Privacy Principles» (IPP) bereits Rechte eingeräumt. Insbesondere die IPP 6 geben betroffenen Personen die Möglichkeit, sich darüber zu erkundigen, ob Daten über sie beschafft wurden, und Auskunft über diese Daten zu erhalten. Gemäss den IPP 7 können betroffene Personen um die Berichtigung von Daten über sie ersuchen. Wenn ihr Gesuch abgelehnt wird, können sie verlangen, dass die Daten mit einem Hinweis versehen werden, aus dem hervorgeht, dass um eine Berichtigung ersucht wurde.

Gegenwärtig muss jede «Agency»[80] dafür sorgen, dass innerhalb der «Agency» mindestens ein «Privacy Officer» (im Folgenden «PO») tätig ist. Die PO sind statutarisch verpflichtet, die Konformität mit den verschiedenen IPP zu fördern, sich um die Ersuchen zu kümmern, die an die «Agency» gerichtet werden, und im Zusammenhang mit Untersuchungen zur «Agency» mit dem PC zusammenzuarbeiten. Hinsichtlich der Pflichten der «Agencies» wird die Revision zwei wichtige Änderungen zur Folge haben. Die «Agencies» sind künftig verpflichtet, dem PC bestimmte Datenschutzverstösse zu melden. Ausserdem verlangt eine neue IPP von

79 Der «Privacy Act 1993» ist unter folgender Adresse verfügbar: www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

80 Als «Agency» gelten praktisch alle Personen und Organisationen, die über Personendaten verfügen.

den «Agencies», angemessene Massnahmen zu treffen, damit beim Austausch von Daten mit ausländischen Staaten ein annehmbarer Datenschutz gewährleistet ist.

Der PC hat eine wichtige Funktion, wenn es darum geht, den Grundsatz des Datenschutzes durch Technikgestaltung (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) umzusetzen. Denn gemäss Abschnitt 13(1)(n) des «Privacy Act 1993» kann er Nachforschungen anstellen und die Entwicklung der Datenbearbeitung und der neuen Technologien im Informatikbereich verfolgen. Im Weiteren hat er insbesondere dafür zu sorgen, dass die negativen Auswirkungen dieser Entwicklungen auf den Schutz der Privatsphäre von Einzelpersonen möglichst gering ausfallen. In diesem Zusammenhang kann der PC den Datenschutz durch Technikgestaltung fördern. Bezüglich Privacy by Design und Privacy by Default sind im Rahmen der Revision keine weiteren Vorschriften vorgesehen.

6.3 Südkorea

Südkorea verfügt seit 2011 über eine Gesetzgebung im Bereich des Datenschutzes. Dabei handelt es sich um den sogenannten «Personal Information Protection Act» (PIPA).

Aufgrund seiner Geschichte und seiner zahlreichen Gesetze verfügt Südkorea über ein ziemlich komplexes System. Dies zeigt sich unter anderem daran, dass mehrere Behörden für den Datenschutz zuständig sind. Für Fragen der Regulierung ist die «Personal Information Protection Commission» verantwortlich. Für die Mediation bei Einzel- oder Kollektivbeschwerden ist das «Personal Information Dispute Mediation Committee» zuständig. Bei Meinungsverschiedenheiten zwischen betroffenen Personen und datenverarbeitenden Institutionen kann dieses Komitee einen Schlichtungsvorschlag unterbreiten (Art. 47 PIPA). Beschwerden im Zusammenhang mit den Informationstechnologien werden von der «Korea Internet & Security Agency» behandelt. Diese betreibt eine Hotline und hat verschiedene Anleitungen und Empfehlungen für den privaten Sektor erarbeitet. Das Innenministerium hat eine wichtige Funktion bei der Umsetzung der Datenschutzgesetzgebung. Zu seinen Aufgaben gehört die Erarbeitung eines drei Jahre gültigen «Data Protection Basic Plan» (Art. 9 PIPA) und von Richtlinien (Art. 12 PIPA).

Gemäss Artikel 4 PIPA haben Privatpersonen das Recht, sich über die Bearbeitung von Daten über sie zu informieren. In diesem Zusammenhang können sie die Löschung oder Berichtigung bestimmter Daten verlangen. Im Gesetz ist auch ein Anspruch auf Schadenersatz vorgesehen.

Für die Datenbearbeitung muss der Verantwortliche die Einwilligung der betroffenen Person einholen (Art. 22 PIPA). Der Verantwortliche muss die betroffene Person informieren, wenn er von einer Drittperson erhaltene Daten bearbeitet (Art. 20 PIPA). Nach Ablauf der vereinbarten Frist oder wenn der Zweck erfüllt ist, muss er die Daten vernichten (Art. 21 PIPA). In Kapitel IV PIPA sind Garantien festgehalten, welche der Verantwortliche gewährleisten muss. Gemäss Artikel 29 sind die Verantwortlichen verpflichtet, alle notwendigen physischen, technischen und administrativen Massnahmen zu ergreifen, um den Verlust, den Diebstahl, die Verbrei-

tung, die Fälschung oder die Vernichtung von Daten zu verhindern. Die Informationen müssen so bearbeitet werden, dass die Risiken einer Verletzung der Privatsphäre auf das Mindestmass beschränkt werden (Art. 3 Abs. 6 PIPA), und für die Bearbeitung müssen die Daten anonymisiert werden (Art. 3 Abs. 7 PIPA).

Im Weiteren müssen Datenschutzverantwortliche in Unternehmen eine Datenschutzstrategie erarbeiten und veröffentlichen (Privacy Policy) (Art. 30 PIPA). Ausserdem wird verlangt, dass ein Datenschutzberater (Privacy Officer) bezeichnet wird (Art. 31 PIPA). Die öffentlichen Institutionen müssen ihre Datenerhebungen registrieren (Art. 32 PIPA) und eine Folgenabschätzung der Datenbearbeitungen vornehmen (Art. 35 PIPA), die ebenfalls registriert wird.

6.4 Japan

Japan verfügt seit 2016 über eine Aufsichtsbehörde im Bereich des Datenschutzes (Personal Information Protection Commission), die Überwachungs-, Regulierungs- und Mediationsfunktionen ausübt. Ausserdem ist auf zwei weitere Institutionen hinzuweisen. Im privaten Sektor gibt das im Jahr 2003 verabschiedete Datenschutzgesetz (Act on the Protection of Personal Information, im Folgenden «APPI»)[81] privaten Datenschutzorganisationen, die über eine Akkreditierung des Ministeriums verfügen, die Möglichkeit, gegen Unternehmen gerichtete Beschwerden zu bearbeiten und Informationen zu liefern, die zu einer besseren Umsetzung des Datenschutzes beitragen. Ferner können sie Massnahmen ergreifen, die für die Umsetzung der Datenschutzgrundsätze erforderlich sind (Art. 37 APPI). Im öffentlichen Sektor ist das «Information Disclosure and Personal Information Protection Review Board» dafür zuständig, den Datenschutz im Rahmen von Untersuchungen zur Transparenz zu gewährleisten.

Der APPI räumt Privatpersonen das Recht ein, Informationen über das Bestehen und den Zweck einer Datenbearbeitung zu erhalten (Art. 24 Abs. 2 und Art. 25 APPI). Für die Bearbeitung eines Antrags können Gebühren erhoben werden (Art. 30 APPI). Im Weiteren können betroffene Personen die Berichtigung, Ergänzung oder Löschung falscher Daten verlangen. In diesem Zusammenhang ist der Verantwortliche verpflichtet, die vorgebrachten Beschwerdegründe zu prüfen und die betroffene Person über eine allfällige Ablehnung ihres Antrags in Kenntnis zu setzen (Art. 30 APPI). Privatpersonen können ebenfalls die Aussetzung einer Datenbearbeitung oder die Löschung von Daten erwirken, wenn eine Datenbearbeitung ihrem Zweck widerspricht oder wenn die Daten mit unlauteren Mitteln beschafft wurden. Ein solches Gesuch ist jedoch nicht zulässig, falls es hohe Kosten verursachen könnte oder wenn es sich als zu kompliziert erweist und der Verantwortliche andere Massnahmen zum Schutz der Daten und Interessen der betroffenen Person ergriffen hat (Art. 27 APPI). Die gleichen Grundsätze gelten für die Datenübermittlung an Dritte (Art. 27 Abs. 2 APPI).

81 Der APPI ist auf Englisch unter folgender Adresse verfügbar: www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

Der Verantwortliche muss den Zweck der Datenbearbeitung möglichst genau angeben (Art. 15 Bst. f APPI). Ausserdem müssen die Informationen zum Zweck der Datenbearbeitung und zu den Rechten der betroffenen Personen der Öffentlichkeit zur Verfügung gestellt werden (Art. 24 APPI). Der Verantwortliche muss die Einwilligung der betroffenen Personen einholen, wobei eine stillschweigende Zustimmung auszureichen scheint. Er darf Daten nicht mit betrügerischen oder unlauteren Mitteln beschaffen (Art. 17 APPI) und muss alles daran setzen, die Richtigkeit der Daten sicherzustellen. Die Übermittlung von Daten an Dritte ist nur in einigen bestimmten Fällen zulässig (beispielsweise um das Leben oder die körperliche Unversehrtheit einer Person zu schützen, um die öffentliche Gesundheit zu wahren oder im Rahmen der Zusammenarbeit mit Behörden; Art. 23 APPI). Grundsätzlich müssen Sicherheitsmassnahmen getroffen werden, um den Verlust oder die Beschädigung von Daten zu verhindern (Art. 20 APPI), und die Personen, die mit der Bearbeitung von Daten beauftragt sind, müssen beaufsichtigt werden (Art. 21 Bst. f APPI). Das Gesetz umfasst jedoch keine Informationspflicht bei einem Datenverlust.

Abgesehen vom bereits erwähnten Artikel 20 APPI liegen keine Informationen zu spezifischen Massnahmen vor, mit denen der Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gefördert werden soll. Es ist indessen davon auszugehen, dass die Aufsichtsbehörde demnächst entsprechende Massnahmen ergreifen wird.

6.5 Singapur

Die zuständige Aufsichtsbehörde ist die «Personal Data Protection Commission» (PDPC). Diese wurde 2013 geschaffen, um den 2012 in Kraft getretenen Personal Data Protection Act[82] (PDPA) umzusetzen. Die PDPC übt unter anderem eine Aufsichts- und Regulierungsfunktion in Bezug auf Datenbearbeitungen aus, die von privaten Organisationen durchgeführt werden (der PDPA findet auf den öffentlichen Sektor keine Anwendung). Sie kann Richtlinien oder Verfügungen erlassen, um die Einhaltung des PDPA zu gewährleisten. Bei Gesetzesverstössen kann sie sogar eine Busse von höchstens 1 Million Dollar aussprechen (Art. 28 und 29 PDPA). Der PDPC stehen diesbezüglich umfangreiche Untersuchungsmassnahmen zur Verfügung. Diese reichen vom Recht, in Privatwohnungen einzudringen, bis zum Recht, das Aushändigen von Informationen und Dokumenten zu verlangen, die beschlagnahmt werden können (Anhang 9 PDPA). Die PDPC kann aber auch versuchen, Streitigkeiten mit einer Mediation beizulegen (Art. 27 PDPA). Im Weiteren erarbeitet und realisiert die PDPC politische Konzepte (beispielsweise durch den Erlass von Verhaltensregeln), um die verschiedenen Organisationen und Privatpersonen für die Berücksichtigung des Datenschutzes zu sensibilisieren. Schliesslich vertritt die PDPC die Regierung Singapurs auf internationaler Ebene bei allen Fragen im Zusammenhang mit dem Datenschutz (Art. 6 PDPA).

82 Der PDPA ist auf Englisch unter folgender Adresse verfügbar: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0.

Die betroffenen Personen können Auskunft über ihre Personendaten verlangen, über die eine Organisation verfügt oder die von ihr kontrolliert werden. Sie haben auch das Recht, über die Art und Weise informiert zu werden, wie ihre Personendaten im Jahr vor ihrem Gesuch verwendet oder bekannt gegeben wurden, sofern dem kein überwiegendes öffentliches oder privates Interesse entgegensteht (Art. 21 PDPA). Im Weiteren können die betroffenen Personen im Zusammenhang mit ihren Personendaten die Berichtigung falscher Informationen oder die Ergänzung fehlender Angaben verlangen (Art. 22 PDPA).

Sobald die Verantwortlichen Personendaten beschaffen, verwenden oder bekannt geben, sind sie grundsätzlich verpflichtet, sich über die ausdrückliche oder stillschweigende Einwilligung der betroffenen Personen zu vergewissern. Das Einwilligungserfordernis seitens der betroffenen Person ist jedoch weniger weitgehend als in den anderen untersuchten Rechtsordnungen. So sieht das Singapurer Recht zahlreiche Ausnahmen vor, bei denen die Einwilligung nicht notwendig ist oder als gegeben vorausgesetzt werden kann (Art. 13–15 PDPA). Die Datenbearbeitung muss zu einem Zweck durchgeführt werden, welcher der betroffenen Person bekannt ist oder der jeder Person unter den gleichen Umständen als sinnvoll erscheint (Art. 18 PDPA). Die Verantwortlichen müssen für die Richtigkeit der Daten sorgen (Art. 23 PDPA) und sie sind verpflichtet, geeignete Vorsichtsmassnahmen zu ergreifen, um das Abhandenkommen, das Kopieren oder den unerlaubten Zugriff auf in ihrem Besitz befindliche Personendaten zu verhindern (Art. 24 PDPA). Die Verantwortlichen müssen Personendaten vernichten oder anonymisieren, sobald deren Aufbewahrung nicht mehr dem Zweck ihrer Beschaffung entspricht und nicht durch einen rechtlichen oder wirtschaftlichen Grund gerechtfertigt ist (Art. 25 PDPA). Die grenzüberschreitende Bekanntgabe von Personendaten ist nur zulässig, wenn das Empfängerland ein Schutzniveau gewährleistet, das mit jenem von Singapur vergleichbar ist (Art. 26 PDPA).

Anscheinend wurden keine spezifischen Massnahmen zur Förderung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen vorgesehen. Die PDPC könnte jedoch gestützt auf ihre gesetzlich verankerte Befugnis, Massnahmen zur Sensibilisierung für den Datenschutz zu ergreifen (Art. 6 PDPA), solche Massnahmen vorsehen.

7 Umsetzung

Im Rahmen der RFA wurde angetönt, unbestimmte Rechtsbegriffe seien nach Möglichkeit zu vermeiden. Beim DSG handelt es sich indes um eine technologieneutrale Rahmengesetzgebung, welche auf eine Vielzahl unterschiedlich gelagerter Fälle anwendbar bleibt und sich dynamisch weiterentwickeln können muss. Bestimmte Begriffe und die Modalitäten bestimmter Rechte und Pflichten können in den Verhaltenskodizes bereichsspezifisch präzisiert werden. Ausserdem kann der Beauftragte weiterhin Leitfäden und andere Arbeitsinstrumente erarbeiten, um die Verantwortlichen und Auftragsbearbeiter bei ihren Aufgaben und die betroffenen Personen bei der Wahrnehmung ihrer Rechte zu unterstützen.

Im Weiteren wird die Verordnung vom 14. Juni 1993[83] zum Bundesgesetz über den Datenschutz (VDSG) angepasst, um das Gesetz nicht mit Detailregelungen zu überlasten.

In der Vorlage ist zwar nicht ausdrücklich eine Überprüfung ihrer Umsetzung vorgesehen, doch die Wirksamkeit ihrer Massnahmen wird gemäss Artikel 170 BV überprüft. Ausserdem muss der Beauftragte regelmässig einen Tätigkeitsbericht zuhanden der Bundesversammlung erarbeiten. Die Informationen dieses Berichts bieten eine Gesamtübersicht über die Umsetzung des künftigen DSG.

Die Übernahme der Richtlinie (EU) 2016/680 durch die Schweiz und die Ratifizierung des Änderungsprotokolls zum Übereinkommen SEV 108 durch die Schweiz ist auch für die Kantone bindend. Diese müssen ihre kantonalen Gesetzgebungen insoweit anpassen, als sie die Anforderungen dieser Instrumente nicht erfüllen.

8 Abschreibung parlamentarischer Vorstösse

Die folgenden parlamentarischen Vorstösse können abgeschrieben werden:

- Postulat Hodgers 10.3383 «Anpassung des Datenschutzgesetzes an die neuen Technologien»: Durch die Revision des DSG und dessen Anpassung an die neuen Technologien hat der Bundesrat das Postulat erfüllt.
- Postulat Graber 10.3651 «Angriff auf die Privatsphäre und indirekte Bedrohungen der persönlichen Freiheit»: Dieses Postulat wurde durch den Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz teilweise erfüllt. Mit der Revisionsvorlage nimmt der Bundesrat die verbleibenden Fragen auf, d. h. die Grenzen, die hinsichtlich der Technologien zur Überwachung und zur Informationserfassung festgelegt werden sollen, und die Frage, ob er es als sinnvoll erachtet, eine Verschärfung der Gesetzgebung zum Schutz der Privatsphäre und von persönlichen Daten vorzuschlagen.
- Postulat Schwaab 12.3152 «Recht auf Vergessen im Internet»: Der Bundesrat hat geprüft, ob es zweckmässig ist, ein «Recht auf Vergessen im Internet» in die Gesetzgebung aufzunehmen und dieses Recht zu präzisieren. Zudem hat er geprüft, wie die Nutzerinnen und Nutzer dieses Recht besser geltend machen können. Das Recht auf Vergessenwerden, ob im Internet oder anderweitig, besteht im DSG bereits. Durch die ausdrückliche Erwähnung des Rechts auf Löschung im E-DSG möchte der Bundesrat erreichen, dass das Gesetz für die betroffenen Personen verständlicher ist. Detailliertere Bestimmungen zu Fragen im Zusammenhang mit dem Internet würden dem technologieneutralen Charakter des Gesetzes widersprechen. Der Bundesrat zieht es vor, wenn in diesem Bereich auf die Verhaltenskodizes der betroffenen Kreise und die Leitfäden des Beauftragten gesetzt wird.

[83] SR **235.11**

- Postulat Recordon 13.3989 «Verletzungen der Persönlichkeitsrechte im Zuge des Fortschritts der Informations- und Kommunikationstechnik»: Im Rahmen der Revisionsarbeiten hat der Bundesrat die neuen Bedrohungen für die Persönlichkeitsrechte geprüft. Der E-DSG enthält Massnahmen zum verbesserten Schutz der Persönlichkeitsrechte.
- Motion Comte 14.3288 «Identitätsmissbrauch. Eine strafbare Handlung für sich»: Mit der Einführung von Artikel 179^{decies} im E-StGB ist diese Motion umgesetzt worden.
- Postulat Derder 14.3655 «Die digitale Identität definieren und Lösungen für ihren Schutz finden»: Der Bundesrat hat die Möglichkeit, im Rahmen der Vorlage die digitale Identität zu definieren, geprüft. Angesichts des technologieneutralen Charakters des Gesetzes hat er darauf verzichtet. Mit den vorgeschlagenen Massnahmen kann jedoch auch die digitale Persönlichkeit der Bürgerinnen und Bürger besser geschützt werden. Die Frage der digitalen Identität kann im Übrigen bei den Arbeiten der Expertenkommission «Zukunft der Datenbearbeitung und Datensicherheit», die 2018 abgeschlossen werden, genauer untersucht werden.
- Postulat Schwaab 14.3739 «Control by Design. Die Rechte auf Eigentum im Falle von unerwünschten Verbindungen verstärken»: Dieses Postulat wird durch den E-DSG insofern erfüllt, als die betroffenen Personen durch seinen Inhalt künftig besser geschützt werden. Die weiteren Aspekte des Postulats, vor allem jene im Zusammenhang mit der Produktsicherheit und der Sicherheit des Internets, werden im Rahmen der Arbeiten der Expertenkommission «Zukunft der Datenbearbeitung und Datensicherheit» vertieft werden.
- Postulate FDP-Liberale Fraktion 14.4137 und Comte 14.4284 «Videoaufnahmen durch Private. Die Privatsphäre besser schützen»: Gemäss dem E-DSG soll der strafrechtliche Teil des Gesetzes ausgebaut werden. Künftig kann die Beschaffung von Daten als Verstoss gegen die Informationspflicht – diese Pflicht wird im privaten Sektor auf alle Arten von Daten ausgeweitet – wirksamer sanktioniert werden. In Kombination mit den geltenden Bestimmungen zu den strafbaren Handlungen gegen den Geheim- oder Privatbereich bietet diese Änderung einen erweiterten Schutz. Im E-DSG wird ausserdem vorgesehen, dass ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, welches den für die Datenbearbeitung Verantwortlichen zur Erstellung einer Datenschutz-Folgenabschätzung verpflichtet, unter anderem vorliegt, wenn systematisch umfangreiche öffentliche Bereiche überwacht werden (Art. 20 Abs. 2 Bst. c E-DSG).
- Postulat Béglé 16.3383 «Elektronische Daten: Information der Geschädigten im Falle eines Hackerangriffs»: Nach Artikel 22 E-DSG müssen Verletzungen der Datensicherheit dem Beauftragten gemeldet werden und unter bestimmten Umständen muss auch die betroffene Person informiert werden. Der Inhalt der Meldung bzw. der Information wird in der Verordnung präzisiert.
- Postulat Béglé 16.3384 «Elektronische medizinische Daten. Eine geschützte, transparente und zielgerichtete Datenerhebung im revidierten Bundesgesetz

über den Datenschutz sicherstellen»: Das Datenschutzgesetz gilt für medizinische Daten unter Vorbehalt der Spezialgesetze. Der E-DSG sieht verschiedene neue Pflichten des Verantwortlichen und des Auftragsbearbeiters vor, die gegebenenfalls auch für medizinische Daten gelten. Diese Pflichten gehen in die Richtung der Forderungen des Postulats. Weitere Massnahmen wie beispielsweise die Stärkung der Kompetenzen des Beauftragten und die Verschärfung der strafrechtlichen Sanktionen oder die Erarbeitung von Verhaltenskodizes und Leitfäden sollten auch im Bereich der medizinischen Daten zu einem verbesserten Schutz führen.

Die folgenden parlamentarischen Vorstösse sind teilweise umgesetzt:

- Postulat Schwaab 14.3782 «Richtlinien für den ‹digitalen Tod›»: Artikel 16 E-DSG sieht einerseits ein Recht auf Einsicht in Daten einer verstorbenen Person vor, andererseits bietet er den Erbinnen und Erben und gegebenenfalls der Willensvollstreckerin oder dem Willensvollstrecker die Möglichkeit, die Löschung von Daten der Erblasserin oder des Erblassers zu verlangen. Damit werden wesentliche Forderungen des Postulats umgesetzt. Weitere Elemente werden im Rahmen der Revision des Erbrechts geprüft.
- Postulat Derder 15.4045 «Recht auf Nutzung der persönlichen Daten. Recht auf Kopie»: Nach Auffassung des Bundesrates ist es nicht wünschenswert, bei der Revision des DSG ein Recht auf Datenportabilität einzuführen (vgl. Ziff. 1.7.4). Diese Frage wird im Rahmen der Strategie «Digitale Schweiz» geprüft werden (vgl. Ziff. 1.1.3).
- Postulat Béglé 16.3386 «Kontrolle über persönliche Daten. ‹Informationelle Selbstbestimmung› fördern»: Aus denselben Gründen wie beim Recht auf Datenportabilität (vgl. Ziff. 1.7.4) sieht der E-DSG auch keine Präzisierung der Wiedererlangung der Kontrolle über persönliche Daten vor. Die Frage wird im Rahmen der Strategie «Digitale Schweiz» geprüft werden (vgl. Ziff. 1.1.3).
- Postulat Schwaab 16.3682 «Die Tätigkeiten von Wirtschaftsauskunfteien einschränken»: Da es sich beim E-DSG um eine allgemeine Regelung handelt, werden darin keine spezifischen Bestimmungen zur Regelung der Tätigkeiten von Wirtschaftsauskunfteien eingeführt. Der Schutz der betroffenen Personen wird jedoch gestärkt, denn der E-DSG sorgt für eine höhere Transparenz der Datenbearbeitungen, stärkt die Rechte der betroffenen Personen und erweitert die Pflichten der Verantwortlichen und die Aufsicht durch den Beauftragten. Zudem werden im E-DSG die Voraussetzungen für die Rechtfertigung der Bearbeitung von Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person durch den Verantwortlichen verschärft (Art. 27 Abs. 2 Bst. c E-DSG). Der Bundesrat beabsichtigt, im Bericht in Erfüllung des Postulats zu prüfen, ob eine spezifische Regelung der Tätigkeiten der Wirtschaftsauskunfteien zweckmässig ist und welche rechtlichen Lösungen in Frage kämen.

9 Erläuterungen

9.1 Erläuterungen zum E-DSG

9.1.1 Ingress

Der Bundesrat erachtet es als angemessen, Artikel 97 Absatz 1 BV im Ingress einzufügen. Dieser weist dem Bund die Kompetenz zu, den Schutz der Konsumentinnen und Konsumenten zu regeln. Der E-DSG enthält nämlich einige Bestimmungen, die insbesondere die Transparenz der Datenbearbeitung, die Kontrolle durch die betroffenen Personen und das Aufsichtssystem des Beauftragten verbessern. Dadurch sind die Konsumentinnen und Konsumenten besser geschützt.

9.1.2 Zweck und Geltungsbereich sowie Aufsichtsbehörde des Bundes

Art. 1 Zweck

Der Zweck des künftigen DSG entspricht dem Zweck des geltenden Rechts (Art. 1 DSG). Das DSG konkretisiert auf Gesetzesebene das in Artikel 13 Absatz 2 BV festgehaltene Recht auf informationelle Selbstbestimmung im Zusammenhang mit Personendaten, d. h. das Recht der betroffenen Person, grundsätzlich selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen.[84]

Die Bestimmung wird lediglich redaktionell geändert, indem ausdrücklich der Schutz auf natürliche Personen beschränkt wird. Diese Anpassung erfolgt aufgrund des geänderten Geltungsbereichs (siehe die Erläuterungen zu Art. 2 E-DSG).

Art. 2 Geltungsbereich

Der Anwendungsbereich des DSG wird durch den E-DSG teilweise erweitert, dies insbesondere, um den Anforderungen des E-SEV 108 gerecht zu werden. So ist vorgesehen, die Ausnahmen in Bezug auf hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren (Art. 2 Abs. 2 Bst. c DSG) und diejenige betreffend öffentliche Register des Privatrechtsverkehrs (Art. 2 Abs. 2 Bst. d DSG) anzupassen.

Zudem ist darauf hinzuweisen, dass der E-DSG genau wie das bisherige Recht das Datenschutzrecht im Allgemeinen regelt. Falls die Bearbeitung von Personendaten in den Anwendungsbereich anderer Bundesgesetze fällt, gelten aufgrund der Lex-specialis-Regel (besondere Normen gehen der allgemeinen Norm vor) grundsätzlich die bereichsspezifischen Datenschutznormen.[85]

84 BGE **140** I 2 E. 9.1.
85 Vgl. hierzu BGE **128** II 311 E. 8; BBl **1988** 413, 444 und Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, N 286 ff.

Abs. 1 Anwendung für natürliche Personen

Das DSG gilt gemäss dem Vorentwurf für die Bearbeitung von Daten natürlicher Personen durch private Personen und Bundesorgane.

Aufhebung des Schutzes für Daten juristischer Personen

Mit dem E-DSG wird vorgeschlagen, auf den Schutz von Daten juristischer Personen zu verzichten. In den datenschutzrechtlichen Bestimmungen der Europäischen Union und des Europarates sowie in den entsprechenden Regelungen der meisten ausländischen Gesetzgeber ist kein solcher Schutz vorgesehen. Dieser Schutz ist nur von geringer praktischer Bedeutung, und der Beauftragte hat zu diesem Bereich noch nie eine Empfehlung abgegeben. Auch bleibt für juristische Personen ein umfassender Schutz unverändert bestehen, wie er durch die Artikel 28 ff. des Zivilgesetzbuchs (ZGB)[86] (Persönlichkeitsverletzungen wie beispielsweise Rufschädigung), das UWG, das Urheberrechtsgesetz vom 9. Oktober 1992[87] oder durch die Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen sowie Artikel 13 BV auf Verfassungsebene gewährleistet wird. Die Änderung erlaubt indessen, den Schutz in jenen Bereichen zu verbessern, in denen er derzeit nicht ausreichend umgesetzt wird und dadurch die Glaubwürdigkeit des Gesetzes zu erhöhen.[88] Diese Lösung hat auch den Vorteil, dass die Bekanntgaben von Daten juristischer Personen ins Ausland nicht mehr davon abhängt, ob im Empfängerland ein angemessener Schutz gewährleistet ist (Art. 13 E-DSG). Dies wird voraussichtlich zu einer Zunahme der Bekanntgabe ins Ausland beitragen. Festzuhalten ist auch, dass die meisten Expertinnen und Experten, die im Rahmen der RFA zur Revision des DSG befragt wurden, sowie die Mehrheit der Vernehmlassungsteilnehmer den Verzicht auf den Schutz von Daten juristischer Personen befürworteten.[89] Dasselbe gilt für das Parlament, das einer Motion, welche den Schutz von Daten juristischer Personen beibehalten wollte,[90] nicht zugestimmt hat.

Im Bereich der Datenbearbeitungen durch Bundesorgane hat die Aufhebung des Schutzes von Daten juristischer Personen zur Folge, dass die bundesrechtlichen Gesetzesgrundlagen, mit denen die Bundesorgane zur Bearbeitung von Personendaten ermächtigt werden, nicht mehr anwendbar sind, wenn diese Daten juristischer Personen bearbeiten. Nach Artikel 5 BV ist die Grundlage staatlichen Handelns jedoch das Recht. Der Gesetzesentwurf führt deshalb im RVOG für die Bundesorgane eine Reihe von Bestimmungen ein, welche deren Umgang mit Daten juristischer Personen regeln (vgl. Ziff. 9.2.8). Ausserdem soll eine Übergangsbestimmung während fünf Jahren mögliche Rechtslücken verhindern (vgl. Art. 66 E-DSG sowie die Erläuterungen unter Ziff. 9.1.11).

86 SR **210**
87 SR **231.1**
88 Zu dieser Frage siehe Drechsler Christian, Plädoyer für die Abschaffung des Datenschutzes für juristische Personen, AJP 2016, S. 80 ff., S. 85–86.
89 Vgl. S. 46 der RFA.
90 Motion Béglé 16.3379 «Förderung der Schweiz als universeller virtueller Datentresor».

Das Öffentlichkeitsgesetz vom 17. Dezember 2004[91] (BGÖ) räumt allen Personen das Recht ein, amtliche Dokumente der Bundesbehörden einzusehen, für die das Öffentlichkeitsprinzip gilt. Der neue Geltungsbereich des E-DSG hat zur Folge, dass der Zugang zu amtlichen Dokumenten, die Daten juristischer Personen enthalten, nicht mehr aus Datenschutzgründen eingeschränkt werden kann, sondern nur wenn dadurch Berufs-, Geschäfts- oder Fabrikationsgeheimnisse offenbart werden können (Art. 7 Abs. 1 Bst. g BGÖ) oder wenn das Risiko besteht, dass die Privatsphäre der juristischen Person beeinträchtigt wird, beispielsweise deren guter Ruf. Um die Rechte juristischer Personen beim Zugang zu amtlichen Dokumenten zu garantieren, wenn ein Gesuch sich auf Dokumente bezieht, bei denen die Gewährung des Zugangs die Privatsphäre der juristischen Person beeinträchtigen könnte, werden im Gesetzesentwurf einige Bestimmungen des BGÖ angepasst (vgl. Ziff. 9.2.7).

Die Aufhebung des Schutzes von Daten juristischer Personen bewirkt ebenfalls, dass diese gestützt auf den E-DSG kein Auskunftsrecht mehr geltend machen können. Sie können aber ihre Verfahrensrechte geltend machen und gegebenenfalls aufgrund des Öffentlichkeitsgesetzes Einsicht in öffentliche Dokumente verlangen, wenn diese Informationen enthalten, die sie betreffen.

Abs. 2 Ausnahmen vom Geltungsbereich

Das DSG ist wie bisher nicht anwendbar auf Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden (Art. 2 Abs. 2 Bst. a E-DSG); die redaktionelle Anpassung beinhaltet keine materiellen Änderungen.

Ebenfalls vom Geltungsbereich ausgenommen bleibt die Bearbeitung von Personendaten, die durch die eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen erfolgt (Art. 2 Abs. 2 Bst. b E-DSG); dies aus denselben Gründen wie sie der Bundesrat bereits in der Botschaft vom 23. März 1988[92] angeführt hat.

Nach Buchstabe c sind die institutionellen Begünstigten gemäss Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007[93] (GSG), die in der Schweiz Immunität von der Gerichtsbarkeit geniessen, dem E-DSG nicht unterstellt. In Bezug auf das IKRK wird damit die aktuelle Situation beibehalten und es werden die übrigen betroffenen institutionellen Begünstigten ausdrücklich erwähnt. Diese anderen betroffenen institutionellen Begünstigten geniessen gestützt auf das Völkerrecht und das GSG selber auch Unabhängigkeit und Handlungsfreiheit, damit sie ihre internationalen Funktionen erfüllen können. Von einem Staat kann nicht erwartet werden, dass er sich in Bezug auf die Daten, die von seinen diplomatischen oder konsularischen Vertretungen bearbeitet werden, den Regeln des Schweizer Rechts unterwirft. Die Schweiz ist ihrerseits nicht verpflichtet, in Bezug auf ihr Vertretungsnetz im Ausland die ausländischen Regeln über den Datenschutz zu beachten. Auch von einer internationalen Organisation, die definitionsgemäss Aktivitäten in zahlreichen Staaten durchführt, kann nicht verlangt werden, dass sie die Anforderungen des

91 SR **152.3**
92 BBl **1988** II 413, 441.
93 SR **192.12**

nationalen Rechts eines jeden Staates, in dem sie tätig ist, befolgt, denn dies würde es ihr verunmöglichen, die Funktionen, die ihr kraft ihrer Statuten zugewiesen wurden, zu erfüllen.

Abs. 3 Bearbeitung von Personendaten in Verfahren

Nach Artikel 2 Absatz 3 E-DSG regelt das anwendbare Verfahrensrecht die Bearbeitung von Personendaten und die Rechte der betroffenen Personen in Gerichtsverfahren und in Verfahren nach bundesrechtlichen Verfahrensordnungen. Die Norm regelt das Verhältnis des DSG zum Verfahrensrecht und hält als allgemeinen Grundsatz fest, dass ausschliesslich das anwendbare Verfahrensrecht darüber bestimmt, wie im Rahmen der Verfahren Personendaten bearbeitet werden und wie die Rechte der betroffenen Personen ausgestaltet sind. Das Verfahrensrecht stellt im Rahmen seiner Regelungen ebenfalls den Schutz der Persönlichkeit und der Grundrechte aller Beteiligten sicher und gewährleistet damit einen dem DSG äquivalenten Schutz. Käme in diesem Bereich das DSG zur Anwendung, bestünde die Gefahr von Normkollisionen und Widersprüchen, die das austarierte System der jeweils anwendbaren Verfahrensordnung stören könnten. Aus diesen Gründen sieht auch Artikel 9 Ziffer 1 Buchstabe a E-SEV 108 eine entsprechende Ausnahme vor. Materiell entspricht die Regelung im E-DSG dem geltenden Recht.

Unter die Ausnahme von Absatz 3 fallen nach dem Wortlaut zunächst «Gerichtsverfahren». Hierzu zählen sämtliche Verfahren vor kantonalen und eidgenössischen Straf-, Zivil- und Verwaltungsgerichten, aber auch vor Schiedsgerichten mit Sitz in der Schweiz. Weiter erfasst die Ausnahme sämtliche Verfahren nach bundesrechtlichen Verfahrensordnungen unabhängig davon, vor welcher Behörde sie stattfinden. Zu den bundesrechtlichen Verfahrensordnungen gehören namentlich das Bundesgerichtsgesetz vom 17. Juni 2005[94] (BGG), das Verwaltungsgerichtsgesetz vom 17. Juni 2005[95] (VGG), das Patentgerichtsgesetz vom 20. März 2009[96], das VwVG, soweit es nicht um das erstinstanzliche Verwaltungsverfahren geht, die Zivilprozessordnung[97] (ZPO), das Bundesgesetz vom 11. April 1889[98] über Schuldbetreibung- und Konkurs (SchKG), die StPO, das VStrR, der Militärstrafprozess vom 23. März 1979[99] und das IRSG.

Anders als das bisherige Recht verzichtet der E-DSG auf den Begriff des hängigen Verfahrens, weil lediglich im Zivilprozessrecht von Rechtshängigkeit die Rede ist und dieser Begriff deshalb mitunter zu Abgrenzungsproblemen führte. Massgebend ist nun, ob ein Verfahren vor einem Gericht stattfindet oder von einer bundesrechtlichen Verfahrensordnung geregelt ist. Ein Verfahren findet vor einem Gericht statt, wenn dieses zum ersten Mal mit einem Fall befasst ist, indem das Verfahren nach der massgebenden Verfahrensordnung eingeleitet wurde. Ein Verfahren ist durch bundesrechtliche Verfahrensordnungen geregelt, sobald ein bestimmter Sachverhalt durch eine Behörde entsprechend den Vorschriften in einem dieser Gesetze behan-

94 SR **173.110**
95 SR **173.32**
96 SR **173.41**
97 SR **272**
98 SR **281.1**
99 SR **322.1**

delt wird. Die massgebende Verfahrensordnung bleibt auch nach Abschluss des Verfahrens anwendbar. Damit die Aktenlage nicht nachträglich durch prozessfremde Instrumente verändert werden kann, sieht das Prozessrecht eigenständige Verfahren zur Aktenpflege, zur Akteneinsicht und zur Aktenaufbewahrung vor. Wesentliches Abgrenzungskriterium für die Nichtanwendbarkeit des DSG ist somit zusammenfassend, ob funktional betrachtet ein unmittelbarer Zusammenhang zu einem (Gerichts-) Verfahren besteht oder nicht. Ein solcher liegt vor, wenn die fragliche Bearbeitung von Personendaten konkrete Auswirkungen auf dieses Verfahren oder dessen Ausgang oder die Verfahrensrechte der Parteien haben kann.

Wenn die Vorschrift von Absatz 3 zum Tragen kommt, regelt ausschliesslich das anwendbare Verfahrensrecht die Bearbeitung von Personendaten und die Rechte der betroffenen Personen. Sowohl Datenbearbeitungen des Gerichts gegenüber den Verfahrensbeteiligten als auch Datenbearbeitungen, welche die Beteiligten gegenüber anderen Verfahrensbeteiligten durchführen, richten sich nach dem anwendbaren Verfahrensrecht. Dies gilt insbesondere für die Rechte der Parteien zur Kenntnisnahme der ins Verfahren einfliessenden Daten und zur allfälligen Berichtigung bestimmter Daten sowie für die Datenbearbeitung im Rahmen der gerichtlichen Verfahren im Allgemeinen. Das bedeutet namentlich, dass die verschiedenen Rechtsbehelfe nach dem DSG weder gegenüber Datenbearbeitungen des Gerichts im Rahmen des Verfahrens noch gegenüber Datenbearbeitungen der anderen Verfahrensbeteiligten zum Tragen kommen. So können die Verfahrensbeteiligten beispielsweise kein Auskunftsrecht nach dem DSG geltend machen, um beim Gericht Akteneinsicht zu erhalten oder bei anderen Verfahrensbeteiligten Beweismittel zu beschaffen (vgl. hierzu Ziff. 9.1.5). Es ist mit anderen Worten nicht möglich, auf dem Wege des DSG verfahrensrelevante Handlungen gegenüber dem Gericht oder unter den Verfahrensbeteiligten vorzunehmen, welche nach dem fraglichen Verfahrensrecht ausgeschlossen wären oder aber umgekehrt unter bestimmten Voraussetzungen nach bestimmten Regeln und Grundsätzen zu erfolgen haben. Auch nach Abschluss des Verfahrens können die Akten lediglich nach den Vorschriften des Prozessrechts abgeändert werden (Berichtigung, Erläuterung, Revision), da die Akten mit dem Ergebnis eines Verfahrens übereinstimmen müssen. Nicht ausgeschlossen ist dadurch, dass das anwendbare Verfahrensrecht nach Abschluss des Verfahrens das DSG für anwendbar erklärt (vgl. Art. 99 StPO). Soweit das anwendbare Prozessrecht in Bezug auf das Akteneinsichtsrecht Dritter nach Abschluss des Verfahrens keine Vorschriften enthält, sollte sich die Rechtsanwendung an den Bestimmungen des DSG orientieren.

Anders als noch die Vernehmlassungsvorlage nimmt der Absatz 3 damit nicht mehr lediglich die Datenbearbeitungen bestimmter Institutionen vom Anwendungsbereich des DSG aus, was in der Vernehmlassung erheblich kritisiert wurde. Vielmehr sind auch Datenbearbeitungen durch die Parteien erfasst. Zudem wird der Normenkonflikt auf andere Weise gelöst, indem die Norm das anwendbare Recht bestimmt. Insbesondere für die eidgenössischen Gerichte bedeutet dies im Ergebnis jedoch nach wie vor, dass sie vom Anwendungsbereich des DSG ausgenommen sind, was Datenbearbeitungen im Rahmen ihrer Rechtsprechungstätigkeit angeht, wodurch der Gewaltenteilung Rechnung getragen wird.

Im Umkehrschluss ergibt sich aus Artikel 2 Absatz 3 jedoch auch, dass das DSG anwendbar ist auf Datenbearbeitungen durch die administrativen Dienste von Gerichten und Behörden, wie beispielsweise die Bearbeitung von Daten über das Personal.[100] Ebenfalls müssen die Gerichte bei der Archivierung von Beweismitteln und Entscheiden die Datensicherheit gewährleisten. Dabei bestehen jedoch Ausnahmen von der Aufsicht durch den Beauftragten (vgl. Art. 3 Abs. 2 E-DSG und die Erläuterungen).

Die Vorschrift von Artikel 2 Absatz 3 E-DSG gilt nach Satz 2 nicht für erstinstanzliche Verwaltungsverfahren. Diese Regelung aus dem bisherigen Recht wird unverändert beibehalten.

Abs. 4 Öffentliche Register des Privatrechtsverkehrs

Die in Artikel 2 Absatz 2 Buchstabe d DSG vorgesehene Ausnahme betreffend die öffentlichen Register des Privatrechtsverkehrs ist mit den Anforderungen von Artikel 3 E-SEV 108 nicht vereinbar. Das künftige Übereinkommen sieht nämlich keine Ausnahme für solche Register vor. Das Gleiche gilt für die Verordnung (EU) 2016/679.

Auch wenn es im Interesse der betroffenen Personen liegt, dass die öffentlichen Register des Privatrechtsverkehrs die Grundsätze des Datenschutzes einhalten, so besteht doch auch ein öffentliches Interesse an der Führung dieser Register und am Zugang dazu (siehe Erwägung 73 der Verordnung [EU] 2016/679). In einem Urteil vom 9. März 2017[101] hatte der Gerichtshof der Europäischen Union die Gelegenheit, sich zur Abgrenzung zwischen dem Datenschutz und der Öffentlichkeit eines von den italienischen Behörden geführten Handelsregisters zu äussern. In dieser Rechtssache verlangte ein ehemaliger Verwalter und Liquidator eines in Konkurs geratenen Unternehmens die Löschung bestimmter Daten zu seiner Person aus dem genannten Register. Zur Beilegung dieser Rechtsstreitigkeit ersuchte das italienische Kassationsgericht den Gerichtshof, zu prüfen, ob der in Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG verankerte Grundsatz der Datenaufbewahrung, wie in der ersten Richtlinie 68/151/EWG[102] vorgesehen, Vorrang vor dem Regime der Öffentlichkeit von Handelsregistern haben soll. Nach diesem Grundsatz werden persönliche Daten nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt, die die Identifizierung der betroffenen Personen ermöglicht.

Gemäss dem Gerichtshof soll die Öffentlichkeit des Handelsregisters die Rechtssicherheit zwischen den Unternehmen und Dritten gewährleisten und Letzteren ermöglichen, von wesentlichen Aktivitäten des betreffenden Unternehmens und von bestimmten Daten zu den vertretungsberechtigten Personen Kenntnis zu erlangen. Die Öffentlichkeit solcher Informationen ist auch nach der Auflösung eines Unter-

100 Vgl. bereits BBl **1988** II 443.
101 Urteil EuGH vom 9. März 2017, Rs. C-398/15, ECLI:EU:C:2017:197 (Manni).
102 Erste Richtlinie 68/151/EWG des Rates vom 9. März 1968 zur Koordinierung der Schutzbestimmungen, die in den Mitgliedstaaten den Gesellschaften im Sinne des Artikels 58 Absatz 2 des Vertrages im Interesse der Gesellschafter sowie Dritter vorgeschrieben sind, um diese Bestimmungen gleichwertig zu gestalten, ABl. L 65 vom 14.3.1968, S. 8.

nehmens gerechtfertigt. Denn es kann sich beispielsweise als notwendig erweisen, im Hinblick auf ein mögliches Gerichtsverfahren die Rechtmässigkeit von Handlungen eines Unternehmens während seiner Geschäftstätigkeit zu überprüfen. Gemäss dem Gerichtshof verunmöglichen aber die unterschiedlichen Verjährungsregelungen in den Mitgliedstaaten die Festlegung einer einheitlichen Frist ab Auflösung des Unternehmens, nach deren Ablauf die im Handelsregister erfassten Daten nicht mehr benötigt werden. Vor diesem Hintergrund hält der Gerichtshof fest, dass die Mitgliedstaaten nach Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG den betroffenen Personen beispielsweise nicht ein Recht auf Löschung ihrer Personendaten nach einer bestimmten Frist ab Auflösung des Unternehmens gewährleisten können. Wenn die Rechtssicherheit und der Schutz der Interessen Dritter überwiegen, ist es dennoch nicht ausgeschlossen, dass eine Person in besonderen und aussergewöhnlichen Situationen ein überwiegendes und schützenswertes Interesse daran geltend machen kann, dass der Zugang zu ihren Personendaten eingeschränkt wird. Der Gerichtshof kommt deshalb zum Schluss, dass es den Mitgliedstaaten obliegt zu bestimmen, ob die betroffenen Personen von der registerführenden Behörde verlangen können, im Einzelfall zu prüfen, ob es aufgrund eines überwiegenden schützenswerten Interesses ausnahmsweise gerechtfertigt ist, nach Ablauf einer ausreichenden Frist nach der Auflösung des betroffenen Unternehmens den Zugang zu ihren Personendaten einzuschränken. Zwar stützt sich das Urteil des Gerichtshofs auf die Richtlinie 95/46/EG, die ab Inkrafttreten der Verordnung (EU) 2016/679 nicht mehr anwendbar ist, die Erwägungen dieses Urteils bewahren ihre Gültigkeit aber auch für die neue Gesetzgebung.

Nach dem in Artikel 9 ZGB festgelegten Grundsatz erbringen öffentliche Register für die durch sie bezeugten Tatsachen vollen Beweis, solange nicht die Unrichtigkeit ihres Inhalts nachgewiesen ist. Angesichts des Zwecks dieser Register ist der Bundesrat der Ansicht, dass Datenschutzgründe die Öffentlichkeit der Register des Privatrechtsverkehrs nicht beeinträchtigen dürfen. Dasselbe gilt für die Register im Bereich des Immaterialgüterrechts: Der Gesetzgeber hat bereits eine Interessenabwägung vorgenommen und garantiert die Öffentlichkeit dieser Register. Nach Ansicht des Bundesrates ist es nicht Aufgabe des DSG, die Rechte der betroffenen Personen auf diesem Gebiet zu regeln. Deshalb ist in Absatz 4 eine Einschränkung zugunsten der Spezialbestimmungen des Bundesrechts vorzusehen. Die Änderung betrifft ausschliesslich öffentliche Register des Privatrechtsverkehrs, die von Bundesbehörden geführt werden, d. h. das elektronische Zivilstandsregister, Zefix, das Luftfahrzeugbuch des Bundesamts für Zivilluftfahrt und die Register des Eidgenössischen Instituts für Geistiges Eigentum (insbesondere das Marken-, das Patent- und das Designregister).

Die öffentlichen Register des Privatrechtsverkehrs, für welche die Kantone zuständig sind, unterstehen dem kantonalen Datenschutzrecht. Dies gilt auch, wenn diese Daten im Rahmen des Vollzugs von Bundesrecht bearbeitet werden. Allerdings darf das kantonale Datenschutzrecht die korrekte und einheitliche Anwendung des Bundesprivatrechts und insbesondere den Grundsatz der Öffentlichkeit der Register nicht behindern. Die Aufhebung von Artikel 2 Absatz 2 Buchstabe d DSG hat daher auf die folgenden kantonalen Register keine Auswirkungen: das Grundbuch, das Schiffsregister, die kantonalen Handelsregister, die Betreibungs- und Konkursregister und das öffentliche Register über die Eigentumsvorbehalte. Absatz 4 hat eben-

falls keine Auswirkungen auf öffentlich-rechtliche Register wie z. B. das Medizinalberuferegister, auf die das betreffende Spezialgesetz anwendbar ist, subsidiär das DSG.

Räumlicher Geltungsbereich

Im Gegensatz zur Verordnung (EU) 2016/679 (Art. 3) enthält der E-DSG keine besondere Bestimmung zum räumlichen Geltungsbereich des Gesetzes. Nach Auffassung des Bundesrates bietet bereits das geltende Recht die Möglichkeit, das DSG weitgehend auf Situationen mit internationalem Charakter anzuwenden. Aufgrund der Auswirkungstheorie gilt dies auch für das öffentliche Recht.[103]

Die Schwierigkeiten sind weniger beim räumlichen Geltungsbereich anzusiedeln als bei der Umsetzung und Vollstreckung von Entscheiden, insbesondere im Bereich des Internets. Der Bundesrat hat geprüft, ob die Verantwortlichen und die Auftragsbearbeiter dazu verpflichtet werden sollen, ein Zustellungsdomizil in der Schweiz anzugeben, um die Vollstreckung von Entscheiden, die sie betreffen, zu erleichtern. Er hat schliesslich aus denselben Gründen darauf verzichtet, die bereits im Bericht vom 11. Dezember 2015 betreffend die zivilrechtliche Verantwortlichkeit von Providern dargestellt worden sind.[104] Vielmehr wäre eine Lösung über bi- oder multilaterale Rechtshilfeabkommen vorzuziehen, welche die direkte Postzustellung von Dokumenten ins Ausland ermöglichen. Solche Abkommen bestehen im Bereich des Zivilrechts bereits mit einigen Staaten, in denen bekannte Internetunternehmen ihren Sitz haben, wie beispielsweise Irland oder die Vereinigten Staaten. Der Bundesrat hat diesen Standpunkt im strafrechtlichen Bereich in seiner Stellungnahme zur Motion Levrat 16.4082 «Den Strafverfolgungsbehörden den Zugang zu Daten von sozialen Netzwerken erleichtern» bestätigt. Schliesslich weist er darauf hin, dass die Pflicht zur Bezeichnung eines Zustellungsdomizils im VwVG und im VGG vorgesehen ist.

Der Beauftragte hätte es vorgezogen, wenn die Gesetzesvorlage eine mit Artikel 3 der Verordnung (EU) 2016/679 vergleichbare Vorschrift enthalten hätte und die für die Datenbearbeitung Verantwortlichen verpflichtet worden wären, eine Vertretung in der Schweiz zu haben.

Art. 3 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Abs. 1 Aufsicht durch den Beauftragten

Absatz 1 nennt die zuständige Aufsichtsbehörde im Bereich des Datenschutzes. Er hält den Grundsatz fest, wonach der Beauftragte die Behörde ist, die für die Überwachung der Einhaltung der Datenschutzvorschriften des Bundes zuständig ist (vgl. Art. 39 ff. E-DSG).

103 Das Bundesgericht hat diesen Grundsatz auch auf den Datenschutz angewendet. Demnach besteht bei Bildern, die in der Schweiz aufgenommen und so veröffentlicht werden, dass sie in der Schweiz abrufbar sind, ein überwiegender Anknüpfungspunkt in der Schweiz, selbst wenn die Bilder im Ausland weiterbearbeitet und nicht direkt von der Schweiz aus ins Internet gestellt werden (BGE **138** II 346 E. 3.3 «Google Street View»).

104 www.ejpd.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-110/ber-br-d.pdf.

Im deutschen Gesetzestext wird ausschliesslich der männliche Begriff verwendet, wenn der Beauftragte in der fraglichen Bestimmung als Institution angesprochen ist. Dies ist in der Mehrheit der Gesetzesbestimmungen der Fall. Im ersten Abschnitt des 7. Kapitels ist hingegen (mit Ausnahme von Art. 42 E-DSG) von der Person der oder des Beauftragten die Rede. In diesen Bestimmungen werden die männliche und die weibliche Form verwendet.

Abs. 2 Ausnahmen von der Aufsicht

Absatz 2 sieht verschiedene Ausnahmen von der Aufsicht des Beauftragten vor. Diese Ausnahmen liegen im Wesentlichen darin begründet, dass die Unterstellung der genannten Behörden unter die Aufsicht des Beauftragten die Gewaltenteilung und die Unabhängigkeit der Justiz beeinträchtigen würde.

Die Bundesversammlung (Bst. a) und der Bundesrat (Bst. b) sind von der Aufsicht des Beauftragten ausgenommen.

Soweit die Bearbeitung von Personendaten durch die eidgenössischen Gerichte unter das DSG fällt, sind sie von der Aufsicht durch den Beauftragten ausgenommen (Bst. c). Die Ausnahme ist im Hinblick darauf zu betrachten, dass der Beauftragte im E-DSG neu die Kompetenz erhält, Verfügungen gegenüber Bundesorganen zu erlassen. Dadurch bestünde gegenüber den eidgenössischen Gerichten die Gefahr, dass die Unabhängigkeit der Gerichte und die Gewaltenteilung beeinträchtigt würden. Darüber hinaus sind namentlich das Bundesverwaltungsgericht und das Bundesgericht Beschwerdeinstanzen für Verfügungen des Datenschutzbeauftragten. Daher könnten sie dazu aufgerufen sein, einen Beschwerdeentscheid in eigener Sache zu fällen. Um den Anforderungen der Richtlinie (EU) 2016/680 und dem E-SEV 108 gerecht zu werden, wird jedes eidgenössische Gericht eine eigene unabhängige Datenschutzaufsicht in die Wege leiten. Diese wird, soweit angebracht, analog zu jener des Beauftragten ausgestaltet sein. Die Einrichtung erfolgt über die Anpassung der entsprechenden Verordnungen der jeweiligen eidgenössischen Gerichte, sobald das revidierte DSG in Kraft getreten ist.

Nach Buchstabe d ist auch die Bundesanwaltschaft von der Aufsicht durch den Beauftragten ausgenommen, soweit sie Personendaten im Rahmen von Strafverfahren bearbeitet.[105] Der Aufsicht des Beauftragten unterstellt bleiben hingegen die eidgenössischen Polizeibehörden, selbst wenn diese im Auftrag der Bundesanwaltschaft handeln. Der Beauftragte wendet dabei die Datenschutzbestimmungen des anwendbaren Verfahrensrechts an (vgl. Art. 2 Abs. 3 E-DSG).

Gemäss Buchstabe e sind schliesslich Bundesbehörden von der Aufsicht des Beauftragten ausgenommen, soweit sie Personendaten im Rahmen einer rechtsprechenden Tätigkeit oder von Verfahren der internationalen Rechtshilfe in Strafsachen bearbeiten. Diese Ausnahme betrifft hauptsächlich die Bundesanwaltschaft und das Bundesamt für Justiz. Nach der Erklärung des Bundesrates zu Artikel 1 des Europäischen Übereinkommens vom 20. April 1959[106] über die Rechtshilfe in Strafsachen ist das Bundesamt für Justiz als schweizerische Justizbehörde im Sinne des Übereinkommens zu betrachten. Die Ausnahme ist allerdings von beschränkter Tragweite.

105 Vgl. Erwägungsgrund 80 der Richtlinie (EU) 2016/680 sowie Artikel 18 dieser Richtlinie.
106 SR **0.351.1**

Denn der Beauftragte kann die Rechtmässigkeit einer Datenbearbeitung überprüfen, wenn eine betroffene Person ihre Rechte nach Artikel 11*c* E-IRSG geltend macht.

9.1.3 Allgemeine Bestimmungen

9.1.3.1 Begriffe und Grundsätze

Art. 4 Begriffe

Bst. a Personendaten

Es ist darauf hinzuweisen, dass der E-DSG grundsätzlich den Begriff der Personendaten verwendet. Innerhalb desselben Absatzes wird insbesondere im deutschen Text synonym auch der Begriff Daten verwendet, wenn eindeutig ist, dass damit Personendaten gemeint sind.

Der Begriff der Personendaten wird im Vergleich zum bisherigen Recht insofern verändert, als das DSG auf juristische Personen nicht mehr anwendbar ist. Bei Personendaten handelt es sich somit um alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Eine natürliche Person ist bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, beispielsweise über den Hinweis auf Informationen, die sich aus den Umständen oder dem Kontext ableiten lassen (Identifikationsnummer, Standortdaten, spezifische Aspekte, die ihre physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder gesellschaftliche Identität betreffen). Die Identifizierung kann über eine einzige Information möglich sein (Telefonnummer, Hausnummer, AHV-Nummer, Fingerabdrücke) oder über den Abgleich verschiedener Informationen (Adresse, Geburtsdatum, Zivilstand). Wie auch nach geltendem Recht reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei bestimmbar. So hält der Bundesrat in seiner Botschaft zum DSG von 1988 fest: «Ist der Aufwand für die Bestimmung der betroffenen Personen derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird […], liegt keine Bestimmbarkeit vor.»[107] Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Ob der Einsatz dieser Mittel vernünftig ist, muss mit Blick auf die Umstände, etwa den zeitlichen und finanziellen Aufwand für die Identifizierung, beurteilt werden. Dabei sind die zum Zeitpunkt der Bearbeitung verfügbaren Technologien und deren Weiterentwicklung zu berücksichtigen.

Das Gesetz gilt nicht für anonymisierte Daten, wenn eine Reidentifizierung durch Dritte unmöglich ist (die Daten wurden vollständig und endgültig anonymisiert) oder wenn dies nur mit einem hohen Aufwand möglich wäre, den kein Interessent auf sich nehmen würde. Das gilt ebenfalls für pseudonymisierte Daten.

[107] BBl **1988** II 444

Bst. b Betroffene Person

Betroffene Personen sind natürliche Personen, über die Daten bearbeitet werden. Die Beschränkung auf natürliche Personen ergibt sich aus der Aufhebung des Schutzes für Daten juristischer Personen (siehe die Erläuterungen zu Art. 2 Abs. 1 E-DSG unter Ziff. 9.1.2).

Bst. c Besonders schützenswerte Personendaten

Ziffer 1 wird nicht geändert.

Ziffer 2 wird ergänzt: Der Begriff der besonders schützenswerten Personendaten wird in Einklang mit der Richtlinie (EU) 2016/680 (Art. 10) und der Verordnung (EU) 2016/679 auf die Daten zur ethnischen Herkunft ausgeweitet. Der E-DSG behält den Verweis auf die Rassenzugehörigkeit bei. Wie die Europäische Union hält auch der Bundesrat fest, dass die Verwendung dieses Begriffs nicht bedeutet, dass er Theorien gutheisst, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen. Die Vorlage behält auch den Verweis auf die Daten über die Gesundheit und die Intimsphäre bei. Als Daten über die Intimsphäre gelten namentlich die Daten über das Sexualleben und die sexuelle Orientierung der betroffenen Person (siehe ebenfalls das Übereinkommen SEV 108 [Art. 6 Abs. 1], die Richtlinie [EU] 2016/680 [Art. 10] und die Verordnung [EU] 2016/679 [Art. 9]). Je nach Umständen kann auch die Geschlechtsidentität einer Person unter diesen Begriff (oder unter die Daten über die Gesundheit) fallen.

Der Begriff «besonders schützenswerte Personendaten» wird ausserdem auf genetische Daten (Ziff. 3) und biometrische Daten, die ein Individuum eindeutig identifizieren (Ziff. 4), ausgeweitet. Mit dieser Änderung werden die Anforderungen des E-SEV 108 (Art. 6 Abs. 1) sowie der Richtlinie (EU) 2016/680 (Art. 10) umgesetzt. Die Verordnung (EU) 2016/679 (Art. 9) sieht eine ähnliche Regelung vor.

Genetische Daten sind Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden; darin eingeschlossen ist auch das DNA-Profil (Art. 3 Bst. l des Bundesgesetzes vom 8. Oktober 2004[108] über genetische Untersuchungen beim Menschen [GUMG]).

Unter biometrischen Daten sind hier Personendaten zu verstehen, die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen. Es handelt sich dabei beispielsweise um einen digitalen Fingerabdruck, Gesichtsbilder, Bilder der Iris oder Aufnahmen der Stimme. Diese Daten müssen zwingend auf einem spezifischen technischen Verfahren beruhen, das die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt. Dies ist beispielsweise grundsätzlich nicht der Fall bei gewöhnlichen Fotografien.

108 SR **810.12**

Bst. d Bearbeiten

Der Begriff des Bearbeitens bleibt inhaltlich unverändert. Synonym wird häufig auch der Begriff der Bearbeitung verwendet. Die Liste wurde jedoch ergänzt um «Speichern» und «Löschen» mit dem Ziel, sich dem Wortlaut des Europäischen Rechts anzunähern (Art. 2 Bst. b E-SEV 108, Art. 4 Ziff. 2 der Verordnung [EU] 2016/679 und Art. 3 Ziff. 2 der Richtlinie [EU] 2016/680). Wie im aktuellen Recht ist die Liste der möglichen Bearbeitungsvorgänge nicht abschliessend, sodass zahlreiche Operationen darunter fallen können (Organisation, Sortieren, Verändern, Auswerten von Daten etc.). Der Begriff «Vernichten» ist stärker als der Begriff «Löschen» und impliziert, dass die Daten unwiderbringlich zerstört werden. Wenn die Daten auf Papier vorhanden sind, ist dieses zu verbrennen oder zu schreddern. Schwieriger gestaltet sich die Datenvernichtung bei elektronischen Daten. Wurden die Daten mittels einer CD oder eines USB-Sticks übermittelt, muss einerseits der Datenträger unbrauchbar gemacht werden und andererseits sind alle Kopien so zu behandeln, dass die Daten auch nicht mehr lesbar gemacht werden können. Bei Personendaten, die im Anhang eines E-Mails übermittelt wurden, müssen auch allfällige Zwischenspeicherungen dieses E-Mails vernichtet werden. Übliche Löschbefehle oder eine reine Umformatierung stellen keine Vernichtung, sondern eine Löschung dar.[109]

Anders als das Schweizer Recht verwendet die Europäische Union den Begriff des Verarbeitens statt des Bearbeitens. Aus Praktikabilitätsgründen wurde darauf verzichtet, das Schweizer Recht auch in dieser Hinsicht anzupassen, zumal inhaltlich kein Unterschied besteht.

Bst. f Profiling

Der Bundesrat schlägt vor, den Begriff «Persönlichkeitsprofil», der in Artikel 3 Buchstabe d DSG definiert ist, aufzuheben. Der Begriff «Persönlichkeitsprofil» ist eine Besonderheit unserer Gesetzgebung. Weder das europäische Recht noch andere ausländische Gesetzgebungen kennen diesen Begriff. Nach dem Inkrafttreten des DSG im Jahr 1992 kam ihm keine grosse Bedeutung zu[110], heute scheint er durch die Entwicklung neuer Technologien überholt. An seiner Stelle wird im E-DSG der Begriff des «Profiling» verwendet. Der Begriff findet sich in Artikel 3 Ziffer 4 der Richtlinie (EU) 2016/680 und Artikel 4 Ziffer 4 der Verordnung (EU) 2016/679. Obwohl die beiden Begriffe Ähnlichkeiten aufweisen, sind sie nicht deckungsgleich. Das Persönlichkeitsprofil ist das Ergebnis eines Bearbeitungsprozesses und erfasst damit etwas Statisches. Hingegen umschreibt das Profiling eine bestimmte Form der Datenbearbeitung, mithin einen dynamischen Prozess. Darüber hinaus ist der Vorgang des Profilings auf einen bestimmten Zweck ausgerichtet.

Der Begriff des Profilings wird aufgrund der Stellungnahmen in der Vernehmlassung inhaltlich an die europäische Terminologie angepasst und erfasst nun insbesondere nur noch die automatisierte Bearbeitung von Personendaten. So ist Profiling definiert als die Bewertung bestimmter Merkmale einer Person auf der Grundlage

109 Siehe BVGer 2015/13 E. 3.3.4 m. w. H.
110 Vgl. jedoch das Urteil des Bundesverwaltungsgerichts A-4232/2015 vom 18. April 2017 i.S. Moneyhouse AG (vgl. Ziff. 9.1.6).

von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Interessen, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen. Diese Analyse kann beispielsweise erfolgen, um herauszufinden, ob eine Person für eine bestimmte Tätigkeit geeignet ist. Ein Profiling ist mit anderen Worten dadurch gekennzeichnet, dass Personendaten automatisiert ausgewertet werden, um auf der Grundlage dieser Auswertung, ebenfalls in automatisierter Weise, die Merkmale einer Person zu bewerten. Ein Profiling liegt somit nur vor, wenn der Bewertungsprozess vollständig automatisiert ist. Als automatisierte Auswertung ist jede Auswertung mit Hilfe von computergestützten Analysetechniken zu betrachten. Dazu können auch Algorithmen verwendet werden, aber deren Verwendung ist nicht konstitutiv für das Vorliegen eines Profilings. Vielmehr ist lediglich verlangt, dass ein automatisierter Auswertungsvorgang stattfindet; liegt hingegen lediglich eine Ansammlung von Daten vor, ohne dass diese ausgewertet werden, erfolgt noch kein Profiling. Die automatisierte Bewertung erfolgt insbesondere, um bestimmte Verhaltensweisen dieser Person zu analysieren oder vorherzusagen. Das Gesetz nennt beispielhaft einige Merkmale einer Person wie die Arbeitsleistung, die wirtschaftliche Lage oder die Gesundheit. Denkbar sind aber auch andere Merkmale wie die Interessen, die Vertrauenswürdigkeit oder der Aufenthaltsort. Ohne Bedeutung ist dabei, ob der Verantwortliche, der das Profiling betreibt, dies für eigene Zwecke tut oder für einen Dritten.

Da der Begriff des Persönlichkeitsprofils nicht mehr verwendet wird, müssen auch die gesetzlichen Grundlagen angepasst werden, die Bundesorganen die Bearbeitung von Persönlichkeitsprofilen erlauben (vgl. Ziff. 9.2.2).

Daten, welche aufgrund eines Profilings entstehen, sind grundsätzlich Personendaten im Sinne von Artikel 4 Buchstabe a E-DSG. Je nach Gegenstand kann es sich dabei auch um besonders schützenswerte Personendaten handeln.

Bst. g Verletzung der Datensicherheit

Anders als der Vorentwurf enthält der E-DSG eine Definition der Verletzung der Datensicherheit, weil sich in der Vernehmlassung herausstellte, dass der Begriff zu wenig klar ist. Demnach handelt es sich um eine Verletzung der Datensicherheit, wenn ein Vorgang dazu führt, dass Personendaten verlorengehen, gelöscht oder vernichtet, verändert oder Unbefugten offengelegt oder zugänglich gemacht werden. Dies gilt ungeachtet davon, ob der Vorgang mit Absicht geschieht oder nicht, ob er widerrechtlich ist oder nicht. Der Begriff knüpft an Artikel 7 an, wonach der Verantwortliche und der Auftragsbearbeiter technische und organisatorische Massnahmen ergreifen müssen, um die Datensicherheit zu gewährleisten. Inhaltlich entspricht der Begriff Artikel 7 Absatz 2 E-SEV 108, Artikel 3 Ziffer 11 der Richtlinie (EU) 2016/680 und Artikel 4 Ziffer 12 der Verordnung (EU) 2016/679.

Massgebend ist alleine, ob die fraglichen Vorgänge geschehen. Irrelevant für das Vorliegen einer Verletzung der Datensicherheit ist ebenfalls, ob lediglich die Möglichkeit bestand, dass die Personendaten Unbefugten offengelegt oder zugänglich gemacht wurden, oder ob ein solcher Zugang tatsächlich stattgefunden hat. Geht beispielsweise ein Datenträger verloren, lässt sich oft kaum nachweisen, ob die darauf gespeicherten Daten tatsächlich durch Unbefugte eingesehen oder verwendet

wurden. Daher stellt bereits der Verlust als solches eine Verletzung der Datensicherheit dar. Der Umfang und die Bedeutung einer Verletzung der Datensicherheit sind vielmehr relevant für die zu treffenden Massnahmen, insbesondere die Einschätzung des Risikos nach Artikel 22 Absatz 1.

Bst. i Verantwortlicher

Der E-DSG sieht vor, den Begriff «Inhaber der Datensammlung» durch «Verantwortlicher» zu ersetzen, damit die gleiche Terminologie wie im E-SEV 108 (Art. 2 Bst. d), in der Richtlinie (EU) 2016/680 (Art. 3 Ziff. 8) und in der Verordnung (EU) 2016/679 (Art. 4 Ziff. 7) verwendet wird. Abgesehen davon, dass der Verweis auf die Datensammlung aufgehoben wird, ergibt sich hier keine materielle Änderung. Der Verantwortliche ist wie der Inhaber der Datensammlung derjenige, der über den Zweck und die Mittel (materielle oder automatisierte Bearbeitung, verwendete Software) der Bearbeitung entscheidet.[111]

Im deutschen Gesetzestext wird ausschliesslich die männliche Form verwendet, da es sich bei den Verantwortlichen überwiegend, aber nicht ausschliesslich um juristische Personen handelt.

Bst. j Auftragsbearbeiter

Dabei handelt es sich um die private Person oder das Bundesorgan, die oder das im Auftrag des Verantwortlichen Daten bearbeitet. Dieser Begriff entspricht jenem im E-SEV 108 (Art. 2 Bst. f), in der Richtlinie (EU) 2016/680 (Art. 3 Ziff. 9) und in der Verordnung (EU) 2016/679 (Art. 4 Ziff. 8).

Der Vertrag zwischen dem Verantwortlichen und dem Auftragsbearbeiter kann unterschiedlicher Art sein. Je nach den Verpflichtungen des Auftragsbearbeiters kann es sich um einen Auftrag (Art. 394 ff. OR), um einen Werkvertrag (Art. 363 ff. OR) oder um einen gemischten Vertrag handeln. Der Auftragsbearbeiter ist ab dem Zeitpunkt, an dem er seine vertragliche Tätigkeit im Auftrag des Verantwortlichen beginnt, kein Dritter mehr.

Im deutschen Gesetzestext wird ausschliesslich die männliche Form verwendet, da es sich bei den Auftragsbearbeitern überwiegend, aber nicht ausschliesslich um juristische Personen handelt.

Unveränderte Begriffe

Die folgenden Begriffe bleiben im Vergleich zum geltenden Recht unverändert bzw. erfahren lediglich redaktionelle Änderungen: Bekanntgeben (Bst. e) und Bundesorgan (Bst. h).

Aufgehobene Begriffe

Neben den Begriffen des Persönlichkeitsprofils und des Inhabers der Datensammlung hebt die Vorlage folgende Begriffe auf:

– Datensammlung: Der E-DSG sieht vor, auf diesen Begriff zu verzichten. Dies entspricht der Lösung im E-SEV 108, in dem stattdessen der Begriff

[111] BBl **1988** II 448

Bearbeiten von Daten verwendet wird. Dank den neuen Technologien können Daten heute wie eine Datensammlung genutzt werden, auch wenn sie nicht zentral gespeichert sind. Ein anschauliches Beispiel ist das Profiling, bei dem auf verschiedene Quellen zugegriffen wird, die keine Datensammlungen darstellen, um anhand der erhobenen Daten bestimmte Merkmale einer Person zu beurteilen. Nach dem derzeitigen Recht fallen solche Aktivitäten nicht unter die Gesetzesbestimmungen, die das Bestehen einer Datensammlung voraussetzen – wie beispielsweise das Auskunftsrecht (Art. 8 DSG) oder die Informationspflicht (Art. 14 DSG) –, während gerade in diesem Zusammenhang mehr Transparenz erforderlich ist. Im Übrigen weist der Bundesrat darauf hin, dass ein Teil der Lehre den Begriff Datensammlung sehr weit auslegt. Dabei besteht das entscheidende Kriterium darin, dass die Zuweisung von Daten zu einer Person keinen unverhältnismässigen Aufwand verursachen darf.[112]

– Gesetz im formellen Sinn: Der E-DSG sieht vor, auf diese Begriffsdefinition zu verzichten, da sie nicht nötig ist.

Art. 5 Grundsätze

Abs. 2 Rechtmässigkeit und Verhältnismässigkeit

Die französische Version von Absatz 2 erfährt eine redaktionelle Änderung.

Gemäss dem Grundsatz der Verhältnismässigkeit dürfen nur Daten bearbeitet werden, die für den Zweck der Bearbeitung geeignet und nötig sind. Zudem muss ein angemessenes Verhältnis zwischen dem Zweck und dem verwendeten Mittel bestehen, und die Rechte der betroffenen Personen sind soweit wie möglich zu wahren (Grundsatz der Verhältnismässigkeit im engeren Sinn).[113] Die Grundsätze der Datenvermeidung und der Datensparsamkeit sind beide Ausdruck davon.[114] Der erste impliziert, dass diese Option zu bevorzugen ist, wenn der Zweck der Bearbeitung erreicht werden kann, ohne dass neue Daten beschafft werden. Der zweite verlangt, dass nur Daten bearbeitet werden, die für den verfolgten Zweck absolut notwendig sind. Diese beiden Grundsätze sind bereits bei der Planung neuer Systeme zu beachten. Somit überschneiden sie sich teilweise mit den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen (siehe Erläuterungen zu Art. 6 E-DSG).

Abs. 3 Zweckbindung und Erkennbarkeit

Absatz 3 vereinigt die Grundsätze der Zweckbindung und der Erkennbarkeit, die gegenwärtig in den Absätzen 3 und 4 des Gesetzes enthalten sind. Damit das Bundesrecht besser mit dem Wortlaut des E-SEV 108 übereinstimmt (Art. 5 Abs. 4 Bst. b), ist im E-DSG vorgesehen, dass Daten nur zu einem bestimmten und für die

112 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, N 563; Belser Urs, in: Maurer-Lambrou/Vogt (Hrsg.), Basler Kommentar, Datenschutzgesetz, 2. Aufl., Basel 2006, Art. 3 DSG N 32; VPB 62.57.

113 BBl **1988** 450

114 Baeriswyl Bruno, Erläuterung zu Art. 4, in: Baeriswyl/Pärli (Hrsg.), Datenschutz – Stämpfli Handkommentar, Bern 2015, N 23.

betroffene Person erkennbaren Zweck beschafft werden dürfen. Diese neue Formulierung hat im Vergleich zum geltenden Recht keine materiellen Änderungen zur Folge. Sowohl die Beschaffung der Daten als auch der Zweck ihrer Bearbeitung müssen erkennbar sein. Dies ist grundsätzlich der Fall, wenn die betroffene Person informiert wird, die Bearbeitung gesetzlich vorgesehen oder aus den Umständen klar ersichtlich ist. Die Bestimmtheit des Zwecks bedingt, dass vage, nicht definierte oder unpräzise Bearbeitungszwecke nicht gnügen. Diese Eigenschaft wird nach den Umständen beurteilt, wobei ein Ausgleich zwischen den Interessen der betroffenen Personen und denen des Verantwortlichen bzw. des Auftragsbearbeiters und der Gesellschaft erfolgen muss.

Absatz 3 hält fest, dass Daten nur in einer Weise bearbeitet werden dürfen, die mit dem anfänglichen Zweck zu vereinbaren ist. Diese neue Formulierung ermöglicht eine terminologische Annäherung des Gesetzes an den E-SEV 108 (Art. 5 Abs. 4 Bst. b). Sie bringt jedoch keine wesentlichen Änderungen mit sich: Wie bereits heute ist eine Weiterbearbeitung nicht zulässig, wenn die betroffene Person dies berechtigterweise als unerwartet, unangebracht oder beanstandbar erachten kann (siehe auch Ziffer 47 des erläuternden Berichts zum E-SEV 108 vom CAHDATA[115]). Dabei sind etwa folgende Fälle denkbar:

- die Weiterverwendung von Adressen zu Werbezwecken, die beim Unterschriftensammeln für eine politische Kampagne erfasst wurden;
- die Beschaffung und Analyse von Daten über Konsumgewohnheiten (zu anderen Zwecken als zur Betrugsbekämpfung) gestützt auf Zahlungen, die mit einer Kredit- oder Kundenkarte getätigt wurden, ohne Einwilligung der betroffenen Person;
- das Sammeln und Benutzen von E-Mail-Adressen, welche die betroffene Person zu einem bestimmten Zweck über das Internet bekannt gegeben hat, um später Spamnachrichten zu versenden;[116]
- die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch ein Privatunternehmen.[117]

Übermittelt die betroffene Person ihre Adresse dagegen im Hinblick auf den Erhalt einer Kundenkarte oder für eine Bestellung (online oder nicht), so liegt die Weiterbenutzung dieser Adresse durch das betreffende Unternehmen zu Werbezwecken im Rahmen einer anfänglich erkennbaren Zweckbestimmung und kann mithin als mit dem anfänglichen Zweck vereinbar angesehen werden.[118] Ist die Änderung des anfänglichen Zwecks gesetzlich vorgesehen, wird sie durch eine Gesetzesänderung verlangt oder ist sie durch einen anderen Rechtfertigungsgrund legitimiert (z. B. durch die Einwilligung der betroffenen Person), so gilt die Weiterbearbeitung ebenfalls als mit dem anfänglichen Zweck vereinbar.

115 rm.coe.int/16806af190.
116 VPB 69.106 E. 5.6.
117 BGE **136** II 508 E. 4.
118 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, N 731.

Abs. 4 Dauer der Aufbewahrung der Personendaten

Gemäss Absatz 4 müssen Daten vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. Dies entspricht den Anforderungen des E-SEV 108 (Art. 5 Abs. 4 Bst. e, vgl. ebenfalls Ziffer 51 des Entwurfs des erläuternden Berichts zum E-SEV 108 vom CAHDATA), der Richtlinie (EU) 2016/680 (Art. 4 Abs. 1 Bst. e) und der Verordnung (EU) 2016/679 (Art. 5 Abs. 1 Bst. e). Die Verpflichtung ergibt sich implizit auch aus dem allgemeinen Verhältnismässigkeitsgrundsatz, der in Absatz 2 der Bestimmung festgehalten ist. Der Bundesrat hält es indes für wichtig, diese Verpflichtung im Hinblick auf die technologische Entwicklung und die beinahe unbegrenzten Speichermöglichkeiten noch ausdrücklich festzuhalten. Die Einhaltung dieser Verpflichtung bedingt, dass der Verantwortliche Aufbewahrungsfristen festlegt. Vorbehalten bleiben spezielle Regelungen, die besondere Aufbewahrungsfristen vorsehen.

Abs. 5 Richtigkeit

Artikel 5 Absatz 5 E-DSG übernimmt den Grundsatz der Richtigkeit der Daten, der gegenwärtig in Artikel 5 DSG enthalten ist. Auf diese Weise werden die wichtigsten Datenschutzgrundsätze in einer einzigen Bestimmung zusammengefasst, wie dies auch in Artikel 5 E-SEV 108, in Artikel 4 der Richtlinie (EU) 2016/680 und in Artikel 5 der Verordnung (EU) 2016/679 der Fall ist. Im französischen Text wird der Begriff «correctes» durch «exactes» ersetzt; auf Deutsch und Italienisch stimmt die verwendete Terminologie bereits jetzt überein.

Der Absatz hält fest, dass jede Person, die Daten bearbeitet, sich über deren Richtigkeit zu vergewissern hat. Sie hat alle angemessenen Massnahmen zu treffen, damit die Daten, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind, berichtigt, gelöscht oder vernichtet werden. Daten, die nicht korrigiert oder ergänzt werden können, sind zu löschen oder zu vernichten. Der Umfang dieser Vergewisserungspflicht ist im Einzelfall zu bestimmen. Er hängt insbesondere vom Zweck und Umfang der Bearbeitung sowie von der Art der bearbeiteten Daten ab. Je nach Fall kann diese Pflicht bedeuten, dass die Daten aktuell gehalten werden.

Bestimmte gesetzliche Pflichten können der Berichtigung, der Löschung oder der Aktualisierung der Daten entgegenstehen.[119] Zudem sind der Grundsatz der Richtigkeit und die damit verbundenen Pflichten in Bezug auf die Tätigkeit von Archiven, Museen, Bibliotheken und anderen Gedächtnisinstitutionen differenziert zu betrachten. Die Aufgabe solcher Institutionen ist es namentlich, Dokumente (auch digitale) aller Art zu sammeln, zu erschliessen, zu erhalten und zu vermitteln (vgl. Art. 2 Abs. 1 des Nationalbibliotheksgesetzes vom 18. Dezember 1992[120]). Die fraglichen Dokumente als solche dürfen dabei nicht verändert werden, weil dies dem Zweck der Archivierung zuwiderlaufen würde. Denn Archive sollen mit Hilfe von Dokumenten eine Momentaufnahme der Vergangenheit erlauben, deren «Richtigkeit» sich allein darauf bezieht, dass die fraglichen Dokumente originalgetreu wiederge-

119 Pflicht, die Daten unversehrt zu halten, beispielsweise Art. 7 des Geldwäschereigesetzes vom 10. Oktober 1997 (GwG; SR **955.0**).
120 SR **432.21**

geben werden. Archive geben mit anderen Worten wieder, wie etwas in der Vergangenheit war, unabhängig davon, ob dies aus aktueller Perspektive noch als zutreffend erachtet wird. An dieser spezifischen Tätigkeit besteht ein erhebliches öffentliches Interesse (diesbezüglich siehe Art. 28 Abs. 1 Bst. b und 37 Abs. 5 E-DSG sowie die entsprechenden Erläuterungen unter Ziff. 9.1.6 und 9.1.7).

Abs. 6 Einwilligung

Sofern eine Einwilligung der betroffenen Person erforderlich ist, ist eine solche gemäss Absatz 6 nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig und eindeutig erfolgt. Die betroffene Person drückt damit ihre Zustimmung zu einer Verletzung der Persönlichkeit aus, die vorliegend durch eine Datenbearbeitung erfolgt.

Die etwas geänderte Formulierung ermöglicht eine terminologische Annäherung an den E-SEV 108 (Art. 5 Abs. 2), um dessen Anforderungen gerecht zu werden. Daraus folgt indessen keine grundsätzliche Änderung der aktuellen Rechtslage. Wie bereits nach dem bestehenden Recht muss für eine gültige Einwilligung die Bearbeitung, insbesondere deren Umfang und Zweck, hinreichend bestimmt sein. Dabei kann auch in mehrere gleichgelagerte oder verschiedene Bearbeitungen eingewilligt werden. Ebenso ist möglich, dass der Bearbeitungszweck verschiedene Bearbeitungen erfordert. So kann beispielsweise die Heilbehandlung bei einer Ärztin oder einem Arzt den Austausch mit vor- oder nachbehandelnden Fachpersonen und Diensten erfordern, ebenso die Bearbeitung zu Abrechnungszwecken oder Abklärungen mit Versicherungen. Die Einwilligung muss den Zweck der Bearbeitung abdecken, für den sie als Rechtfertigungsgrund dient. Werden die Daten noch zu weiteren Zwecken bearbeitet, in die nicht eingewilligt wurde, muss diese Bearbeitung durch andere Gründe gerechtfertigt sein. Die Einwilligung muss darüber hinaus eindeutig sein. Demnach muss aus der Erklärung der betroffenen Person deren Wille zweifelsfrei hervorgehen. Dies hängt von den konkreten Umständen des Einzelfalls ab. Gemäss dem Verhältnismässigkeitsgrundsatz muss die Zustimmung umso eindeutiger sein, je sensibler die fraglichen Personendaten sind.[121] Die Einwilligung kann nach wie vor formfrei erfolgen und ist damit insbesondere nicht an eine schriftliche Erklärung gebunden.[122] Eine eindeutige Einwilligung im Sinne von Absatz 6 kann auch durch eine stillschweigende Willenserklärung erfolgen (vgl. Art. 1 OR). Eine solche liegt vor, wenn sich die Willensäusserung nicht aus der Erklärung selbst ergibt, sondern durch ein Verhalten, das aufgrund der Umstände, in denen es erfolgt, als eindeutiger Ausdruck des Willens verstanden werden kann.[123] Dies ist der Fall bei sogenanntem konkludentem (schlüssigem) Verhalten, bei dem die erklärende Person ihren Willen äussert, indem sie ihn durch eine entsprechende Handlung deutlich macht, z. B. indem sie ihre vertragliche Pflicht erfüllt. Es muss mithin eine Willensäusserung erfolgen, sodass grundsätzlich blosses Schweigen oder Untätigkeit

121 BBl **2003** 2127
122 Vgl. bereits BBl **2003** 2127
123 Kren Kostkiewicz Jolanta, Art. 1 OR N 17, in: Kren Kostkiewicz Jolanta et al. (Hrsg.), OR, Schweizerisches Obligationenrecht, Kommentar, 3. Aufl., Zürich 2016 und die Hinweise dort.

nicht als gültige Einwilligung in eine Persönlichkeitsverletzung gelten kann.[124] Vorbehalten bleibt Artikel 6 OR, wenn die Parteien Schweigen als Zustimmung vereinbart haben.

Gemäss dem zweiten Satz von Absatz 6 muss die Einwilligung ausdrücklich erfolgen, wenn es um die Bearbeitung besonders schützenswerter Personendaten und das Profiling geht. An die Einwilligung für das Profiling werden ebenfalls erhöhte Anforderungen gestellt, wie dies bereits im geltenden Recht für die Bearbeitung von Persönlichkeitsprofilen der Fall ist. «Ausdrücklich» ist eine erhöhte Anforderung an die «eindeutige» Einwilligung gemäss Satz 1 dieser Bestimmung. Die Tragweite dieser Anforderung ist bereits im aktuellen Recht teilweise umstritten.[125] Der Bundesrat sieht indes keinen Anlass, von der aktuellen Rechtslage abzuweichen. Zur Klärung der Begrifflichkeiten werden allerdings in der französischen und italienischen Version des Textes die Begriffe «explicite» und «esplicito» durch die Begriffe «exprès» und «espresso» ersetzt und damit an die Terminologie von Artikel 1 OR angepasst. Der deutsche Text erfährt keine Änderung. Eine Willenserklärung ist «ausdrücklich», wenn sie durch geschriebene oder gesprochene Worte oder ein Zeichen erfolgt und der geäusserte Willen aus den verwendeten Worten oder dem Zeichen unmittelbar hervorgeht.[126] Die Willensäusserung als solche muss durch die Art und Weise, in der sie erfolgt, bereits Klarheit über den Willen schaffen.[127] Dies ist insbesondere möglich durch das Ankreuzen eines Kästchens, die aktive Auswahl bestimmter technischer Parameter für die Dienste eines Informationsverarbeitungsunternehmens oder anderweitige Erklärungen. Dasselbe gilt für die nonverbale Äusserung mittels eines im konkreten Kontext klaren Zeichens oder einer entsprechenden Bewegung, was namentlich im Rahmen eines ärztlichen Behandlungsverhältnisses häufig der Fall sein kann. Beispiele hierfür sind das zustimmende Kopfnicken oder das Öffnen des Mundes zur Entnahme von Wangenschleimhaut im Anschluss an die klare Aufklärung. Wo eine ausdrückliche Einwilligung erforderlich ist, kann diese nicht stillschweigend gegeben werden.

Art. 6 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Artikel 6 E-DSG führt die Pflicht zum Datenschutz durch Technik sowie durch datenschutzfreundliche Voreinstellungen ein. Weil diese Pflichten eng mit den Datenschutzgrundsätzen zusammenhängen, wurden sie in die allgemeinen Datenschutzbestimmungen überführt. Die Norm setzt die Anforderungen von Artikel 8bis

124 Haas Raphaël, Die Einwilligung in eine Persönlichkeitsverletzung nach Art. 28 Abs. 2 ZGB, Diss. Luzern, Zürich 2007, N 393 mit zahlreichen Hinweisen.

125 Vgl. Vasella David, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter 16. November 2015.

126 BGE **121** III 31, E. 2c S. 34; Kren Kostkiewicz Jolanta, Art. 1 OR N 17, in: Kren Kostkiewicz Jolanta et al. (Hrsg.), OR, Schweizerisches Obligationenrecht, Kommentar, 3. Aufl., Zürich 2016; Gauch Peter/Schluep Walter/Schmid Jörg/Emmenegger Susan, Schweizerisches Obligationenrecht Allgemeiner Teil, Band 1, 10. Aufl., Zürich 2014 N 188.

127 Vasella David, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, Jusletter 16. November 2015, N 26 f.

Ziffer 3 E-SEV 108 sowie von Artikel 20 Absatz 1 der Richtlinie (EU) 2016/680 um. Der Artikel 25 der Verordnung (EU) 2016/679 enthält eine ähnliche Regelung.

Abs. 1 Datenschutz durch Technik

Absatz 1 verlangt vom Verantwortlichen, ab dem Zeitpunkt der Planung eine Datenbearbeitung so auszugestalten, dass durch die getroffenen Vorkehren die Datenschutzvorschriften umgesetzt werden. Damit wird neu die Pflicht zum sogenannten «Datenschutz durch Technik» (Privacy by Design) eingeführt. Die Grundidee des technikgestützten Datenschutzes besteht darin, dass sich Technik und Recht gegenseitig ergänzen. So kann datenschutzfreundliche Technik den Bedarf nach rechtlichen Regeln (oder Verhaltenskodizes) reduzieren, indem technische Vorkehren den Verstoss gegen Datenschutzvorschriften verunmöglichen oder zumindest die Gefahr erheblich verringern. Zugleich sind datenschutzfreundliche Technologien unabdingbar für die praktische Umsetzung der Datenschutzvorschriften. Denn Datenbearbeitung ist in vieler Hinsicht bereits allgegenwärtig und wird tendenziell weiter zunehmen (Ubiquitous Computing). Dies sorgt für kaum überblickbare Datenmengen, die im Einklang mit den Datenschutzregeln bearbeitet werden müssen, wofür technische Vorkehren zentral sind. Insgesamt zielt der technikgestützte Datenschutz nicht auf eine bestimmte Technologie. Vielmehr geht es darum, Systeme zur Datenbearbeitung technisch und organisatorisch so auszugestalten, dass sie insbesondere den Grundsätzen nach Artikel 5 E-DSG entsprechen. Die gesetzlichen Anforderungen für eine datenschutzkonforme Bearbeitung werden mit anderen Worten bereits so im System verwirklicht, dass dieses die Gefahr von Verstössen gegen Datenschutzvorschriften reduziert oder ausschliesst. So kann beispielsweise dafür gesorgt werden, dass Daten in regelmässigen Abständen gelöscht oder standardmässig anonymisiert werden. Besonders bedeutsam für den technikgestützten Datenschutz ist dabei die sogenannte Datenminimierung, welche sich bereits aus den allgemeinen Grundsätzen nach Artikel 5 E-DSG ergibt. Entsprechend dem Konzept der Datenminimierung wird eine Datenbearbeitung bereits von Beginn weg so angelegt, dass möglichst wenige Daten anfallen und bearbeitet werden oder dass Daten zumindest nur möglichst kurze Zeit aufbewahrt werden.

Die Bundesorgane müssen schon heute den von ihnen bezeichneten Datenschutzverantwortlichen oder, falls kein solcher besteht, dem Beauftragten unverzüglich alle Projekte zur automatisierten Bearbeitung von Personendaten melden, damit die Erfordernisse des Datenschutzes bereits bei der Planung berücksichtigt werden (Art. 20 VDSG).

Abs. 2 Angemessenheit der Vorkehren

Absatz 2 präzisiert die Anforderungen an die Vorkehren nach Absatz 1. Diese müssen insbesondere nach dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken, welche die fragliche Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Person mit sich bringt, angemessen sein. Die vorliegende Bestimmung bezieht sich auf Datenbearbeitungen durch private Bearbeiter und Bundesorgane, sodass von Risiken für die Persönlichkeit und die Grundrechte die Rede ist.

Die Norm bringt den risikobasierten Ansatz zum Ausdruck. Das Risiko, das mit einer Bearbeitung einhergeht, muss in Beziehung gesetzt werden zu den technischen Möglichkeiten, um dieses zu verringern. Je höher das Risiko, je grösser die Eintrittswahrscheinlichkeit und je umfangreicher die Datenbearbeitung ist, umso höher sind die Anforderungen an die technischen Vorkehren, damit sie im Sinne der vorliegenden Bestimmung als angemessen gelten können.

Abs. 3 Datenschutzfreundliche Voreinstellungen

Gemäss Absatz 3 ist der Verantwortliche verpflichtet, mittels geeigneter Voreinstellungen dafür zu sorgen, dass grundsätzlich nur so wenige Personendaten bearbeitet werden, wie im Hinblick auf den Verwendungszweck möglich ist, soweit die betroffene Person nicht etwas anderes bestimmt. Dies führt neu die Pflicht zur Verwendung datenschutzfreundlicher Voreinstellungen (Privacy by Default) ein. Bei Voreinstellungen handelt es sich um jene Einstellungen, insbesondere von Software, die standardmässig zur Anwendung kommen, d.h. falls keine abweichende Eingabe durch den Nutzer erfolgt. Diese Standardeinstellungen können werkseitig vorliegen oder entsprechend programmiert werden, wie dies zum Beispiel der Fall ist, wenn ein bestimmter Drucker als Standarddrucker definiert wird. Im Zusammenhang mit einer Datenbearbeitung bedeutet dies, dass der fragliche Bearbeitungsvorgang standardmässig möglichst datenschutzfreundlich eingerichtet ist, ausser die betroffene Person würde diese vorgegebenen Einstellungen verändern. Beispielsweise wäre es denkbar, dass eine Website grundsätzlich Einkäufe erlaubt, ohne dass dafür ein Benutzerprofil erstellt werden muss. Die Kunden müssen lediglich minimale Angaben wie Namen und Adresse machen. Falls die Kunden aber von weiteren Diensten dieser Website profitieren möchten, zum Beispiel vom Zugriff auf ihre gesamten Einkäufe in der Vergangenheit oder dem Anlegen von Listen mit Einkaufswünschen, müssen sie ein Benutzerprofil anlegen, wodurch auch eine umfassendere Bearbeitung ihrer Personendaten erfolgt. Dies macht den engen Zusammenhang mit der Verwendung datenschutzfreundlicher Technik und dem Grundsatz der Datenminimierung deutlich. So gehören entsprechende Voreinstellungen regelmässig zur datenschutzfreundlichen Ausgestaltung eines gesamten Systems. Spezifisch an datenschutzfreundlichen Voreinstellungen sind jedoch die Einflussmöglichkeiten der betroffenen Person. Während diese das System als solches kaum beeinflussen kann, geben ihr datenschutzfreundliche Voreinstellungen allenfalls die Möglichkeit, eine andere Wahl zu treffen. Sie hängen daher eng mit der Einwilligung der betroffenen Person zusammen (vgl. Art. 5 Abs. 6 E-DSG). So erlauben es datenschutzfreundliche Voreinstellungen der betroffenen Person, einer bestimmten Datenbearbeitung zuzustimmen.

Der Grundsatz des Datenschutzes mittels Voreinstellungen spielt im öffentlichen Sektor eine untergeordnete Rolle, da die Datenbearbeitung dort weniger auf der Einwilligung der betroffenen Person beruht als auf gesetzlichen Pflichten.

Der Verantwortliche kann insbesondere durch die Zertifizierung oder eine Datenschutz-Folgenabschätzung aufzeigen, dass er den Verpflichtungen dieser Bestimmung nachkommt.

Art. 7 Datensicherheit

Artikel 7 E-DSG übernimmt Artikel 7 DSG mit einigen Änderungen. Die Pflicht, die Datensicherheit sicherzustellen, ist eine Anforderung des E-SEV 108 (Art. 7) und der Richtlinie (EU) 2016/680 (Art. 29). Die Verordnung (EU) 2016/679 (Art. 32) enthält eine ähnliche Regelung. Der Verantwortliche und der Auftragsbearbeiter müssen durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten. Darin kommt der risikobasierte Ansatz zum Ausdruck. Je grösser das Risiko einer Verletzung der Datensicherheit, umso höher sind die Anforderungen an die zu treffenden Massnahmen.

Absatz 2 bestimmt das Ziel dieser Massnahmen. Diese sollen es erlauben, Verletzungen der Datensicherheit zu vermeiden, d.h. jede Verletzung der Sicherheit, die ungeachtet der Absicht oder der Widerrechtlichkeit dazu führt, dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (Art. 4 Bst. g E-DSG). Solche Vorkehren können beispielsweise sein: die Pseudonymisierung von Personendaten, Massnahmen zur Wahrung der Vertraulichkeit und Verfügbarkeit des Systems oder dessen Dienste, die Entwicklung von Verfahren, mit denen regelmässig geprüft, analysiert und bewertet werden kann, ob die getroffenen Sicherheitsvorkehren wirksam sind.

Datenschutz und Datensicherheit stehen zwar in einer Wechselwirkung, sind aber voneinander abzugrenzen. Beim Datenschutz geht es um den Persönlichkeitsschutz des Einzelnen. Die Datensicherheit zielt hingegen generell auf die bei einem Verantwortlichen oder Auftragsbearbeiter vorhandenen Daten ab und umfasst den allgemeinen technischen und organisatorischen Rahmen der Datenbearbeitung. Demnach ist individueller Datenschutz nur möglich, wenn zugleich allgemeine technische Vorkehrungen zur Datensicherheit getroffen werden. Daraus ergibt sich auch die Abgrenzung der Pflicht zur Datensicherheit nach Artikel 7 E-DSG zum Datenschutz durch Technik nach Artikel 6 Absatz 1 E-DSG. Artikel 7 verpflichtet sowohl den Verantwortlichen als auch den Auftragsbearbeiter dazu, für ihre Systeme eine geeignete Sicherheitsarchitektur vorzusehen und sie z. B. gegen Schadsoftware oder Datenverlust zu schützen. Artikel 6 Absatz 1 zielt hingegen darauf ab, mit technischen Mitteln die Einhaltung von Datenschutzvorschriften sicherzustellen, z. B. dass die Datenbearbeitung verhältnismässig bleibt. Dabei können einzelne Massnahmen wie beispielsweise die Anonymisierung von Daten für beide Pflichten bedeutsam sein.

Absatz 3 verpflichtet den Bundesrat, Mindestanforderungen an die Datensicherheit zu definieren.

Art. 8 Bearbeitung durch Auftragsbearbeiter

Artikel 8 übernimmt im Wesentlichen den geltenden Artikel 10*a* DSG (Datenbearbeitung durch Dritte). In den Absätzen 1, 2 und 4 erfolgen terminologische Änderungen, die infolge der neuen Begriffe (Auftragsbearbeiter, Verantwortlicher) erforderlich sind. Wie nach bisherigen Recht lässt sich insbesondere festhalten, dass die Auftragsbearbeitung für Personendaten, die durch Artikel 321 StGB geschützt sind (z. B. Daten, die unter das Artzgeheimnis fallen), durch die Vorschrift in Artikel 8 Absatz 1 Buchstabe b E-DSG nicht ausgeschlossen ist, wenn die Dritten als Hilfs-

personen im Sinne von Artikel 321 Ziff. 1 Abs. 1 StGB zu qualifizieren sind.[128] Sind die übrigen Voraussetzungen der Auftragsbearbeitung erfüllt, so ist diese damit zulässig, ohne dass die betroffene Person zusätzlich ihre Einwilligung dazu geben müsste.[129]

Absatz 1 begründet eine Sorgfaltspflicht für den Verantwortlichen, bei der Auftragsbearbeitung die Rechte der betroffenen Person zu wahren. Der Verantwortliche muss aktiv sicherstellen, dass der Auftragsbearbeiter das Gesetz im selben Umfang einhält, wie er selbst es tut. Das betrifft insbesondere die Einhaltung der allgemeinen Grundsätze, der Regeln betreffend die Datensicherheit, die in Absatz 2 ausdrücklich erwähnt werden, sowie der Regeln betreffend die Bekanntgabe ins Ausland. Der Verantwortliche muss analog wie bei Artikel 55 OR Verstösse gegen das DSG verhindern. Er ist daher verpflichtet, seinen Auftragsbearbeiter sorgfältig auszuwählen, ihn angemessen zu instruieren und soweit als nötig zu überwachen.[130]

Absatz 3 ist neu und sieht vor, dass der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen darf. Im Privatsektor ist die Genehmigung an keine besondere Form gebunden. Der Auftragsbearbeiter muss jedoch nachweisen, dass die Genehmigung vorliegt. Es liegt somit in seinem Interesse, dies zu dokumentieren. Im öffentlichen Sektor hat die Genehmigung hingegen schriftlich zu erfolgen. Es handelt sich um eine Anforderung der Richtlinie (EU) 2016/680 (Art. 22 Abs. 2). Der Bundesrat wird dies in einer Verordnung festlegen. Sowohl im privaten als auch im öffentlichen Sektor kann die Genehmigung spezifischer oder allgemeiner Art sein. In letzterem Fall informiert der Auftragsbearbeiter den Verantwortlichen über jede Änderung (Hinzuziehung oder Ersetzung anderer Auftragsbearbeiter), damit er Einspruch gegen diese Änderungen erheben kann.

Die Datenbearbeitung innerhalb der gleichen juristischen Person (Filiale, Verwaltungseinheit, Mitarbeitende) stellt grundsätzlich keine Bearbeitung durch Auftragsbearbeiter dar.[131]

Werden Daten in einer sogenannten Cloud aufbewahrt, handelt es sich dabei grundsätzlich um einen Anwendungsfall der Auftragsbearbeitung, welche die entsprechenden Voraussetzungen erfüllen muss. Falls hierfür Daten ins Ausland bekanntgegeben werden, müssen zudem die Voraussetzungen der Artikel 13 und 14 vorliegen.

Art. 9 Datenschutzberaterin oder -berater

Artikel 9 regelt die interne Datenschutzberaterin oder den internen Datenschutzberater. Das bisherige Recht verwendet auf Deutsch den Begriff des Datenschutzverantwortlichen, auf Italienisch responsabile, während auf Französisch vom conseiller die

128 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, Nr. 1227 mit weiteren Hinweisen.

129 Eine andere Ansicht vertreten einzelne Lehrmeinungen, vgl. Wohlers Wolfgang, Outsourcing durch Berufsgeheimnisträger, Patienten- und Mandantengeheimnisse als Schranke bei der Auslagerung von Datenverarbeitungen, digma 2016, S. 114 ff.

130 BBl **1988** 413 463

131 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, Nr. 1201. In Bezug auf Mitarbeitende siehe auch die Ziffer 23 des Entwurfs des erläuternden Berichts zum E-SEV 108 vom CAHDATA.

Rede ist (Art. 11*a* Abs. 5 Bst. e DSG). Um Verwechslungen mit dem Verantwortlichen nach Artikel 4 Buchstabe i E-DSG bzw. mit dem responsabile nach Artikel 4 Buchstabe j E-DSG zu vermeiden, führt der E-DSG auf Deutsch und Italienisch den Begriff der Datenschutzberaterin und des Datenschutzberaters bzw. des consulente per la protezione dei dati ein. Dadurch ist die Terminologie in allen drei Sprachen einheitlich.

Die Datenschutzberaterin oder der Datenschutzberater überwacht die Einhaltung der Datenschutzvorschriften innerhalb eines Unternehmens und berät den Verantwortlichen in Datenschutzbelangen. Der Verantwortliche trägt jedoch allein die Verantwortung dafür, dass die Personendaten datenschutzkonform bearbeitet werden.

Die Bestimmung wird aufgrund der Vernehmlassung in den E-DSG eingefügt. Sie hat ergeben, dass eine ausdrückliche Erwähnung der Datenschutzberaterin oder des Datenschutzberaters im Gesetz erwünscht ist. Der E-DSG geht indes weniger weit als das europäische Recht, das in gewissen Fällen eine Pflicht zur Ernennung einer Datenschutzberaterin oder eines Datenschutzberaters vorsieht. Diese Lösung hätte auch der Beauftragte bevorzugt. Nach dem E-DSG bleibt es hingegen den Unternehmen überlassen, ob sie eine Datenschutzberaterin oder einen Datenschutzberater ernennen wollen, während Bundesorgane grundsätzlich verpflichtet sind, einen solchen einzusetzen.

Abs. 1 und 2 Ernennung

Private Verantwortliche können grundsätzlich jederzeit eine Datenschutzberaterin oder einen Datenschutzberater ernennen, wie dies in Absatz 1 festgehalten ist. Das Gesetz sieht jedoch in Bezug auf die Datenschutz-Folgenabschätzung Erleichterungen vor für Verantwortliche, die eine solche Beraterin oder einen solchen Berater ernannt haben.

Absatz 2 definiert die Voraussetzungen, die erfüllt sein müssen, damit diese Erleichterungen zur Anwendung kommen können (Bst. a). Dabei übernimmt der E-DSG weitgehend geltendes Recht (vgl. Art. 12*a* f. VDSG).

Der Verantwortliche kann eine Mitarbeiterin oder einen Mitarbeiter oder eine Drittperson zur Datenschutzberaterin oder zum Datenschutzberater ernennen. Nach Buchstabe a muss die Person ihre Funktion jedoch fachlich unabhängig ausüben; sie oder er ist gegenüber dem Verantwortlichen nicht weisungsgebunden. Handelt es sich um eine Mitarbeiterin oder einen Mitarbeiter, muss die hierarchische Einordnung innerhalb des Unternehmens sicherstellen, dass die Datenschutzberaterin oder der Datenschutzberater unabhängig bleibt. Grundsätzlich sollte sie oder er direkt der Geschäftsleitung des Verantwortlichen unterstellt sein.

Buchstabe b konkretisiert die Unabhängigkeit der Datenschutzberaterin oder des Datenschutzberaters weiter. Demnach dürfen diese Personen keine Tätigkeiten übernehmen, die mit ihren Aufgaben unvereinbar sind. Dies könnte beispielsweise der Fall sein, wenn die Datenschutzberaterin oder der Datenschutzberater Mitglied der Geschäftsleitung ist, Funktionen in Bereichen der Personalführung oder der Informationssystemverwaltung ausübt oder zu einer Dienststelle gehört, die selbst besonders schützenswerte Personendaten bearbeitet. Hingegen ist es z. B. denkbar,

die Aufgabe der Datenschutzberaterin oder des Datenschutzberaters zu kumulieren mit derjenigen des Informationssicherheitsbeauftragten.

Nach Buchstabe c muss die Datenschutzberaterin oder der Datenschutzberater schliesslich über die erforderlichen Fachkenntnisse verfügen, um diese Aufgabe zu übernehmen. So ist für diese Tätigkeit Fachwissen sowohl im Bereich der Datenschutzgesetzgebung als auch über technische Standards zur Datensicherheit erforderlich.

Die Datenschutzberaterin oder der Datenschutzberater ist sowohl für die betroffene Person als auch für den Beauftragten ein wichtiger Ansprechpartner in Bezug auf die Datenbearbeitungen, welche das fragliche Unternehmen vornimmt. Nach Buchstabe d muss der Verantwortliche die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters daher veröffentlichen und dem Beauftragten mitteilen. Eine analoge Pflicht ist in der Verordnung auch für Bundesorgane vorzusehen.

Abs. 3 Datenschutzberaterin oder -berater von Bundesorganen

Absatz 3 verpflichtet den Bundesrat, Regeln zur Bestellung der Datenschutzberaterin oder des Datenschutzberaters durch die Bundesorgane zu erlassen. Diese befinden sich auch nach bisherigen Recht überwiegend in der Verordnung.

Die Bundesorgane sind im Schengen-Bereich aufgrund von Artikel 32 der Richtlinie (EU) 2016/680 dazu verpflichtet, eine Datenschutzberaterin oder einen Datenschutzberater zu ernennen.

Art. 10 Verhaltenskodizes

Der Bundesrat möchte die Erarbeitung von Verhaltenskodizes fördern. Diese entsprechen einem Bedürfnis, das die Regulierungsfolgenabschätzung (vgl. Ziff. 1.8) angesichts des allgemeinen Charakters der Gesetzgebung und ihres äusserst umfassenden persönlichen und sachlichen Geltungsbereichs ergeben hat. In solchen Kodizes können einzelne Begriffe wie das hohe Risiko (Art. 20 E-DSG) oder die Modalitäten von Pflichten wie der Informationspflicht (Art. 17–19 E-DSG) und der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 20 E-DSG) präzisiert werden. Ausserdem sollen präzisere Lösungen gefunden werden in Bereichen, die heute zahlreiche Fragen aufwerfen, beispielsweise bei der Videoüberwachung, dem Cloud Computing oder sozialen Netzwerken.[132]

132 Im Bereich des Internets und der Telekommunikation haben die interessierten Kreise Verhaltenskodizes erlassen, die, obwohl sie nicht speziell auf die Aspekte des Datenschutzes ausgerichtet sind, in bestimmten Fällen auch die Rechte der betroffenen Personen in diesem Bereich schützen. Es handelt sich zum einen um die neue Brancheninitiative des Schweizerischen Verbandes der Telekommunikation für verbesserten Jugendmedienschutz in den neuen Medien und zur Förderung der Medienkompetenz in der Gesellschaft, deren Unterzeichnende sich verpflichten, bestimmte Websites zu sperren und Massnahmen zur Verbesserung des Jugendmedienschutzes zu ergreifen. Zum andern handelt es sich um den Code of Conduct Hosting (CCH) der Swiss Internet Industry Association (Simsa) vom 1. Februar 2013, der einen Verhaltenskodex für Schweizer Hosting Provider darstellt.

Indem der Bundesrat den interessierten Kreisen ermöglicht, selbst aktiv zu werden und zur Regulierung der einzelnen Bereiche beizutragen, möchte er konzertierte und breit abgestützte Branchenlösungen fördern. Zur Förderung der Selbstregulierung schlägt er zudem vor, dass Verantwortliche, die Verhaltenskodizes einhalten, unter bestimmten Voraussetzungen auf die Durchführung einer Datenschutz-Folgenabschätzung verzichten können (Art. 20 Abs. 5 E-DSG).

Die Förderung der Einführung von Verhaltenskodizes durch die Staaten und die Aufsichtsbehörden ist auch in der Verordnung (EU) 2016/679 (Art. 40 und 57 Abs. 1 Bst. m) vorgesehen.

Im privaten Sektor müssen die Verhaltenskodizes von Berufs- oder Wirtschaftsverbänden stammen, die nach ihren Statuten zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt sind.[133] Einzelne Verantwortliche oder Auftragsbearbeiter können dem Beauftragten keine Verhaltenskodizes vorlegen, da die Verhaltenskodizes eine gewisse Vereinheitlichung innerhalb einer bestimmten Branche zum Ziel haben. Im öffentlichen Sektor können Verhaltenskodizes hingegen von einem einzelnen Bundesorgan stammen. Dies rechtfertigt sich insbesondere aufgrund der zahlreichen gesetzlichen Grundlagen und der Vielfalt der Aufgaben der verschiedenen Organe.

Absatz 1 sieht vor, dass die Verhaltenskodizes dem Beauftragten vorgelegt werden können. Dieser nimmt dazu Stellung (Abs. 2). Die Frist, innerhalb der er Stellung nehmen muss, hängt von den Umständen des Einzelfalls ab.

Die Stellungnahme stellt keine Verfügung dar. Die interessierten Kreise können somit aus einer positiven Stellungnahme bzw. einem Verzicht auf eine Stellungnahme keine Rechte ableiten. Dennoch kann bei einer positiven Stellungnahme des Beauftragten davon ausgegangen werden, dass ein dem Verhaltenskodex entsprechendes Verhalten keine Verwaltungsmassnahmen nach sich zieht. Der Beauftragte veröffentlicht seine Stellungnahme, und zwar unabhängig davon, ob er den vorgelegten Verhaltenskodex positiv oder negativ beurteilt.

Der Beauftragte hätte es vorgezogen, wenn die Verbände dazu verpflichtet worden wären, ihm die Kodizes zur Genehmigung vorzulegen. Der Bundesrat hat aufgrund der Vernehmlassungsergebnisse darauf verzichtet, aber auch weil der Beauftragte auf dem Wege einer Verfügung hätte darüber entscheiden müssen, was zusätzliche Kosten nach sich gezogen hätte.

Art. 11 Verzeichnis der Bearbeitungstätigkeiten

Der E-DSG sieht anstelle der Dokumentationspflicht im Vorentwurf die Pflicht vor, ein Verzeichnis der Bearbeitungstätigkeiten zu führen. Die Vernehmlassung hat ergeben, dass zu wenig deutlich wurde, was die Dokumentationspflicht umfasst. Zudem wird das Verzeichnis der Bearbeitungstätigkeiten neu bei den allgemeinen Datenschutzbestimmungen eingeordnet. Dies verdeutlicht den engen Zusammenhang mit den Datenschutzgrundsätzen. Die Pflicht zur Führung eines Verzeichnisses ersetzt die Meldepflicht von Datensammlungen nach dem bisherigen Recht. Die

[133] Es handelt sich um denselben Begriff wie in Artikel 10 Absatz 2 UWG.

Richtlinie (EU) 2016/680 sieht in Artikel 24 ein solches Verzeichnis vor; die Verordnung (EU) 2016/679 enthält in Artikel 30 eine analoge Vorschrift.

Die Pflicht zur Führung eines Verzeichnisses obliegt nach Absatz 1 dem Verantwortlichen und dem Auftragsbearbeiter.

Absatz 2 zählt die Mindestangaben auf, die das Verzeichnis enthalten muss. Dazu gehören zunächst die Identität (der Name) des Verantwortlichen (Bst. a) und der Bearbeitungszweck (Bst. b). Anzugeben ist weiter eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten (Bst. c). Mit Kategorien betroffener Personen sind typisierte Gruppen gemeint, die bestimmte gemeinsame Merkmale haben, wie z. B. «Konsumenten», «Armeeangehörige» oder «Arbeitnehmer». Die Kategorien bearbeiteter Personendaten bezeichnet die Art der bearbeiteten Daten, z. B. besonders schützenswerte Personendaten. Aufgeführt werden müssen ebenfalls die Kategorien von Empfängern (Bst. d), denen gegebenenfalls die Personendaten bekanntgegeben werden. Auch hier sind wiederum typisierte Gruppen mit gemeinsamen Merkmalen gemeint, wie z. B. «Aufsichtsbehörden». Nach Buchstabe e muss das Verzeichnis die Aufbewahrungsdauer der Personendaten enthalten. Da sich die Aufbewahrungsdauer gemäss Artikel 5 Absatz 4 nach dem Verwendungszweck richtet, lässt sich die Aufbewahrungsdauer mitunter nicht exakt festlegen, was durch die Wendung «wenn möglich» ausgedrückt wird. Sind genaue Angaben nicht möglich, muss das Verzeichnis zumindest die Kriterien enthalten, nach denen diese Dauer festgelegt wird. Gemäss Buchstabe f muss das Verzeichnis schliesslich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 7 enthalten, soweit dies möglich ist. Durch die Beschreibung soll das Verzeichnis erlauben, Mängel in den Sicherheitsvorkehren aufzuzeigen. Die Wendung «wenn möglich» macht deutlich, dass die Beschreibung nur erfolgen soll, wenn die Vorkehrungen hinreichend konkret umschrieben werden können. Befinden sich diese Empfänger im Ausland, muss aus dem Verzeichnis auch hervorgehen, ob grundsätzlich die Voraussetzungen für Bekanntgabe ins Ausland erfüllt sind. Deswegen ist nach Buchstabe g der Staat anzugeben sowie die Garantien nach Artikel 13 Absatz 2.

Die Aufzählung in Absatz 2 macht deutlich, dass das Verzeichnis eine generelle Beschreibung der Bearbeitungstätigkeit ist, aus der sich Art und Umfang einer Bearbeitung ergibt. Hingegen ist das Verzeichnis kein Journal sämtlicher Datenbearbeitungen des Verantwortlichen oder des Auftragsbearbeiters, in dem protokollartig einzelne Handlungen aufgeführt werden. Das Verzeichnis ist mithin eine schriftliche Darstellung der wesentlichen Informationen zu allen Datenbearbeitungen eines Verantwortlichen oder Auftragsbearbeiters. Es lässt damit wesentliche Rückschlüsse darauf zu, ob eine Datenbearbeitung dem Grundsatz nach datenschutzkonform ausgestaltet ist oder nicht. Darüber hinaus korrelieren die Mindestangaben des Verzeichnisses in Absatz 2 in vieler Hinsicht mit den Angaben, welche die betroffene Person aufgrund der Informationspflicht und des Auskunftsrechts erhalten muss.

Absatz 3 enthält eine verkürzte Liste von Mindestangaben des Auftragsbearbeiters. Dieser muss insbesondere die Kategorien von Bearbeitungen aufführen, die im Auftrag jedes Verantwortlichen durchgeführt werden. Das Verzeichnis des Auftragsbearbeiters enthält zudem die Identität der Verantwortlichen, für die er tätig ist.

Nach Absatz 4 melden die Bundesorgane ihre Verzeichnisse dem Beauftragten. Dieser führt nach Artikel 50 ein Register der Bearbeitungstätigkeiten der Bundesorgane. Dieses wird veröffentlicht. Für Bundesorgane werden sich damit grundsätzlich keine Änderungen im Verhältnis zum bisherigen Recht ergeben. Denn sie müssen bereits jetzt ein Bearbeitungsreglement erarbeiten sowie eine Anmeldung der Datensammlung beim Beauftragten vornehmen.

Absatz 5 gibt dem Bundesrat die Möglichkeit, für Unternehmen, die weniger als 50 Mitarbeiterinnen und Mitarbeiter beschäftigen, Ausnahmen von der Pflicht, ein Verzeichnis zu führen, vorzusehen. Dies dient insbesondere dazu, kleine und mittlere Unternehmen zu entlasten. Hierbei wird der Bundesrat jedoch nicht alleine auf die Grösse eines Unternehmens abstellen, sondern auch berücksichtigen, welche Risiken mit einer Datenbearbeitung einhergehen.

Art. 12 Zertifizierung

Artikel 12 E-DSG regelt die fakultative Zertifizierung, die gegenwärtig in Artikel 11 DSG geregelt ist. Neben Datenbearbeitungssystemen (Verfahren, Organisation) und Produkten (Programme, Systeme), ist es künftig auch möglich, bestimmte Dienstleistungen zu zertifizieren.

Zertifizierte Verantwortliche sind von der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung entbunden (Art. 20 Abs. 5 E-DSG).

Das Akkreditierungsverfahren für unabhängige Zertifizierungsstellen durch die schweizerische Akkreditierungsstelle, mit der auch der Beauftragte assoziiert ist, bleibt unverändert.[134]

Der Beauftragte hätte es vorgezogen, wenn für Bearbeitungen mit hohem Risiko eine Zertifizierungspflicht eingeführt worden wäre. Der Bundesrat hat darauf verzichtet, weil es sich dabei nicht um eine Anforderung des europäischen Rechts handelt.

9.1.3.2 Bekanntgabe von Personendaten ins Ausland

Art. 13 Grundsätze

Diese Bestimmung entspricht den Anforderungen von Artikel 12 E-SEV 108, wonach Daten grundsätzlich nur ins Ausland übermittelt werden dürfen, wenn ein angemessenes Datenschutzniveau besteht (Abs. 2). Artikel 12 Absatz 3 E-SEV 108 definiert die Fälle, in denen diese Voraussetzung erfüllt ist. Durch die Regelung in Artikel 13 E-DSG erfolgt auch eine Angleichung an das Recht der Europäischen Union (Art. 45 ff. der Verordnung [EU] 2016/679).

134 Vgl. Verordnung vom 17. Juni 1996 über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen (SR **946.512**) und Art. 2 der Verordnung vom 28. September 2007 über die Datenschutzzertifizierungen (SR **235.13**).

Die Bestimmungen zur Bekanntgabe von Personendaten ins Ausland sind unter Berücksichtigung der Ergebnisse des Vernehmlassungsverfahrens teilweise überarbeitet worden. Der Grundsatz, wonach Personendaten nicht ins Ausland bekannt gegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, wird aufgehoben, da er in Bezug auf die Systematik der Regelung eine Rechtsunsicherheit schafft. Die Terminologie betreffend die Bekanntgabe von Personendaten ins Ausland auf der Grundlage geeigneter Garantien wird an jene der Verordnung (EU) 2016/679 angepasst. Die Ausnahmen im Zusammenhang mit der Bekanntgabe von Personendaten in einen Staat, dessen Gesetzgebung keinen angemessenen Datenschutz bietet, werden zudem leicht gelockert. Schliesslich werden lediglich die durch den E-SEV 108 geforderten Pflichten zur Information des Beauftragten und zur Einholung seiner Genehmigung beibehalten.

Abs. 1 Feststellung per Entscheid des Bundesrats

Gemäss Absatz 1 dürfen Daten ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet. Diese Bestimmung überträgt dem Bundesrat ausdrücklich die Zuständigkeit, die Angemessenheit der ausländischen Gesetzgebung im Bereich des Datenschutzes zu prüfen.

Die aktuelle Situation ist unbefriedigend, weil es dem Inhaber einer Datensammlung, der Daten bekannt geben will, obliegt zu prüfen, ob die Gesetzgebung des betreffenden Staates einen angemessenen Schutz[135] gewährleistet. Gegebenenfalls hat er die Liste des Beauftragten mit den Staaten, die diese Anforderung erfüllen, beizuziehen (Art. 7 VDSG).[136]

Um eine einheitliche Anwendung von Artikel 13 sicherzustellen, wird die Angemessenheit der ausländischen Gesetzgebung in Zukunft durch den Bundesrat geprüft. Bei seiner Prüfung muss der Bundesrat nicht nur untersuchen, ob der ausländische Staat über eine Gesetzgebung verfügt, die materiell den Anforderungen des E-SEV 108 genügt, sondern auch wie diese Gesetzgebung angewendet wird. Der Bundesrat kann auch prüfen, ob der durch ein internationales Organ garantierte Datenschutz angemessen ist. Der Begriff «internationales Organ» bezieht sich auf alle internationalen Institutionen, seien dies Organisationen oder Gerichte.

Das Ergebnis dieser Prüfung wird in einer Verordnung des Bundesrates veröffentlicht, die in die Amtliche Sammlung aufgenommen wird. In der künftigen Verordnung wird präzisiert werden, dass der Bundesrat die Situation periodisch evaluieren und dass der Beauftragte auf seiner Website eine Liste der Staaten oder internationalen Organe veröffentlichen wird, die gemäss der Feststellung des Bundesrates einen angemessenen Datenschutz gewährleisten.

Die Verordnung ist als Positiv-Liste konzipiert und enthält eine Aufzählung jener Staaten, die über eine Gesetzgebung verfügen, aufgrund welcher ein angemessener Schutz sichergestellt ist. Wenn ein ausländischer Staat nicht in der Verordnung des

135 BBl **2003** 2128–2129

136 Die Liste des Beauftragten ist unter der folgenden Adresse abrufbar: www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de.

Bundesrates enthalten ist, kann dies zwei Ursachen haben: Entweder wurde die Gesetzgebung des fraglichen Staates noch nicht geprüft oder der Bundesrat ist zum Schluss gekommen, dass die Gesetzgebung des Staates den Anforderungen der Gewährleistung eines angemessenen Schutzes nicht entspricht. Mit der Revision wird die Feststellung des Bundesrates für die Verantwortlichen, die eine Bekanntgabe von Daten ins Ausland vorsehen, ein gesetzlich verbindliches Kriterium, während die bisherige Liste des Beauftragten lediglich als Hilfsmittel gedacht war, das diesen zur Verfügung gestellt wurde. Diese Lösung dient der Rechtssicherheit.

Für seine Prüfung kann sich der Bundesrat auf die verfügbaren Quellen stützen, namentlich die Evaluationen, die im Rahmen des Übereinkommens SEV 108 oder durch die Europäische Union durchgeführt werden. Es wäre auch denkbar, mit ausländischen Behörden zusammenzuarbeiten und sich deren Evaluationsprozess anzuschliessen.

Wenn der Bundesrat feststellt, dass die Gesetzgebung eines Staates oder ein internationales Organ einen angemessenen Schutz gewährleistet, ist der freie Verkehr von Personendaten aus der Schweiz in diesen Staat oder zu diesem Organ sowohl durch private Verantwortliche als auch durch Bundesorgane zulässig.

Abs. 2 Kein Entscheid des Bundesrates

Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, sieht Absatz 2 vor, dass Personendaten ins Ausland bekannt gegeben werden können, wenn ein geeigneter Datenschutz gewährleistet wird.

Nach Buchstabe a kann ein geeigneter Schutz durch einen völkerrechtlichen Vertrag gewährleistet werden. Unter «völkerrechtlicher Vertrag» ist nicht nur ein internationales Datenschutzübereinkommen wie das Übereinkommen SEV 108 und sein Zusatzprotokoll zu verstehen, dem der Empfängerstaat angehört und dessen Anforderungen von der Vertragspartei im innerstaatlichen Recht umgesetzt worden sind, sondern auch jedes andere internationale Abkommen, das einen Datenaustausch zwischen den Vertragsparteien vorsieht und materiell den Anforderungen des Übereinkommens SEV 108 entspricht. Dabei kann es sich auch um einen Staatsvertrag handeln, den der Bundesrat im Rahmen von Artikel 61 Buchstabe b E-DSG abgeschlossen hat.

Absatz 2 Buchstaben b–d entspricht den Anforderungen von Artikel 12 Absatz 3 Buchstabe b E-SEV 108. Dieser sieht vor, dass ein angemessenes Datenschutzniveau durch genehmigte Ad-hoc- und standardisierte Garantien gewährleistet werden kann, die auf rechtlich bindenden und durchsetzbaren Instrumenten beruhen, welche durch die mit der Bekanntgabe und Weiterbearbeitung der Daten befassten Personen vereinbart und umgesetzt werden. In Artikel 46 der Verordnung (EU) 2016/679 und in Artikel 37 der Richtlinie (EU) 2016/680 sind entsprechende Regelungen vorgesehen.

Bst. b Datenschutzklauseln in einem Vertrag

Nach Absatz 2 Buchstabe b dürfen Personendaten ins Ausland bekannt gegeben werden, wenn der Verantwortliche und der Vertragspartner in ihrem Vertrag Datenschutzklauseln vereinbart haben. Der Begriff «Datenschutzklauseln» entspricht der

Terminologie von Artikel 46 Absatz 3 Buchstabe a der Verordnung (EU) 2016/679. Die Klauseln müssen dem Beauftragten vorgängig mitgeteilt werden. Sobald der Verantwortliche dieser Pflicht nachgekommen ist, dürfen die Personendaten ins Ausland bekanntgegeben werden. Gegebenenfalls muss der Beauftragte eine Untersuchung eröffnen, um festzustellen, ob die Klauseln den Anforderungen genügen. Wie es heute bereits der Fall ist, ist es Sache des Verantwortlichen, nachzuweisen, dass er alle erforderlichen Massnahmen getroffen hat, um sich zu vergewissern, dass ein geeigneter Schutz besteht und dass der Empfänger die vertraglichen Datenschutzklauseln einhält. Im Gegensatz zu den Standarddatenschutzklauseln (siehe Bst. d) gelten die Datenschutzklauseln in einem Vertrag nur für die Bekanntgabe, die im entsprechenden Vertrag vorgesehen ist.

Bst. c Spezifische Garantien

Im öffentlichen Sektor kann ein Bundesorgan, das einem ausländischen Staat die Zusage für die Zusammenarbeit erteilt, die Zusage an spezifische Garantien für den Bereich des Datenschutzes knüpfen. Dabei kann es sich beispielsweise um entsprechende Vereinbarungen mit dem fraglichen ausländischen Staatsorgan handeln. Das Bundesorgan muss sie dem Beauftragten vorgängig mitteilen. Sobald der Verantwortliche dieser Pflicht nachgekommen ist, dürfen die Personendaten ins Ausland bekanntgegeben werden.

Bst. d Standarddatenschutzklauseln

Nach Absatz 2 Buchstabe d können Daten gestützt auf Standarddatenschutzklauseln ins Ausland bekannt gegeben werden. Die Bestimmung übernimmt die Terminologie von Artikel 46 Absatz 2 Buchstaben c und d der Verordnung (EU) 2016/679. Die Standardklauseln können von Privaten, interessierten Kreisen oder Bundesorganen erarbeitet oder vom Beauftragten ausgestellt oder anerkannt werden. Auch die Bundesorgane können auf diese Art von Garantien zurückgreifen. Der Begriff der «Standarddatenschutzklausel» betrifft beispielsweise standardisierte Vertragsklauseln, die in den Vertrag zwischen dem Verantwortlichen und dem Empfänger eingefügt werden. Es kann sich auch um einen von Privaten erarbeiteten Verhaltenskodex handeln, dem sich Privatpersonen freiwillig unterstellen können.

Im ersten Fall müssen die Standarddatenschutzklauseln vorgängig vom Beauftragten genehmigt werden. Diese Bedingung stellt gegenüber dem geltenden Recht, wonach der Beauftragte lediglich informiert werden muss (Art. 6 Abs. 3 DSG), eine Verschärfung dar. Sie entspricht der Anforderung von Artikel 12bis Absatz 2 Buchstabe b E-SEV 108. Der Verantwortliche darf gestützt auf die Standarddatenschutzklauseln keine Daten ins Ausland bekannt geben, bis er vom Beauftragten eine entsprechende beschwerdefähige Verfügung (Art. 5 VwVG) erhalten hat. Während der Dauer des Verfahrens kann er sich auf Artikel 13 Absatz 2 Buchstaben b oder c stützen. Die Frist, innerhalb der der Verantwortliche eine Verfügung erlassen muss, wird durch die Ordnungsfristenverordnung vom 25. Mai 2011[137] (OrFV) geregelt. Gemäss Artikel 4 OrFV hängt die Frist, innerhalb der eine Behörde ihren Entscheid fällt, von der Komplexität des Entscheids ab, wobei die maximale Frist drei Monate beträgt.

137 SR **172.010.14**

Im zweiten Fall kann der Verantwortliche auch auf Standarddatenschutzklauseln zurückgreifen, die der Beauftrage ausgestellt oder anerkannt hat, beispielsweise Musterverträge.

Beschliesst ein Verantwortlicher, Daten gestützt auf Standarddatenschutzklauseln im Sinne von Absatz 2 Buchstabe d ins Ausland bekannt zu geben, wird vermutet, dass er alle notwendigen Massnahmen getroffen hat, um sich eines angemessenen Schutzes zu vergewissern. Allerdings befreit ihn diese Vermutung nicht von der Haftung für Nachteile, die sich aus einer Verletzung dieser Klauseln insbesondere durch den Empfänger der Daten ergeben können. In der künftigen Verordnung ist daher die Pflicht des Beauftragten vorzusehen, eine Liste der ausgestellten oder anerkannten Standarddatenschutzklauseln zu veröffentlichen, wie es im Übrigen im geltenden Recht vorgesehen ist (Art. 6 Abs. 3 VDSG).

Bst. e Verbindliche unternehmensinterne Datenschutzvorschriften

Nach Absatz 2 Buchstabe e kann die Bekanntgabe von Daten ins Ausland auch gestützt auf verbindliche unternehmensinterne Datenschutzvorschriften erfolgen, die vorgängig durch den Beauftragten oder durch eine ausländische Behörde, die für den Datenschutz zuständig ist, genehmigt wurden. Diese Bestimmung ersetzt Artikel 6 Absatz 2 Buchstabe g DSG. Absatz 2 Buchstabe e nähert sich dem Recht der Europäischen Union an, das in Artikel 47 der Verordnung (EU) 2016/679 vorsieht, dass Daten gestützt auf vorgängig von der Datenschutzaufsichtsbehörde genehmigte, verbindliche interne Datenschutzvorschriften zwischen den Mitgliedern einer Unternehmensgruppe übermittelt werden können. Die Genehmigung verbindlicher unternehmensinterner Vorschriften ist in Artikel 57 Absatz 1 Buchstabe s der Verordnung (EU) 2016/679 festgehalten. Absatz 2 Buchstabe e stellt insofern eine Verschärfung des geltenden Rechts dar, als die verbindlichen unternehmensinternen Datenschutzvorschriften neu genehmigt werden müssen. Der Verantwortliche darf gestützt auf die verbindlichen unternehmensinternen Datenschutzvorschriften keine Daten ins Ausland bekannt geben, bis er vom Beauftragten eine entsprechende beschwerdefähige Verfügung (Art. 5 VwVG) erhalten hat. Während der Dauer des Verfahrens kann er sich auf Artikel 13 Absatz 2 Buchstaben b oder c stützen.

Zur Berücksichtigung der Bedürfnisse von Unternehmensgruppen, die sich über mehrere Länder erstrecken, sieht Absatz 2 Buchstabe e vor, dass ein Unternehmen mit Sitz in der Schweiz, das zu einer solchen Gruppe gehört, auch verbindliche Datenschutzvorschriften befolgen kann, die durch eine ausländische Behörde genehmigt wurden, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet.

Die in Absatz 2 Buchstabe e erwähnten Instrumente müssen in dem Sinne «verbindlich» sein, als alle Gesellschaften, die zur selben Unternehmensgruppe gehören, die Vorschriften einzuhalten und anzuwenden haben. Diese Normen präzisieren mindestens die fragliche Datenbekanntgabe, die Kategorien bekannt gegebener Daten, den Zweck der Bearbeitung, die Kategorien betroffener Personen und die Empfängerstaaten. Ausserdem müssen die Normen die Rechte der betroffenen Personen regeln und auch Angaben über die Mechanismen enthalten, die innerhalb der Unternehmensgruppe eingerichtet worden sind, um ihre Einhaltung zu überprüfen. Gegebe-

nenfalls kann der Bundesrat in der Ausführungsverordnung Kriterien definieren, welche die verbindlichen unternehmensinternen Vorschriften erfüllen müssen.

Abs. 3 Rechtsetzungsdelegation

In dieser Bestimmung wird der Bundesrat ermächtigt, andere geeignete Garantien nach Absatz 2 vorzusehen. Denn es ist nicht ausgeschlossen, dass andere Systeme entwickelt werden wie beispielsweise Selbstzertifizierungsregelungen gemäss dem Modell des Swiss-US Privacy Shield (siehe Art. 46 Abs. 2 Bst. f der Verordnung [EU] 2016/679).

Art. 14 Ausnahmen

Abs. 1

In Anlehnung an das geltende Recht (Art. 6 Abs. 2 DSG) regelt Artikel 14 Absatz 1 E-DSG die Fälle, in denen Daten ins Ausland bekannt gegeben werden können, obwohl im Ausland ein angemessener Schutz fehlt. Er entspricht im Wesentlichen Artikel 12 Absatz 4 E-SEV 108 und Artikel 49 der Verordnung (EU) 2016/679. Die Richtlinie (EU) 2016/680 enthält eine entsprechende Regelung in Artikel 38.

Buchstabe a entspricht Artikel 6 Absatz 2 Buchstabe b DSG, wobei die betroffene Person ausdrücklich einwilligen muss und der Ausdruck «im Einzelfall» gestrichen wird. Die ausdrückliche Einwilligung ist eine Anforderung des E-SEV 108 (Art. 12 Abs. 4 Bst. a). Diesbezüglich kann auf die Erläuterungen zu Artikel 5 Absatz 6 E-DSG verwiesen werden. Die betroffene Person muss insbesondere den Namen des Drittstaats kennen (Art. 17 Abs. 4 E-DSG) und über die Risiken der Bekanntgabe im Zusammenhang mit dem Datenschutzniveau im ausländischen Staat informiert werden. Was den Ausdruck «im Einzelfall» betrifft, ist der Bundesrat der Auffassung, dass er gestrichen werden kann. Wie aus Artikel 5 Absatz 6 E-DSG hervorgeht, willigt die betroffene Person für eine oder mehrere bestimmte Bearbeitungen ein. Die Präzisierung «im Einzelfall» ist somit überflüssig.

Buchstabe b entspricht Artikel 6 Absatz 2 Buchstabe c DSG unter dem Vorbehalt, dass Personendaten ins Ausland bekannt gegeben werden dürfen, wenn die Bekanntgabe in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person oder zwischen dem Verantwortlichen und seinem Vertragspartner im Interesse der betroffenen Person steht. Artikel 49 Absatz 1 der Verordnung (EU) 2016/679 sieht eine analoge Bestimmung vor.

Buchstabe c Ziffer 1 entspricht Artikel 6 Absatz 2 Buchstabe d erster Satzteil DSG. Der Ausdruck «unerlässlich» wird in Anlehnung an die europäischen Rechtsakte im Einleitungssatz durch «notwendig» ersetzt. Das Vorliegen eines überwiegenden öffentlichen Interesses muss unter den konkreten Umständen nachgewiesen werden. Ein rein hypothetisches Interesse genügt nicht. Unter der «Wahrung eines überwiegenden öffentlichen Interesses» ist beispielsweise die innere Sicherheit der Schweiz oder eines Drittstaates zu verstehen. Aufgrund dieser Bestimmung dürfen Personendaten auch aus humanitären Gründen ins Ausland bekannt gegeben werden, beispielsweise wenn der Verantwortliche sie bekannt gibt, um bei der Suche nach

Personen zu helfen, die in einem Konfliktgebiet vermisst werden oder in einer Region, in der eine Naturkatastrophe stattgefunden hat.

Buchstabe c Ziffer 2 entspricht Artikel 6 Absatz 2 Buchstabe d zweiter Satzteil DSG, ausser dass der Ausdruck «vor Gericht», der als zu eng befunden wird, durch «vor einem Gericht oder einer anderen zuständigen ausländischen Behörde» ersetzt wird.

In Buchstabe d wird präzisiert, dass die Bekanntgabe auch zulässig ist, wenn sie notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, soweit es nicht möglich ist, die Einwilligung der betroffenen Person innert angemessener Frist einzuholen. Dies kann der Fall sein, weil diese körperlich nicht dazu in der Lage ist oder weil sie mit Hilfe der üblichen Kommunikationsmittel nicht erreichbar ist.

Buchstabe e entspricht Artikel 6 Absatz 2 Buchstabe f DSG.

Buchstabe f ist eine neue Bestimmung. Sie präzisiert, dass die Anforderung eines angemessenen Schutzes nicht anwendbar ist, wenn die ins Ausland bekannt zu gebenden Daten aus einem gesetzlich geregelten öffentlichen Register stammen und bestimmte gesetzliche Voraussetzungen erfüllt sind. Artikel 49 Absatz 1 Buchstabe g der Verordnung (EU) 2016/679 verfolgt dieselbe Stossrichtung: Er sieht vor, dass die Bekanntgabe von Daten aus einem Register trotz des Fehlens eines angemessenen Schutzes zulässig ist, wenn das Register gemäss dem Recht der Europäischen Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und bestimmte gesetzliche Voraussetzungen erfüllt sind.

Abs. 2

Gemäss dieser Bestimmung kann der Beauftragte den Verantwortlichen oder den Auftragsbearbeiter anfragen, ihm die nach Absatz 1 Buchstaben b Ziffer 2, c und d erfolgten Bekanntgaben von Personendaten mitzuteilen. Die Bestimmung entspricht den Anforderungen von Artikel 12 Absatz 5 E-SEV 108. Der vorletzte Satz von Artikel 49 Absatz 1 der Verordnung (EU) 2016/679 geht weiter als diese Bestimmung, denn er sieht vor, dass die Verantwortlichen die Aufsichtsbehörde von selbst über die nach Artikel 47 erfolgten Übermittlungen von Personendaten in Kenntnis setzen.

Art. 15 Veröffentlichung von Personendaten in elektronischer Form

Diese Bestimmung übernimmt den Inhalt von Artikel 5 VDSG. Sie regelt die Veröffentlichung von Personendaten über das Internet oder andere Informations- und Kommunikationsdienste zwecks Information der Öffentlichkeit. So ist es möglich, im Ausland – auch in Staaten, die nicht einen angemessenen Datenschutz gewährleisten – im Internet Informationen mit oder ohne Personendaten abzurufen. Die Veröffentlichung von Personendaten im Internet zwecks Information der Öffentlichkeit wird, wie beispielsweise im Falle der Medien, nicht als Bekanntgabe von Personendaten ins Ausland betrachtet.

9.1.3.3 Daten von verstorbenen Personen

Art. 16

Die Bestimmung regelt verschiedene Aspekte des Umgangs mit Daten einer verstorbenen Person. Dieser gibt in der Praxis regelmässig zu Fragen Anlass. Dabei stellen sich grundsätzliche Fragen wie zum Beispiel, in welchem Umfang die Persönlichkeit einer verstorbenen Person geschützt ist und in welchem Verhältnis ein allfälliger Schutz zu Anliegen von Hinterbliebenen steht. Verfassungsrechtlich reicht der Persönlichkeitsschutz (Art. 10 und 13 Abs. 1 BV) über den Tod eines Menschen hinaus, z. B. in Bezug auf Bestattungswünsche der verstorbenen Person.[138] Hingegen ist in der Schweiz bislang kein eigentliches postmortales Persönlichkeitsrecht anerkannt, das die verstorbene Person auch dann schützt, wenn sie zu Lebzeiten keine entsprechenden Wünsche geäussert hat oder keine Angehörigen vorhanden sind, die sich für ihren Schutz einsetzen.[139] Zivilrechtlich erlischt die Persönlichkeit mit dem Tod (vgl. Art. 31 Abs. 1 ZGB).[140] Dennoch geht das Bundesgericht davon aus, dass in bestimmten Bereichen die Wirkungen des Persönlichkeitsrechts und damit auch des Persönlichkeitsschutzes über den Tod hinausgehen können.[141] Da der Datenschutz dem Persönlichkeitsschutz dient, muss dies prinzipiell auch für Daten verstorbener Personen gelten. Strafrechtlich ist die Persönlichkeit über den Tod hinaus geschützt, so u. a. wenn es um den strafrechtlichen Geheimnisschutz geht.[142]

Der Umgang mit Daten Verstorbener wird bisher einzig durch eine Verordnungsbestimmung in Artikel 1 Absatz 7 VDSG geregelt. So ist die Einsicht in Daten Verstorbener bisher ein Teilanspruch des Auskunftsrechts. Dabei handelt es sich jedoch um ein Recht der betroffenen Person, das nur in Bezug auf Datenbearbeitungen, die sie selbst betreffen, geltend gemacht werden kann. Aufgrund der Verordnungsbestimmung wird das Auskunftsrecht auf Drittpersonen ausgeweitet, die Auskunft über Daten einer weiteren Drittperson verlangen können, ohne dass hierfür im Gesetz eine entsprechende Grundlage vorhanden gewesen wäre. Durch die Aufnahme ins Gesetz soll dieses Problem beseitigt werden. Systematisch wird die Norm nun den allgemeinen Datenschutzbestimmungen zugeordnet und dadurch vom Auskunftsrecht losgelöst, weil dieses auf die betroffene Person beschränkt bleiben soll. Im Ergebnis wird damit das geltende Recht übernommen und, wo nötig, materiell und formell präzisiert sowie ergänzt sowie bestehende Unsicherheiten beseitigt. Gleichzeitig wird sichergestellt, dass dem Willen der verstorbenen Person bestmöglich Rechnung getragen wird.

Neben der Einsicht in die Daten einer verstorbenen Person wird mit der vorgesehenen Bestimmung teilweise dem Postulat 14.3782 Schwaab «Richtlinien für den ‹digitalen Tod›» Rechnung getragen, indem in Absatz 2 ein Recht auf Löschung

138 BGE **129** I 173 E. 4; **127** I 115 E. 4a; SGK-Schweizer, Art. 10 BV N 10; BSK-Tschentscher, Art. 10 BV N 47 ff. Unklar ist, ob dies auch für die informationelle Selbstbestimmung nach Artikel 13 Absatz 2 BV gilt.
139 Vgl. hierzu BSK-Tschentscher, Art. 10 BV N 47 ff.
140 Vgl. BGE **109** II 353; **127** I 145; **129** I 173; **129** I 302.
141 BGE **129** I 302 E. 1.2.
142 Vgl. BGE **135** III 597; **125** IV 298; **118** IV 319; **118** IV 153.

bzw. Vernichtung der Daten des Verstorbenen durch die Erben vorgesehen ist. Dies erlaubt es den Erben sowie einem allfälligen Willensvollstrecker grundsätzlich, den «digitalen Tod» herbeizuführen, ausser dem stünden überwiegende Interessen des Verantwortlichen oder Dritter oder ein besonderes Schutzbedürfnis des Erblassers entgegen oder der Erblasser hätte dies ausdrücklich untersagt. Weitere Fragen, die sich im Zusammenhang mit dem erwähnten Postulat stellen, zum Beispiel betreffend die Übertragbarkeit oder eine mögliche Vererbung von Daten, werden im Rahmen der derzeit laufenden Revision des Erbrechts[143] geprüft. Parallel zu Artikel 16 E-DSG sieht die laufende Revision des Erbrechts ein Einsichtsrecht vor, das ausschliesslich für Personen gilt, die erbrechtliche (und damit vermögensrechtliche) Ansprüche geltend machen können und ihnen erlauben soll, im Rahmen des Erbgangs ihre Vermögensrechte geltend zu machen (Art. 601*a* VE-ZGB).

Die Bestimmung wurde im Vergleich zur Vernehmlassungsvorlage gestrafft und etwas differenziert, ohne den Inhalt grundlegend zu verändern. Insbesondere wurde Artikel 12 Absatz 3 VE-DSG nicht übernommen, und die Bestimmungen zum Amts- und Berufsgeheimnis bleiben entsprechend anwendbar (siehe dazu unten), weil strafrechtlich relevante Schutzlücken zu vermeiden sind.

Abs. 1 Einsicht

Gemäss Absatz 1 muss der Verantwortliche kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn kumulativ die drei Voraussetzungen erfüllt sind, die in den Buchstaben a bis c aufgezählt sind.

Nach Buchstabe a ist Voraussetzung der Einsicht, dass entweder ein schutzwürdiges Interesse daran vorliegt oder dass die Person, die Einsicht verlangt, mit der verstorbenen Person in gerader Linie verwandt, mit ihr zum Todeszeitpunkt verheiratet war, in eingetragener Partnerschaft lebte oder eine faktische Lebensgemeinschaft führte oder ihr Willenvollstrecker ist. Ein schutzwürdiges Interesse, das die Einsicht rechtfertigt, liegt beispielsweise vor, wenn die fraglichen Daten für die Einsicht verlangende Person in einem Verfahren oder im Zusammenhang mit eigenen rechtlichen Ansprüchen, insb. ihrem Persönlichkeitsschutz, relevant sind bzw. relevant sein können (z. B. als Beweismittel). Auch die Klärung von familiären oder persönlichen Konflikten oder ein wissenschaftliches Forschungsprojekt kann ein schutzwürdiges Interesse darstellen. Reine Neugier reicht hingegen als schutzwürdiges Interesse nicht aus. Die in Buchstabe a aufgezählten nahestehenden Personen müssen im Unterschied zu allen übrigen Personen hingegen kein schutzwürdiges Interesse nachweisen, weil das enge Verwandtschafts- oder Beziehungsverhältnis zu einer Person stets für ein solches schutzwürdiges Interesse an der Einsicht in die Daten dieser Person spricht.[144] Dasselbe gilt für den Willensvollstrecker, der nur auf diese Weise seiner Funktion, die Interessen des Erblassers zu wahren und dessen Willen umzusetzen, insbesondere aber die Erbschaft zu verwalten, vollumfänglich gerecht werden kann. Die betreffenden Personen müssen lediglich nachweisen, dass sie zur verstorbenen Person in einer solchen engeren Beziehung standen.

143 Vgl. www.bj.admin.ch/bj/de/home/gesellschaft/gesetzgebung/erbrecht.html.

144 In Bezug auf den Begriff der faktischen Lebensgemeinschaft ist insbesondere auf Lehre und Rechtsprechung betreffend Artikel 165 Absatz 1 Buchstabe a ZPO oder Artikel 10 Absatz 1 Ziffer 2 SchKG zu verweisen.

Nach Buchstabe b dürfen der Einsicht nicht eine ausdrückliche Erklärung der verstorbenen Person oder ein besonderes Schutzbedürfnis dieser Person entgegenstehen. Nach dieser Bestimmung ist die Einsicht stets zu verweigern, wenn die verstorbene Person die Einsicht in ihre Daten ausdrücklich untersagt hat. Auf diese Weise wird der explizit geäusserte Willen der verstorbenen Person verwirklicht, indem dieser stets vorgeht. Damit ist sichergestellt, dass jede Person selbst entscheiden und darüber verfügen kann, ob und wer Einsicht in ihre Daten erhält, auch nach ihrem Tod. Denkbar ist, dass eine verstorbene Person die Einsicht pauschal untersagt oder beschränkt auf bestimmte Personen oder auf bestimmte Daten. Eine solche Erklärung hat wie in Artikel 26 Absatz 2 Buchstabe b E-DSG ausdrücklich zu erfolgen; dazu kann auf die Ausführungen bei diesem Artikel verwiesen werden. Angesichts des Ablebens der erklärenden Person hat eine solche Erklärung im Interesse der möglichst einfachen Beweisbarkeit sinnvollerweise in einer möglichst durch Text nachweisbaren Form zu erfolgen, beispielsweise im Rahmen einer Patientenverfügung oder in einer eindeutigen Mitteilung (schriftlich, aber z. B. auch elektronisch per E-Mail) direkt gegenüber dem Verantwortlichen. Ebenfalls möglich wäre eine entsprechende Erklärung in einem Testament. Auch ohne ausdrückliche Erklärung der verstorbenen Person kann der Einsicht ein besonderes Schutzbedürfnis der verstorbenen Person entgegenstehen, sodass die Einsicht zu verweigern ist, weil diese geradezu stossend erschiene. Von einem solchen besonderen Schutzbedürfnis ist etwa dann auszugehen, wenn es um spezifische (medizinische) Daten in einem Patientendossier oder in der Anwaltskorrespondenz geht, die nicht mehr zu den üblichen Angaben und Informationen zu zählen sind, wie beispielsweise Daten zu Sexualleben oder Geschlechtskrankheiten, zu (lasterhaftem) Lebenswandel oder bestimmten Rechtsgeschäften, bei denen im konkreten Fall davon auszugehen ist, dass sie die verstorbene Person nicht oder nicht gegenüber der Einsicht verlangenden Person preisgeben wollte.

Gemäss Buchstabe c dürfen der Einsicht schliesslich keine überwiegenden Interessen des Verantwortlichen oder von Dritten entgegenstehen. Die Interessen von Angehörigen gemäss dem aktuellen Artikel 1 Absatz 7 VDSG sind zu den Interessen Dritter zu zählen. Die Bestimmung verlangt eine Interessenabwägung. Auf der einen Seite steht dabei das Interesse der Einsicht verlangenden Person am Zugang zu den fraglichen Daten und damit daran, die fraglichen Informationen zu erhalten. Auf der anderen Seite steht das Interesse des Verantwortlichen oder von Dritten, dass die fraglichen Informationen geheim bleiben oder der Einsicht verlangenden Person nicht zur Kenntnis gebracht werden. Wann diese Interessen überwiegen, ist im Einzelfall zu entscheiden. Dabei ist unter anderem zu berücksichtigen, welche Bedeutung die fraglichen Daten für die beteiligten Person haben und zu welchem Zweck die Einsicht verlangt wird. Überwiegende Interessen des Verantwortlichen, die einer Einsicht entgegenstehen, können beispielsweise eigene Geheimhaltungsinteressen oder sogar Geheimhaltungspflichten sein. Am bedeutsamsten dürften in der Praxis diejenigen Fälle sein, in denen der Einsicht Interessen Dritter entgegenstehen. So ist beispielsweise denkbar, dass durch die Einsicht in Daten zugleich bekannt wird, dass die verstorbene Person schon einmal verheiratet war oder ein uneheliches Kind hatte. Zu beachten ist, dass Personen gegebenenfalls das Recht auf Nichtwissen haben (vgl. Art. 6 GUMG).

Artikel 16 E-DSG gilt auch, wenn Einsicht in Daten verlangt wird, die durch eine strafrechtliche Amts- oder Berufsgeheimnispflicht (Art. 320 f. StGB) des Verantwortlichen oder durch die Strafbestimmung von Artikel 56 geschützt sind. Zu denken ist beispielsweise an den Sohn, der beim Hausarzt seines verstorbenen Vaters Einsicht in dessen medizinischen Daten verlangt. Zwar gilt die strafrechtliche Schweigepflicht für Amts- und Berufsgeheimnisträger auch über den Tod des Geheimnisherrn hinaus,[145] weshalb Geheimnisträger grundsätzlich nicht zur Offenbarung verpflichtet werden können. Sind aber die Voraussetzungen von Artikel 16 Absatz 1 E-DSG erfüllt, ist auch ein solcher Geheimnisträger *berechtigt*, Einsicht in die Daten einer verstorbenen Person zu geben. Die Offenbarung ist diesfalls eine rechtmässige Handlung im Sinne von Artikel 14 StGB und der Geheimnisträger kann nicht wegen Verletzung des Amts- oder Berufsgeheimnisses bestraft werden. Artikel 16 E-DSG schafft damit einen neuen Rechtfertigungsgrund für den Geheimnisträger, wo bislang lediglich die Einwilligung des Geheimnisherrn bzw. dessen mutmassliche Einwilligung einen solchen Grund bildeten.

Artikel 16 E-DSG verlangt eine Interessenabwägung durch den Geheimnisträger, die in den meisten Fällen unproblematisch sein dürfte. Irrt der Geheimnisträger jedoch über das Vorliegen oder die Bedeutung der Voraussetzungen von Artikel 16 Absatz 1 E-DSG, ist ein Sachverhaltsirrtum nach Artikel 13 StGB oder ein Verbotsirrtum nach Artikel 21 StGB zu prüfen. Zweifelt er an der Richtigkeit seiner Interessenabwägung und sind die Voraussetzungen von Artikel 16 nicht erfüllt, liegt möglicherweise eine eventualvorsätzliche Verletzung seiner strafrechtlichen Geheimnispflicht vor, wenn er ein Geheimnis offenbart.

Wenn dem Amts- oder Berufsgeheimnisträger die Gewichtung der Interessen nicht klar erscheint, steht es ihm jedenfalls frei, sich durch eine zuständige Behörde nach Artikel 320 Ziffer 2 bzw. Artikel 321 Ziffer 2 StGB formell von seiner Geheimnispflicht entbinden zu lassen. Die Behörde nimmt diesfalls eine Interessenabwägung nach Artikel 16 Absatz 1 E-DSG vor; der Amts- oder Berufsgeheimnisträger trägt diesfalls kein Strafbarkeitsrisiko.

Wird ein Berufsgeheimnis (Art. 321 StGB) erst nach dem Tod des Geheimnisherrn offenbart, können Dritte den Strafantrag stellen, sofern ein Gesetz dies vorsieht; diese Befugnis kann sich auch aus einer ausserstrafgesetzlichen Norm ergeben. Betrifft eine Information mehrere Personen (z. B. Angaben über eine geheim gehaltene Vaterschaft) haben Dritte ein Strafantragsrecht, wenn ihnen hinsichtlich der Information die Stellung als Geheimnisherr zukommt.[146]

Falls der Geheimnisträger hingegen eigene Interessen an der Wahrung des Amts- oder Berufsgeheimnisses hat, können diese im Rahmen der Abwägung nach Absatz 1 Buchstabe c berücksichtigt werden.

Klagen zur Geltendmachung der Einsicht nach Artikel 16 Absatz 1 E-DSG können gegenüber privaten Verantwortlichen gemäss Artikel 243 Absatz 2 Buchstabe d E-ZPO im vereinfachten Verfahren geltend gemacht werden. Dieses Verfahren zeichnet sich insbesondere dadurch aus, dass es möglichst unkompliziert und laien-

145 BGE **87** IV 105, 107.
146 Zum Ganzen vgl. BGE **87** IV 105, 110; Oberholzer Niklaus, Basler Kommentar Strafrecht II, Basel 2013, Art. 321 N 34; Riedo Christof, Der Strafantrag, Basel 2004, 302 ff.

freundlich ausgestaltet ist («sozialer Zivilprozess»).[147] So ermittelt der Richter den Sachverhalt in den Fällen nach Artikel 243 Absatz 2 ZPO von Amtes wegen (beschränkte Untersuchungsmaxime, Art. 247 Abs. 2 Bst. b ZPO) und greift insgesamt stärker in die Prozessführung ein. Dies soll es auch Laien erlauben, grundsätzlich ohne Beizug eines Anwalts an das Gericht zu gelangen. Das Verfahren ist aufgrund von Artikel 113 Absatz 2 Buchstabe g und Artikel 114 Buchstabe f E-ZPO zudem von den Gerichtskosten befreit.

Abs. 2 Gesuch an die Aufsichtsbehörde

Absatz 2 betrifft die Konstellation, dass ein Verantwortlicher, der einem Amts- oder Berufsgeheimnis untersteht, die Einsicht unter Hinweis auf dieses Geheimnis verweigert. Für diesen Fall sieht Absatz 2 vor, dass sich auch die nach Absatz 1 Buchstabe a berechtigten Personen an die zuständige Behörde nach den Artikeln 320 und 321 des Strafgesetzbuches wenden können, um diese um Entbindung des Verantwortlichen von seiner Geheimhaltungspflicht zu ersuchen.

Grundsätzlich kann lediglich der Geheimnisträger, hier der Verantwortliche, an die Aufsichtsbehörde bzw. die vorgesetzte Behörde gelangen, um sich vom Amts- oder Berufsgeheimnis entbinden zu lassen, denn es liegt in seinem Interesse, einen Rechtfertigungsgrund für das tatbestandsmässige Verhalten zu erlangen[148]. Nach Absatz 2 soll es nun in diesen Fällen auch Drittpersonen erlaubt sein, direkt an die zuständige Behörde zu gelangen und um die Entbindung des Geheimnisträgers ersuchen zu können. Diese Möglichkeit wird nun für die besondere Konstellation des datenschutzrechtlichen Einsichtsrechts in Daten einer verstorbenen Person vorgesehen, zumal hier – eine Entbindung zu Lebzeiten vorbehalten – eine Entbindung durch den (verstorbenen) Geheimnisherr ausgeschlossen ist. Dadurch wird den verschiedenen sich gegenüberstehenden Interessen in ausgewogener Weise Rechnung getragen. Der Verantwortliche kann die Einsicht verlangende Person an die Aufsichtsbehörde verweisen und ist dadurch entlastet, insbesondere wenn er Zweifel daran hat, ob er zur Einsichtsgewährung berechtigt ist oder nicht. Umgekehrt wird die Einsicht verlangende Person in ihrem Begehren nicht alleine dadurch blockiert, dass der Verantwortliche nicht an die Aufsichtsbehörde gelangen möchte.

Die Aufsichtsbehörde entscheidet dabei ausschliesslich über die Frage der Entbindung vom Amts- oder Berufsgeheimnis, verpflichtet aber den Geheimnisträger nicht, die Einsicht zu gewähren. Sollte der Geheimnisträger trotz der Entbindung durch die Aufsichtsbehörde die Einsicht verweigern, beispielsweise weil seiner Ansicht nach die Einsicht verlangende Person nicht in faktischer Lebensgemeinschaft mit der verstorbenen Person gelebt hatte, handelt es sich hierbei um einen zivilrechtlichen Anspruch, der im Streitfall auf dem Prozessrechtsweg durchgesetzt werden kann bzw. muss, wenn es sich um einen privaten Verantwortlichen handelt.

147 Vgl. hierzu Mazan Stephan, Vorbemerkungen zu Art. 243-247 ZPO, in: Spühler Karl/Tenchio Luca/Infanger Dominik, Basler Kommentar, Schweizerische Zivilprozessordnung, 3. Aufl., Basel 2017.

148 BGE **123** IV 75, 77 E. 2b.

Abs. 3 Löschung

Gemäss Absatz 3 können die Erben oder ein allfälliger Willensvollstrecker verlangen, dass der Verantwortliche Daten des Erblassers löscht oder vernichtet. Dieser Anspruch besteht unabhängig von einer Persönlichkeitsverletzung bzw. einer widerrechtlichen Datenbearbeitung. Es handelt sich dabei um einen Spezialfall des Rechts auf Vergessen, wie es für Lebende in Artikel 28 E-DSG vorgesehen ist.

Bewusst wurde dieser Anspruch auf die Erben und den Willensvollstrecker beschränkt. Anders als noch in der Vernehmlassungsvorlage vorgesehen, können die Erben diesen Anspruch nur gemeinsam geltend machen. Diese Anpassung erfolgt im Hinblick auf die Vermeidung möglicher Konflikte zwischen den Erben in Bezug auf die Ausübung des Löschungsanspruchs; sind sich die Erben nicht einig, so kann eine Löschung der Daten des Erblassers grundsätzlich nicht in Betracht kommen. Gegenüber der Vernehmlassungsvorlage wurde ergänzt, dass auch ein allfälliger Willensvollstrecker diesen Anspruch geltend machen kann.

Die Löschung bzw. Vernichtung muss nach Buchstabe a verweigert werden, wenn der Erblasser sie zu Lebzeiten ausdrücklich untersagt hat. Hier soll dem Willen des Erblassers Rechnung getragen werden, der beispielsweise über das Schicksal persönlicher Archive nach seinem Tod verfügt hat.

Ebenfalls zu verweigern ist die Löschung oder Vernichtung, wenn ihr überwiegende Interessen des Erblassers, des Verantwortlichen oder von Dritten entgegenstehen (Buchstabe b). Hierzu kann grundsätzlich auf die obigen Ausführungen betreffend Absatz 1 Buchstabe b verwiesen werden. Entgegen den Befürchtungen verschiedener Vernehmlassungsteilnehmer ist es damit nicht möglich, dass die Erben einen Verantwortlichen dazu verpflichten könnten, belastendes Material für einen Prozess zu löschen. Als überwiegendes Interesse des Verantwortlichen können aber auch gesetzliche Pflichten gelten, denen dieser unterstellt ist und die der Löschung entgegenstehen.

Buchstabe c schliesst die Löschung oder Vernichtung aus, wenn ihr ein überwiegendes öffentliches Interesse entgegensteht. Sowohl private Verantwortliche als auch Bundesorgane können ein solches Interesse geltend machen. Solche überwiegenden öffentlichen Interessen können beispielsweise vorliegen bei Dokumenten, für die Ansprüche nach dem BGÖ geltend gemacht werden können. Zu denken ist aber auch an Aufbewahrungspflichten nach Massgabe des Bundesrechts oder des kantonalen Rechts.

Klagen zur Geltendmachung der Löschung nach Artikel 16 Absatz 3 E-DSG können gegenüber privaten Verantwortlichen gemäss Artikel 243 Absatz 2 Buchstabe d E-ZPO im vereinfachten Verfahren geltend gemacht werden.

9.1.4 Pflichten des Verantwortlichen und des Auftragsbearbeiters

Das 3. Kapitel fasst die Pflichten des Verantwortlichen und des Auftragsbearbeiters zusammen. Sie gelten unabhängig davon, ob es sich dabei um eine private Person oder ein Bundesorgan handelt.

Art. 17 Informationspflicht bei der Beschaffung von Personendaten

In Artikel 17 E-DSG wird neu die Informationspflicht bei der Beschaffung von Daten geregelt. Die Artikel 14, 18 und 18*a* DSG werden damit in einer Norm zusammengeführt. Dadurch werden Doppelspurigkeiten vermieden und es gilt eine einheitliche Regelung für die Datenbearbeitung durch Bundesorgane und private Verantwortliche. Die Bestimmung entspricht den Anforderungen von Artikel 7bis E-SEV 108 sowie Artikel 13 der Richtlinie (EU) 2016/680. Die Artikel 13 f. der Verordnung (EU) 2016/679 enthalten eine ähnliche Regelung.

Die Informationspflicht verbessert die Transparenz bei der Datenbearbeitung, die ein zentrales Ziel der Revision ist. Denn regelmässig kann die betroffene Person ohne entsprechende Informationen nicht erkennen, dass Daten über sie bearbeitet werden. Zugleich kann die betroffene Person ihre Rechte gemäss dem DSG nur wahrnehmen, wenn ihr eine Datenbearbeitung bekannt ist. Durch die verbesserte Transparenz bei der Datenbearbeitung werden daher auch die Rechte der betroffenen Person gestärkt, was ebenfalls ein zentrales Anliegen der Revision ist. Schliesslich dient die Informationspflicht der Sensibilisierung der Bevölkerung für den Datenschutz, die mit der Revision ebenso angestrebt wird.

Abs. 1 Grundsatz

Gemäss Absatz 1 muss der Verantwortliche die betroffene Person über die Beschaffung von Personendaten informieren. Dies gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

Der E-DSG legt nicht fest, auf welche Weise die Information erfolgen muss. Der Verantwortliche muss aber sicherstellen, dass die betroffene Person die Information tatsächlich zur Kenntnis nehmen kann. Sicherzustellen ist damit die Möglichkeit, sich in einfach zugänglicher Weise zu informieren, nicht aber, dass sich die betroffene Person im konkreten Fall wirklich informiert. Diese Möglichkeit, Informationen zur Kenntnis zu nehmen, hängt wesentlich davon ab, ob die Daten bei der betroffenen Person beschafft werden oder nicht.

So kann eine allgemeine Information genügen, wenn die Personendaten bei der betroffenen Person beschafft werden (zu allgemeinen Geschäftsbedingungen vgl. Art. 18 Abs. 1). Denkbar sind in diesem Fall eine Datenschutzerklärung auf einer Website, aber gegebenenfalls auch Symbole oder Piktogramme, soweit sie die nötigen Informationen wiedergeben. Wird eine allgemeine Form gewählt, muss die Information leicht zugänglich, vollständig und genügend sichtbar gemacht sein. Auch ein mehrstufiger Zugang ist möglich, der beispielsweise auf einer ersten Stufe eine Übersicht enthält, die auf einer zweiten Stufe Zugang zu detaillierten Informationen gibt. Nicht ausreichend ist hingegen, wenn einfach eine Kontaktperson angegeben wird. Die betroffene Person soll die Informationen erhalten, ohne dass sie zuerst danach fragen muss.

Werden die Daten hingegen nicht bei der betroffenen Person beschafft, muss der Verantwortliche prüfen, wie die Information erfolgen muss, damit die betroffene Person tatsächlich von ihr Kenntnis nehmen kann. Gegebenenfalls reicht es in diesem Fall nicht aus, lediglich Informationen zur Verfügung zu stellen, sondern die betroffene Person muss aktiv informiert werden, sei dies in einer geeigneten allge-

meinen Form oder durch individuelle Information. So wird beispielsweise eine Person, die nie Bücher kauft, kaum die Website eines Online-Buchändlers besuchen und dessen Datenschutzerklärung lesen. Dementsprechend wird sie aufgrund dieser allgemeinen Erklärung auch nicht erfahren, dass der Online-Buchhändler Daten über sie bearbeitet, weil sie gar nicht damit rechnet. Die Informationspflicht soll damit grundsätzlich auch verhindern, dass ohne Wissen der betroffenen Person Daten über sie bearbeitet werden; vorbehalten bleiben die Ausnahmen in Artikel 18.

Die Information ist zwar keinem Formerfordernis unterworfen, aber es ist insgesamt eine Form zu wählen, welche dem Zweck einer transparenten Datenbearbeitung gerecht wird. Aus Beweisgründen ist es zudem empfehlenswert, die Information zu dokumentieren oder schriftlich zu geben. Auch muss die Information verständlich abgefasst sein, sodass sie tatsächlich dem Zweck einer transparenten Datenbearbeitung dient.

Abs. 2 Mitzuteilende Informationen

Der Einleitungssatz von Absatz 2 legt den Grundsatz fest, an dem sich der Verantwortliche bei der Mitteilung von Informationen orientieren muss. Demnach muss er der betroffenen Person diejenigen Informationen mitteilen, die erforderlich sind, um ihre Rechte nach dem Gesetz geltend zu machen und eine transparente Datenbearbeitung zu gewährleisten. Die Buchstaben a–c konkretisieren diesen Grundsatz durch Mindestangaben, welche der betroffenen Person in jedem Fall mitgeteilt werden müssen. Dabei handelt es sich nach Buchstabe a um die Identität, d.h. den Namen, und die Kontaktdaten des Verantwortlichen und nach Buchstabe b den Bearbeitungszweck. Gegebenenfalls sind zudem nach Buchstabe c die Empfänger oder die Kategorien von Empfängern anzugeben, denen die Personendaten bekanntgegeben werden. Dabei besteht ein Wahlreicht auf Seiten des Verantwortlichen, ob er die Empfänger oder lediglich die Kategorien von Empfängern angeben möchte. Wie auch in der Europäischen Union (vgl. Art. 4 Ziff. 9 der Verordnung [EU] 2016/679) gehören auch Auftragsbearbeiter zu den Empfängern im Sinne der Bestimmung. Will der Verantwortliche deren Identität jedoch nicht offenlegen, kann er sich mit der Angabe der Kategorie begnügen. Der Beauftragte hätte bevorzugt, wenn darüber hinaus auch die Rechtsgrundlage der Bearbeitung mitgeteilt hätte werden müssen.

Durch die Kombination aus einer allgemeinen Vorschrift, welche die grundsätzlichen Anforderungen an die zu übermittelnden Informationen enthält, und spezifischen Mindestangaben lässt sich die Informationspflicht flexibel handhaben. Entsprechend der Art der bearbeiteten Daten, der Natur und dem Umfang der fraglichen Datenbearbeitung muss der Verantwortliche verstärkt informieren oder nicht. So kann es beispielswise auch nötig sein, über die Dauer der Bearbeitung, oder die Anonymisierung von Daten zu informieren. Diese Flexibilität ist erforderlich, weil das DSG auf eine Vielzahl unterschiedlicher Datenbearbeitungen anwendbar ist. Zugleich wird durch eine flexible Regelung sichergestellt, dass die Verantwortlichen keine unnötigen Informationen übermitteln müssen und die betroffenen Personen nur erforderliche Informationen erhalten. Ebenfalls erlaubt dies den Verantwortlichen, die Informationspflicht für ihre spezifische Branche in Verhaltenskodizes zu konkretisieren.

Abs. 3 Kategorien der Personendaten

Nur wenn die Daten nicht bei der betroffenen Person beschafft werden, muss der Verantwortliche nach Absatz 3 der betroffenen Person zudem mitteilen, welche Kategorien von Personendaten er bearbeitet. Diese Einschränkung ergibt sich aus der Annahme, dass der betroffenen Person zumindest die Kategorien von Daten oder sogar die Daten bekannt sein dürften, wenn diese bei ihr beschafft werden. Wenn die Daten nicht bei der betroffenen Person beschafft werden, hat diese keine Möglichkeit zu erfahren, welche Kategorien von Daten über sie bearbeitet werden, und muss daher entsprechend informiert werden.

Abs. 4 Bekanntgabe ins Ausland

Werden die Personendaten ins Ausland bekanntgegeben, muss der Verantwortliche die betroffene Person auch über den Staat informieren, in den die Daten gelangen. Falls dieser Staat keinen angemessenen Schutz gewährleistet und der Verantwortliche auf Garantien nach Artikel 13 Absatz 2 zurückgreift, muss er der betroffenen Person auch diese Garantien mitteilen. Dasselbe gilt, wenn die Bekanntgabe aufgrund einer Ausnahme nach Artikel 14 erfolgt.

Abs. 5 *Zeitpunkt der Information*

Werden die Daten bei der betroffenen Person beschafft, muss sie in diesem Zeitpunkt informiert werden. Dies ergibt sich aus Absatz 2.

Absatz 5 regelt den Zeitpunkt der Information, wenn die Daten nicht bei der betroffenen Person beschafft werden. Die Bestimmung legt dafür eine maximale Frist von einem Monat fest, innerhalb der die Information erfolgen muss. Satz 2 enthält eine kürzere Frist für den Fall, dass der Verantwortliche die Personendaten vor Ablauf dieser einmonatigen Frist an Empfänger bekanntgibt. Dann muss die betroffene Person spätestens zum Zeitpunkt der Bekanntgabe informiert werden.

Zusammenfassend gilt damit eine grundsätzliche Frist von einem Monat, nachdem der Verantwortliche die Daten erhalten hat. Diese Frist gilt unabhängig davon, wofür die Personendaten verwendet werden. Eine kürzere Frist gilt nur, wenn der Verantwortliche die Personendaten an Empfänger bekanntgibt.

Art. 18 Ausnahmen von der Informationspflicht und Einschränkungen

Artikel 18 E-DSG regelt, unter welchen Umständen die Informationspflicht gänzlich entfällt (Abs. 1 und 2), und wann die Information eingeschränkt werden kann, obschon grundsätzlich die Pflicht zur Information besteht (Abs. 3). Die beiden Konstellationen sind klar voneinander abzugrenzen. Die Vorschrift übernimmt dabei teilweise geltendes Recht (Art. 9, Art. 14 Abs. 4 und 5, sowie 18*b* DSG), das der Klarheit halber in einer Bestimmung zusammengeführt wird.

Abs. 1 Allgemeine Ausnahmen von der Informationspflicht

Absatz 1 legt einige Konstellationen fest, in denen die Informationspflicht gänzlich entfällt und der Verantwortliche die betroffene Person demnach gar nicht informieren muss.

Nach Buchstabe a ist der Verantwortliche von der Informationspflicht entbunden, wenn die betroffene Person bereits über die Informationen nach Artikel 17 verfügt. Davon ist in verschiedenen Fällen auszugehen. Zunächst ist es möglich, dass die betroffene Person zu einem früheren Zeitpunkt bereits informiert wurde und sich die Informationen, welche übermittelt werden müssen, in der Zwischenzeit nicht geändert haben. Grundsätzlich ist ebenfalls davon auszugehen, dass die betroffene Person die Informationen bereits erhalten hat, um in eine Datenbearbeitung einzuwilligen. Denn eine gültige Einwilligung ist nur möglich, wenn die betroffene Person angemessen informiert wurde. Die dafür notwendigen Informationen entsprechen denjenigen, die nach Artikel 17 mitzuteilen sind oder gehen sogar darüber hinaus. Regelmässig erfolgt die Einwilligung mittels Allgemeiner Geschäftsbedingungen (AGB). Diese können damit grundsätzlich ebenfalls dazu dienen, die betroffene Person zu informieren, soweit sie die erforderlichen Informationen enthalten. Wenn die betroffene Person die Daten selbst, ohne Dazutun des Verantwortlichen zugänglich gemacht hat, gilt sie grundsätzlich ebenfalls als über die Datenbeschaffung informiert (z. B. Zustellung von Bewerbungsunterlagen).

Nach Buchstabe b entfällt die Informationspflicht, wenn die Bearbeitung im Gesetz vorgesehen ist. Darunter können sowohl Bearbeitungen durch die Bundesorgane als auch durch die Privaten fallen. Bundesorgane können Daten ohnehin nur bearbeiten, wenn eine gesetzliche Grundlage besteht. Dieser lassen sich regelmässig auch die entsprechenden Informationen entnehmen. Dasselbe gilt für Private, die durch das Gesetz zur Bearbeitung bestimmter Daten verpflichtet werden, wie dies z. B. betreffend die Geldwäscherei der Fall ist.

Nach Buchstabe c ist der private Verantwortliche von der Informationspflicht entbunden, wenn er einer gesetzlichen Geheimhaltungspflicht untersteht. Damit wird ein möglicher Normkonflikt dahingehend geregelt, dass grundsätzlich die Geheimhaltungspflicht der Informationspflicht vorgeht.

Nach Buchstabe d entfällt die Informationspflicht schliesslich, wenn die Voraussetzungen von Artikel 25 erfüllt sind. Dieser Artikel regelt die Einschränkung des Auskunftsrechts in Bezug auf periodisch erscheinende Medien. Ein analoges Medienprivileg ist aus denselben Gründen auch für die Informationspflicht erforderlich, um der besonderen Funktion der Medien ausreichend gerecht zu werden.[149]

Abs. 2 Spezifische Einschränkung

Absatz 2 sieht eine spezifische Einschränkung der Informationspflicht für Fälle vor, in denen Daten nicht bei der betroffenen Person beschafft werden. Die Informationspflicht ihr gegenüber entfällt, wenn die Information nicht möglich ist (Bst. a) oder unverhältnismässigen Aufwand erfordert (Bst. b).

Die Information ist nicht möglich, wenn die betroffene Person gar nicht identifiziert werden kann, z. B. weil es sich um das Foto eines Unbekannten handelt. Dabei reicht allerdings nicht aus, dass lediglich vermutet wird, die Identifikation sei unmöglich. Vielmehr sind Nachforschungen in einem verhältnismässigen Umfang erforderlich.

149 Vgl. hierzu Weber Rolf H., Medien im Spannungsfeld von Informationsauftrag und Datenschutz, Jusletter 8. Mai 2017.

Der Aufwand für die Information der betroffenen Person ist unverhältnismässig, wenn der zu betreibende Aufwand im Verhältnis zum Informationszugewinn der betroffenen Person sachlich nicht gerechtfertigt erscheint. Zu berücksichtigen ist insbesondere, ob eine sehr grosse Anzahl von Personen betroffen sind. So kann die Information beispielsweise mit einem unverhältnismässigen Aufwand verbunden sein, wenn Personendaten ausschliesslich zu Archivzwecken im öffentlichen Interesse bearbeitet werden. Es wäre regelmässig mit einem extrem hohen Aufwand verbunden, sämtliche betroffenen Personen zu informieren, und deren Interesse an der Information dürfte sich oft in Grenzen halten, z. B. weil die fraglichen Daten sehr alt sind.

Diese Ausnahme ist eng auszulegen. Der Verantwortliche darf sich nicht mit der Vermutung begnügen, die Information sei unmöglich oder nur mit unverhältnismässigem Aufwand zu bewerkstelligen. Vielmehr hat er grundsätzlich sämtliche Vorkehren zu treffen, die unter den gegebenen Umständen von ihm erwartet werden können, um der Informationspflicht nachzukommen. Erst wenn diese erfolglos bleiben, darf der Verantwortliche davon ausgehen, die Information sei unmöglich.

Abs. 3 Einschränkung der Information

Absatz 3 legt fest, unter welchen Voraussetzungen der Verantwortliche auf die Mitteilung von Informationen verzichten, diese einschränken oder aufschieben kann. Im Gegensatz zu den Absätzen 1 und 2 erfasst Absatz 3 damit Konstellationen, in denen eine Interessenabwägung erfolgt. Teilweise wird danach unterschieden, ob es sich beim Verantwortlichen um ein Bundesorgan oder einen Privaten handelt. Aufgrund der Interessenabwägung hat der Verantwortliche die Information entsprechend auszugestalten, d. h. je nach dem muss er deren Mitteilung einschränken, aufschieben oder ganz darauf verzichten. Die Aufzählung der verschiedenen Ausnahmen ist abschliessend und die Bestimmung ist prinzipiell restriktiv auszulegen. Die Information sollte nur soweit beschränkt werden, als dies wirklich unerlässlich ist. Dabei müssen der Grund für die Beschränkung der Informationspflicht und das Interesse an einer transparenten Datenbearbeitung zueinander in Beziehung gesetzt werden. Grundsätzlich sollte die für die betroffene Person günstigste Lösung gewählt werden, welche eine transparente Datenbearbeitung unter den gegebenen Umständen soweit als möglich gewährleistet.

Bst. a

Nach Buchstabe a kann jeder Verantwortliche die Mitteilung der Informationen einschränken, aufschieben oder darauf verzichten, wenn dies wegen überwiegender Interessen Dritter erforderlich ist. Dabei stehen Konstellationen im Vordergrund, bei denen die betroffene Person durch die Information über die Datenbearbeitung auch Informationen über Drittpersonen erhält und dadurch die Interessen dieser Drittpersonen beeinträchtigt werden können.

Bst. b

Gemäss Buchstabe b kann jeder Verantwortliche die Mitteilung der Informationen einschränken, aufschieben oder darauf verzichten, wenn die Information den Zweck der Datenbearbeitung vereitelt. Diese Ausnahme ist eng auszulegen. Der Verant-

wortliche kann sich nur darauf berufen, wenn die Information der betroffenen Person völlig ausschliesst, zugleich den Zweck der Bearbeitung zu verwirklichen. Werden mit einer Bearbeitung mehrere Zwecke verfolgt, ist der zentrale Zweck massgebend. Dabei muss es sich um einen Zweck handeln, dem eine erhebliche Bedeutung zukommt, die eine solch weitgehende Einschränkung der Informationspflicht rechtfertigt. Zu denken ist beispielsweise an investigativen Journalismus, der nicht unter die Ausnahme in Artikel 18 Absatz 1 Buchstabe d E-DSG fällt. So könnte eine Journalistin oder ein Journalist, die oder der für einen Dokumentarfilm an der Aufdeckung eines politischen Skandals arbeitet, durch die Informationspflicht daran gehindert werden, den in Frage stehenden Sachverhalt ungestört zu ermitteln. An einer solchen Tätigkeit besteht auch ein erhebliches öffentliches Interesse, das eine weitgehende Einschränkung der Informationspflicht rechtfertigt. Ebenfalls denkbar ist, dass in unmittelbarem Zusammenhang mit einem Verfahren mit hohem Streitwert Daten bearbeitet werden, die erst im Laufe des Prozesses eingesetzt werden sollen. Auch in diesem Fall würde durch die frühzeitige Preisgabe der Daten deren Bearbeitunszweck vollumfänglich vereitelt. Zudem handelt es sich hier um eine Bearbeitung, welche sowohl für den Verantwortlichen als auch für die betroffene Person einen Einzelfall darstellt, weil bei beiden davon auszugehen ist, dass sie nicht alltäglich in solche Gerichtsverfahren involviert sind. In beiden Beispielen besteht ein gewichtiges Interesse an der Datenbearbeitung und die Gefahr, dass der Bearbeitungszweck durch die Informationspflicht gänzlich vereitelt wird, ist unmittelbar und konkret. Schliesslich ist es in beiden Fällen so, dass die betroffene Person spätestens im Zeitpunkt der Publikation der fraglichen Daten bzw. der Verwendung im Gerichtsprozess von der Datenbearbeitung erfährt.

Entsprechend der systematischen Einordnung in Absatz 3 bleibt die Informationspflicht grundsätzlich bestehen. Der Verantwortliche darf die Information lediglich so weit einschränken, aufschieben oder darauf verzichten, als sie unmittelbar den Zweck der Bearbeitung vereitelt. Dabei muss der Verantwortliche diejenige Massnahme treffen, welche aus Sicht der betroffenen Person die mildeste ist und ihren Anspruch auf transparente Datenbearbeitung so wenig einschränkt, wie im Hinblick auf die Gründe für die Einschränkung der Information möglich ist.

Abzugrenzen ist die Ausnahme nach Buchstabe b schliesschlich von derjenigen nach Buchstabe c. Buchstabe b ist eng auszulegen und kann nur dort zur Anwendung kommen, wo die Information der betroffenen Person den Bearbeitungszweck gänzlich vereiteln würde. Hingegen kann sich der Verantwortliche nicht auf Buchstabe b berufen, wenn es für ihn lediglich angenehmer oder praktischer wäre, auf die Information zu verzichten. Ebenfalls könnte sich ein Verantwortlicher nicht systematisch, für seine gesamte Bearbeitungstätigkeit auf die Ausnahme berufen. Schliesslich fallen auch rein wirtschaftliche Interessen (z. B. Verwendung der Daten zu Werbezwecken) grundsätzlich nicht in den Anwendungsbereich des Buchstaben b. Gegebenenfalls können solche weniger gewichtige Interessen des Verantwortlichen indes unter Buchstabe c fallen.

Bst. c

Der private Verantwortliche kann nach Absatz 3, Buchstabe c die Mitteilung von Informationen einschränken, aufschieben oder darauf verzichten, wenn eigene überwiegende Interessen es erfordern und er die Daten nicht Dritten bekannt gibt. Ein solches überwiegendes Interesse ist nicht leichthin anzunehmen. Das Interesse der betroffenen Person, über eine bestimmte Datenbearbeitung informiert zu werden, um ihre Rechte geltend machen zu können, ist sorgfältig abzuwägen gegenüber allfälligen Interessen des Verantwortlichen. Von Bedeutung kann dabei sein, welche Art von Daten auf welche Weise bearbeitet werden, wie gross die Gefahr einer Persönlichkeitsverletzung ist, welchem Zweck die Datenbearbeitung dient und in welchem Umfang die Information der betroffenen Person diesem Zweck entgegenstehen kann, sowie welche Bedeutung diesem Zweck mit Blick auf die Tätigkeit des Verantwortlichen zukommt.

Bst. d

Ein Bundesorgan kann nach Absatz 3, Buchstabe d die Mitteilung einschränken, aufschieben oder darauf verzichten, wenn es wegen überwiegender öffentlicher Interessen erforderlich ist (Ziff. 1). Als überwiegendes öffentliches Interesse gilt insbesondere die innere oder äussere Sicherheit der Eidgenossenschaft. Der Begriff der äusseren Sicherheit schliesst nebst der Beachtung von völkerrechtlichen Verpflichtungen auch die Pflege guter Beziehungen zum Ausland ein. Das Bundesorgan kann die Mitteilung ebenfalls einschränken, aufschieben oder darauf verzichten, wenn dadurch Ermittlungen, Untersuchungen oder behördliche oder gerichtliche Verfahren gefährdet werden können (Ziff. 2). Auf diese Weise soll sichergestellt werden, dass nicht über den Umweg des DSG die Vorschriften zum rechtlichen Gehör etc. nach den Verfahrensgesetzen umgangen werden können.

Art. 19 Informationspflicht bei einer automatisierten Einzelentscheidung

Nach Artikel 19 E-DSG besteht eine Informationspflicht bei einer automatisierten Einzelentscheidung. Dies entspricht den Anforderungen von Artikel 8 Buchstabe a E-SEV 108 sowie Artikel 11 der Richtlinie (EU) 2016/680. Artikel 22 der Verordnung (EU) 2016/679 enthält eine ähnliche Bestimmung. Die Einführung dieses neuen Begriffs erfolgt, weil aufgrund der technologischen Entwicklung solche Entscheidungen immer häufiger auftreten werden.

Abs. 1 Information

Nach Absatz 1 muss der Verantwortliche die betroffene Person informieren über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung, einschliesslich Profiling, beruht und für die betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt.

Der Bundesrat wird in der Verordnung falls erforderlich präzisieren, wann eine Entscheidung vorliegt, die ausschliesslich auf einer automatisierten Bearbeitung beruht. Dies ist der Fall, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat. Das heisst, die inhaltliche Beurteilung des Sachverhalts, auf dem die Entscheidung beruht, erfolgte ohne

Dazutun einer natürlichen Person. Darüber hinaus wird auch der Entscheid, der auf der Basis dieser Sachverhaltsbeurteilung ergeht, nicht von einer natürlichen Person getroffen. Eine automatisierte Einzelentscheidung kann selbst dann vorliegen, wenn sie anschliessend durch eine natürliche Person mitgeteilt wird, falls diese die automatisch gefällte Entscheidung nicht mehr beeinflussen kann. Massgebend ist somit, inwieweit eine natürliche Person eine inhaltliche Prüfung vornehmen und darauf aufbauend die endgültige Entscheidung fällen kann. Erforderlich ist allerdings, dass die Entscheidung eine gewisse Komplexität aufweist. Reine Wenn-Dann-Entscheidungen sind vom Begriff nicht erfasst, wie dies z. B. bei einem Bancomatbezug der Fall ist (angefragter Geldbetrag wird ausgegeben, wenn Kontodeckung genügend).

Die betroffene Person muss nicht über jede automatisierte Einzelentscheidung informiert werden. Vielmehr ist dies nur erforderlich, wenn die Entscheidung mit einer Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt. Die Entscheidung ist mit einer Rechtsfolge verbunden, wenn sie unmittelbare, rechtlich vorgesehene Konsequenzen für die betroffene Person nach sich zieht. Dies ist im privatrechtlichen Bereich namentlich bei Abschluss eines Vertrags oder dessen Kündigung der Fall. Dabei ist eine differenzierte Betrachtung nötig. So hat der Abschluss eines Versicherungsvertrags eine Rechtsfolge für die betroffene Person. Wird hingegen der betroffenen Person anschliessend in regelmässigen Abständen eine Prämienrechnung zugestellt, ist nicht jede einzelne Prämienrechnung für sich eine weitere Einzelentscheidung mit Rechtsfolge, weil sich die Rechnungsstellung aus dem Vertragsabschluss ergibt. Nicht mit einer Rechtsfolge verbunden ist ebenfalls, wenn mit der betroffenen Person kein Vertrag zustande kommt. Im öffentlichrechtlichen Bereich liegt eine Rechtsfolge insbesondere vor, wenn Verfügungen aufgrund einer automatisierten Einzelentscheidung ergehen, so z. B. eine automatisierte Steuerveranlagung.

Eine erhebliche Beeinträchtigung der betroffenen Person ist anzunehmen, wenn diese auf nachhaltige Weise z. B. in ihren wirtschaftlichen oder persönlichen Belangen eingeschränkt ist. Eine blosse Belästigung reicht dafür nicht aus. Massgebend sind die konkreten Umstände des Einzelfalls. Zu berücksichtigen ist insbesondere, wie bedeutsam das fragliche Gut für die betroffene Person ist, wie dauerhaft sich die Entscheidung auswirkt und ob allenfalls Alternativen zugänglich sind. Je nach den konkreten Auswirkungen kann ein nicht abgeschlossener Vertrag daher eine erhebliche Beeinträchtigung darstellen oder nicht. Eine erhebliche Beeinträchtigung kann auch vorliegen, wenn medizinische Leistungen auf der Basis automatisierter Entscheidungen zugeteilt werden.

Der Verantwortliche muss die betroffene Person auch über ein Profiling informieren, wenn dieses zu einer Entscheidung führt, die für die betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt. So ist beispielsweise möglich, dass die betroffene Person ausschliesslich aufgrund eines negativen Kreditscorings keinen Kreditkartenvertrag abschliessen kann. Insbesondere dieses Beispiel zeigt auch die Problematik automatisierter Einzelentscheidungen auf. So kann ein negatives Kreditscoring durchaus die tatsächlichen finanziellen Verhältnisse einer Person wiederspiegeln. Ebenso ist aber möglich, dass dieses Krediscoring auf falschen oder veralteten Daten beruht, welche den tatsächlichen finanziellen

Verhältnissen der betroffenen Person völlig widersprechen. Die automatisierte Entscheidung führt in diesem Fall für sie zu einer ungerechtfertigen Beeinträchtigung.

Abs. 2 Darstellung des Standpunktes

Der Verantwortliche muss der betroffenen Person nach Absatz 2 die Möglichkeit geben, ihren Standpunkt darzulegen, wenn sie dies verlangt. Sie soll insbesondere die Gelegenheit erhalten, ihre Ansicht zum Ergebnis der Entscheidung zu äussern und gegebenenfalls nachzufragen, wie die Entscheidung zustande gekommen ist. Dadurch soll unter anderem verhindert werden, dass die Datenbearbeitung auf unvollständigen, veralteten oder unzutreffenden Daten beruht. Dies liegt auch im Interesse des Verantwortlichen, weil unzutreffende automatisierte Einzelentscheidungen auch für ihn negative Konsequenzen nach sich ziehen können, beispielsweise indem ein Vertrag mit einer Person nicht abgeschlossen wird, weil sie zu Unrecht als nicht kreditwürdig eingestuft wurde. Die Vertragsfreiheit bleibt dadurch unberührt.

Das Gesetz legt nicht fest, wann die betroffene Person informiert werden muss und wann sie Gelegenheit erhält, ihren Standpunkt darzulegen. Dementsprechend kann dies vor oder nach der Entscheidung erfolgen. Somit ist die Information und Anhörung beispielsweise auch möglich, indem der betroffenen Person eine automatisiert erfolgte Verfügung zugestellt wird, die entsprechend gekennzeichnet ist, und sie anschliessend die Möglichkeit erhält, sich im Rahmen des rechtlichen Gehörs oder durch Einlegen eines Rechtsmittels zu äussern. Dieses darf für die betroffene Person allerdings nicht mit so hohen Kosten (z. B. Verfahrenskosten) verbunden sein, dass sie deswegen davon absieht.

Abs. 3 Ausnahmen

Die Pflicht zur Information und Anhörung entfällt gemäss Absatz 3, wenn die automatisierte Einzelentscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen steht, soweit ihrem Begehren stattgegeben wird (Bst. a). In einem solchen Fall ist davon auszugehen, dass die betroffene Person kein Interesse mehr an der Information hat. Dem Begehren der betroffenen Person wird stattgegeben, wenn der Vertragsabschluss genau zu den Konditionen erfolgt, wie sie z. B. in der Offerte dargestellt wurden oder wie sie die betroffene Person verlangt hatte. So wird beispielsweise ihrem Begehren stattgegeben, wenn ein Leasingvertrag zum im Angebot aufgeführten Zins abgeschlossen wird; anderes gilt, wenn der Leasingvertrag zwar abgeschlossen wird, aber aufgrund eines schlechten Kreditratings der betroffenen Person zu einem weniger vorteilhaften Zins als im Angebot genannt. Abzustellen ist dabei darauf, ob gesamthaft den Begehren der betroffenen Person stattgegeben wurde. Es reicht nicht aus, wenn dies nur in Bezug auf einzelne Elemente der Fall ist.

Die Pflicht zur Information und Anhörung entfällt ebenfalls, wenn die betroffene Person ausdrücklich eingewilligt hat, dass eine Entscheidung automatisiert erfolgt (Bst. b). Diese Ausnahme ist folgerichtig, weil die betroffene Person bereits informiert werden muss, um rechtsgültig einzuwilligen.

Abs. 4 Einzelentscheidungen durch Bundesorgane

Absatz 4 betrifft automatisierte Einzelentscheidungen, die durch ein Bundesorgan ergehen. Dabei handelt es sich grundsätzlich um Verfügungen. Gemäss Absatz 4 muss das Bundesorgan diese als automatisierte Einzelentscheidungen kennzeichnen, damit die betroffene Person erkennen kann, dass der Entscheid nicht durch eine natürliche Person bearbeitet wurde. Gegen Verfügungen steht der betroffenen Person grundsätzlich ein Rechtsmittel zur Verfügung, in dem die betroffene Person ihren Standpunkt darlegen kann und eine natürliche Person den Entscheid überprüft. Die Rechte nach Artikel 19 Absatz 2 E-DSG werden mit anderen Worten bereits durch den Rechtsweg gewährleistet. Deswegen sieht Satz 2 der Bestimmung vor, dass Absatz 2 von Artikel 19 nicht gilt, wenn die betroffene Person ein Rechtsmittel ergreifen kann.

Art. 20 Datenschutz-Folgenabschätzung

Artikel 20 E-DSG führt neu die Pflicht zum Erstellen einer Datenschutz-Folgenabschätzung ein. Diese Bestimmung verwirklicht die Anforderungen von Artikel 8bis Absatz 2 E-SEV 108 sowie von Artikel 27 f. der Richtlinie (EU) 2016/680. Die Artikel 35 f. der Verordnung (EU) 2016/679 enthalten ähnliche Vorschriften.

Begriff und Funktion der Datenschutz-Folgenabschätzung ergeben sich aus Artikel 20 Absatz 3. Eine Datenschutz-Folgenabschätzung ist ein Instrument, um Risiken zu erkennen und zu bewerten, welche für die betroffene Person durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Auf der Basis dieser Abschätzung sollen gegebenenfalls angemessene Massnahmen definiert werden, um diese Risiken für die betroffene Person zu bewältigen. Eine solche Abschätzung ist daher auch für den Verantwortlichen vorteilhaft, weil sie ihm erlaubt, allfällige datenschutzrechtliche Probleme präventiv anzugehen und dadurch nicht zuletzt Kosten zu sparen.

Die Bundesorgane sind bereits heute verpflichtet, dem Datenschutzverantwortlichen oder, falls kein solcher besteht, dem Beauftragten Projekte zur automatisierten Bearbeitung von Daten zu melden (Art. 20 Abs. 2 VDSG). Das Vorgehen gemäss der Projektmanagementmethode Hermes dürfte den Anforderungen einer Datenschutz-Folgenabschätzung weitgehend entsprechen.

Abs. 1 und 2 Gründe für die Datenschutz-Folgenabschätzung

Nach Absatz 1 muss der Verantwortliche eine Datenschutz-Folgenabschätzung durchführen, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.[150] Die vorliegende Bestimmung gilt sowohl für private Verantwortliche als auch für Bundesorgane, weshalb nicht nur von einem Risiko für die Persönlichkeit der betroffenen Person, sondern auch für deren Grundrechte die Rede ist. Der Verantwortliche ist demnach verpflichtet, eine Prognose darüber zu machen, welche

150 Vgl. hierzu auch Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, Working Paper der Article 29 Data Protection Working Party vom 4. April 2017, S. 7 ff. insbes.

Folgen eine geplante Datenbearbeitung für die betroffene Person hat. Massgebend ist hierfür insbesondere, auf welche Weise und in welchem Umfang sich eine Bearbeitung auf die Persönlichkeit oder die Grundrechte der betroffenen Person auswirkt.

Bei der Konkretisierung dieses Risikos stehen das Recht auf informationelle Selbstbestimmung sowie das Recht auf Privatsphäre im Vordergrund. Diese schützen sowohl die Autonomie des Einzelnen als auch dessen Würde und Identität[151]. In Bezug auf Daten bedeutet Autonomie insbesondere, selbständig über die persönlichen Daten verfügen zu können und nicht annehmen zu müssen, dass diese sich in unbekannter Menge in den Händen einer Vielzahl von Drittpersonen befinden, welche darüber unbeschränkt verfügen können. Denn Daten sind eng mit der Identität einer Person verbunden. Wer Daten über eine Person hat und sie miteinander in Verbindung bringt, kann ein sehr intimes und umfassendes Bild einer Person erhalten, welches sie freiwillig vielleicht lediglich besonders nahestehenden Personen offenbaren würde. Dies ist nicht nur in Bezug auf die Verfügungsfreiheit problematisch. Vielmehr können Informationen über eine andere Person deren Beziehungen zur Umwelt vielfältig beeinflussen, gegebenenfalls ohne dass die betroffene Person die Gründe kennt (z. B. Stigmatisierung wegen einer Krankheit, Einschränkungen bei Vertragsabschlüssen wegen einer Bonitätseinschätzung etc.). Die betroffene Person kann sich auch dazu gezwungen fühlen, ihr Verhalten zu ändern, beispielsweise weil sie weiss, dass ihr Verhalten überwacht wird. Schliesslich können solche Informationen auch zu Missbrauch einladen, der die Würde des Einzelnen empfindlich treffen kann.

Zur Evaluation des Risikos sind die informationelle Selbstbestimmung und das Recht auf Privatsphäre in Beziehung zu setzen zur fraglichen Datenbearbeitung. Die Bearbeitung muss mit anderen Worten im Hinblick auf die Selbstbestimmung, die Identität und die Würde einer betroffenen Person betrachtet werden. Von einem hohen Risiko ist grundsätzlich auszugehen, wenn die spezifischen Eigenschaften der geplanten Datenbearbeitung darauf schliessen lassen, dass die Verfügungsfreiheit der betroffenen Person über ihre Daten in hohem Masse eingeschränkt wird oder werden kann. Das hohe Risiko kann sich beispielsweise ergeben aus der Art der bearbeiteten Daten bzw. deren Inhalt (z. B. besonders schützenswerte Daten), der Art und dem Zweck der Datenbearbeitung (z. B. Profiling), der Menge an bearbeiteten Daten, der Übermittlung in Drittstaaten (z. B. wenn die ausländische Gesetzgebung keinen angemessenen Schutz gewährleistet) oder wenn eine grosse oder gar unbegrenzte Anzahl Personen auf die Daten zugreifen können.

Absatz 2 konkretisiert dies weiter und hält fest, dass sich das hohe Risiko aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ergibt. Je umfangreicher die Bearbeitung, je sensibler die bearbeiteten Daten, je umfassender der Bearbeitungszweck, umso eher ist ein hohes Risiko anzunehmen. Beispielhaft zählt die Bestimmung zwei Fälle auf, in denen ein hohes Risiko vorliegt. Nach Buchstabe a liegt ein solches vor, wenn in umfangreicher Form besonders schützenswerte Personendaten bearbeitet werden, wie dies beispielsweise bei medizinischen Forschungsprojekten der Fall sein kann. Nach Buchstabe b besteht bei einem

151 Vgl. hierzu Diggelmann Oliver, in: Waldmann/Belser/Epiney (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015, Art. 13 BV N 7.

Profiling ebenfalls ein hohes Risiko. Dasselbe kann gelten im Falle von Entscheidungen, die ausschliesslich auf einer automatisierten Bearbeitung, einschliesslich Profiling, beruhen und für die betroffene Person mit einer Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen. Solche Entscheidungen können gegebenenfalls für die betroffene Person mit erheblichen Folgen verbunden sein. In solchen Fällen ist ebenfalls eine Datenschutz-Folgenabschätzung erforderlich. Nach Buchstabe c besteht schliesslich ein hohes Risiko, wenn systematisch umfangreiche öffentliche Bereiche überwacht werden. Zu denken ist beispielsweise an die Überwachung einer Bahnhofshalle.

Satz 2 von Absatz 1 erlaubt es dem Verantwortlichen, eine gemeinsame Abschätzung zu erstellen, wenn er mehrere ähnliche Bearbeitungsvorgänge plant. Gemeint sind damit insbesondere Bearbeitungsvorgänge, die einen übergreifenden gemeinsamen Zweck haben. Dementsprechend müssen nicht einzelne Bearbeitungsschritte einer Bearbeitungsplattform separat untersucht werden, sondern die Datenschutz-Folgenabschätzung kann die gesamte Bearbeitungsplattform erfassen.

Abs. 3 Inhalt der Datenschutz-Folgenabschätzung

Nach Absatz 3 muss in der Datenschutz-Folgenabschätzung zunächst die geplante Bearbeitung dargelegt werden. So müssen beispielsweise die verschiedenen Bearbeitungsvorgänge (z. B. die verwendete Technologie), der Zweck der Bearbeitung oder die Aufbewahrungsdauer aufgeführt werden. Im Weiteren muss gemäss Absatz 3 aufgezeigt werden, welche Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person die fraglichen Bearbeitungsvorgänge mit sich bringen können. Es handelt sich hier um eine Vertiefung der Risikobewertung, die bereits im Hinblick auf die Notwendigkeit einer Datenschutz-Folgenabschätzung vorzunehmen ist. So ist darzustellen, in welcher Hinsicht von der fraglichen Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person ausgeht und wie dieses Risiko zu bewerten ist. Schliesslich muss die Datenschutz-Folgenabschätzung nach Absatz 3 erläutern, mit welchen Massnahmen diese Risiken bewältigt werden sollen. Massgebend dafür sind insbesondere die Grundsätze nach Artikel 5 E-DSG, aber auch die Pflicht zum Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen (privacy by design/by default; Art. 6 E-DSG) können relevant sein. Bei diesen Massnahmen darf auch eine Abwägung zwischen den Interessen der betroffenen Person und denjenigen des Verantwortlichen erfolgen. Diese Interessenabwägung ist in der Datenschutz-Folgenabschätzung ebenfalls aufzuführen und entsprechend zu begründen.

Abs. 4 Ausnahmen für gesetzliche Pflichten

Nach Absatz 4 müssen private Verantwortliche, die Daten in Erfüllung einer gesetzlichen Pflicht bearbeiten, keine Datenschutz-Folgenabschätzung erstellen. Dabei ist beispielsweise an die Bearbeitung von Daten zur Bekämpfung von Terrorismus oder Geldwäscherei zu denken. Werden Daten aufgrund einer gesetzlichen Verpflichtung lediglich für solche Zwecke bearbeitet, ist davon auszugehen, dass der Gesetzgeber allfällige Risiken für die betroffene Person im Vergleich zum Bearbeitungszweck abgewogen und gegebenenfalls entsprechende Vorschriften erlassen hat.

Nicht erfasst von Absatz 4 sind hingegen Bearbeitungen von Privaten, die nicht ausschliesslich zur Erfüllung einer gesetzlichen Pflicht erfolgen. Hierfür muss eine Datenschutz-Folgenabschätzung erstellt werden.

Abs. 5 Ausnahmen

Private Verantwortliche können von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn sie sich einer Zertifizierung nach Artikel 12 unterzogen haben. Die Zertifizierung muss sich auf die fragliche Bearbeitung einschliessen, die mittels der Datenschutz-Folgenabschätzung zu prüfen wäre. Der Beauftragte hätte bevorzugt, wenn sich die Ausnahme lediglich auf die Zertifizierung beschränken würde.

Darüber hinaus können sie davon absehen, wenn sie einen Verhaltenskodex einhalten, der die Voraussetzungen von Absatz 5 Buchstaben a–c erfüllt. Es handelt sich dabei um einen Verhaltenskodex nach Artikel 10. Dieser muss auf einer Datenschutz-Folgenabschätzung beruhen, in der die fragliche Bearbeitung untersucht wurde (Bst. a). Der Verhaltenskodex muss Massnahmen zum Schutz der Persönlichkeit oder der Grundrechte der betroffenen Person vorsehen (Bst. b). Darüber hinaus muss der Verhaltenskodex dem Beauftragten vorgelegt worden sein (Bst. c). So ist beispielsweise denkbar, dass eine Standesorganisation für Anwälte eine Plattform zur Verwaltung von Klientendaten entwickeln lässt, hierfür eine Datenschutz-Folgenabschätzung vornimmt und aufgrund deren Ergebnis einen Verhaltenskodex entwickelt. Hält nun ein privater Verantwortlicher diesen Kodex ein, wenn er die Plattform verwendet, ist er von der Erstellung einer Datenschutz-Folgenabschätzung entbunden.

Der Beauftragte hätte es bevorzugt, wenn diese Ausnahme auf den Fall der Zertifizierung begrenzt worden wäre.

Art. 21 Konsultation des Beauftragten

Anders als in der Vernehmlassungsvorlage wird die Mitteilung des Ergebnisses einer Datenschutz-Folgenabschätzung an den Beauftragten im E-DSG in einer separaten Bestimmung geregelt.

Abs. 1 Konsultationspflicht

Nach Absatz 1 muss der Verantwortliche vorgängig die Stellungnahme des Beauftragten einholen, wenn sich aus der Datenschutz-Folgenabschätzung ergibt, dass die geplante Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hätte, wenn der Verantwortliche keine Massnahmen träfe. Diese Konsultation wird durch den E-SEV 108 nicht vorgeschrieben, aber sie entspricht den europäischen Regelungen (Art. 28 der Richtlinie [EU] 2016/680 und Art. 36 der Verordnung [EU] 2016/679).[152] Sie wird namentlich in den E-DSG aufgenommen, weil sie dem Beauftragten erlaubt, präventiv und beratend tätig zu sein. Dies ist nicht zuletzt auch für den Verantwortlichen effizienter, da mögliche

[152] Vgl. auch den Erwägungsgrund 94 der Verordnung (EU) 2016/679.

datenschutzrechtliche Schwierigkeiten bereits in einem frühen Stadium der Datenbearbeitung behoben werden können.

Abs. 2 und 3 Einwände des Beauftragten

Gemäss Absatz 2 hat der Beauftragte zwei Monate Zeit, um dem Verantwortlichen seine Einwände gegen die geplante Bearbeitung mitzuteilen. In besonders komplexen Fällen kann diese Frist um einen Monat verlängert werden. Erhält der Verantwortliche innerhalb der Zweimonatsfrist keine Nachricht vom Beauftragten, kann er grundsätzlich davon ausgehen, dass der Beauftragte keine Einwände gegen die vorgeschlagenen Massnahmen hat.

Nachdem er über eine Datenschutz-Folgenabschätzung benachrichtigt worden ist, überprüft der Beauftragte, ob die vorgeschlagenen Massnahmen zum Schutz der Grundrechte und der Persönlichkeit der betroffenen Person ausreichend sind. Kommt er zum Schluss, dass die geplante Bearbeitung in der vorgeschlagenen Form gegen die Datenschutzvorschriften verstossen würde, schlägt er dem Verantwortlichen geeignete Massnahmen vor, um die festgestellten Risiken einzudämmen.

Dem Datenschutzbeauftragten bleibt es indes unbenommen, zu einem späteren Zeitpunkt eine Untersuchung zu eröffnen, wenn die Voraussetzungen nach Artikel 43 E-DSG erfüllt sind. Dies kann insbesondere der Fall sein, wenn im Rahmen der Datenschutz-Folgenabschätzung die Risiken nicht korrekt eingeschätzt wurden und sich dementsprechend auch die fraglichen Massnahmen nicht als zielgenau oder als nicht ausreichend erweisen.

Abs. 4 Konsultation der Datenschutzberaterin oder des Datenschutzberaters

Der private Verantwortliche kann von der Konsultation des Beauftragten absehen, wenn er einen Datenschutzberater nach Artikel 9 E-DSG eingesetzt und diesen in Bezug auf die Datenschutz-Folgenabschätzung konsultiert hat. Der Datenschutzberater muss sich tatsächlich mit der Datenschutz-Folgenabschätzung auseinandergesetzt haben. Das heisst, es reicht für die Privilegierung nicht aus, dass der Verantwortliche lediglich einen Datenschutzberater ernennt. Vielmehr muss dieser aktiv in die Erarbeitung der Datenschutz-Folgenabschätzung involviert sein. So muss er insbesondere die Risikobewertung und die vorgeschlagenen Massnahmen zur Bewältigung dieser Risiken prüfen. Die Bestimmung soll Unternehmen entlasten und ihnen zugleich einen Anreiz geben, einen Datenschutzberater einzusetzen.

Eine solche Ausnahme wurde auf europäischer Ebene zwar diskutiert, aber schliesslich in der Verordnung (EU) 2016/679 nicht vorgesehen. Dem Bundesrat erscheint es sinnvoll, in diesem Punkt weitergehende Erleichterungen vorzusehen, insbesondere um den Verwaltungsaufwand zu reduzieren. Der Beauftragte hätte es vorgezogen, wenn diese Vorschrift nicht in den Entwurf aufgenommen worden wäre.

Art. 22 Meldung von Verletzungen der Datensicherheit

Artikel 22 E-DSG führt die Pflicht zur Meldung von Verletzungen der Datensicherheit ein. Diese Bestimmung verwirklicht die Anforderungen von Artikel 7 Absatz 2 E-SEV 108 sowie der Artikel 30 f. der Richtlinie (EU) 2016/680. Die Artikel 33 f. der Verordnung (EU) 2016/679 enthalten eine ähnliche Regelung.

Abs. 1 Begriff und Grundsatz

Nach Absatz 1 meldet der Verantwortliche dem Datenschutzbeauftragen so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Die vorliegende Bestimmung gilt sowohl für private Verantwortliche als auch für Bundesorgane, weshalb nicht nur von einem Risiko für die Persönlichkeit der betroffenen Person, sondern auch für deren Grundrechte die Rede ist.

Die Verletzung der Datensicherheit ist in Artikel 4 Buchstabe g E-DSG definiert. Demnach handelt es sich dabei um eine Verletzung der Sicherheit, die, ungeachtet der Absicht oder der Widerrechtlichkeit, dazu führt, dass Personendaten verlorengehen, gelöscht oder vernichtet, verändert oder Unbefugten offengelegt oder zugänglich gemacht werden. Die Verletzung kann durch Dritte erfolgen, aber auch durch Mitarbeiter, die ihre Kompetenzen missbrauchen oder fahrlässig handeln. Durch eine Verletzung der Datensicherheit kann die betroffene Person die Kontrolle über ihre Daten verlieren, oder diese Daten werden missbraucht. Darüber hinaus kann sie auch zu einer Verletzung der Persönlichkeit der betroffenen Person führen, zum Beispiel indem geheime Informationen über sie bekannt werden. Dementsprechend gilt nach Artikel 26 Absatz 2 Buchstabe a E-DSG eine Verletzung der Datensicherheit als Persönlichkeitsverletzung.

Auf diese Gefährdungen kann die betroffene Person nur reagieren, wenn sie von der Verletzung der Datensicherheit weiss. Daher muss der Verantwortliche prinzipiell eine unbefugte Bearbeitung melden, wobei die Meldung zunächst an den Beauftragten geht und nur unter den Voraussetzungen von Absatz 4 an die betroffene Person. Die Meldung hat ab dem Zeitpunkt der Kenntnisnahme so rasch als möglich zu erfolgen. Der Verantwortliche muss grundsätzlich schnell handeln, aber die Bestimmung gibt einen gewissen Ermessensspielraum. Massgebend ist dabei unter anderem das Ausmass der Gefährdung der betroffenen Person. Je erheblicher die Gefährdung, je grösser die Anzahl der betroffenen Personen, umso schneller muss der Verantwortliche handeln.

Die Meldung an den Beauftragten ist jedoch nur nötig, wenn die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Dies soll verhindern, dass selbst unbedeutende Verletzungen gemeldet werden müssen. Der Verantwortliche muss dafür eine Prognose in Bezug auf die möglichen Auswirkungen der Verletzung für die betroffene Person stellen.

Abs. 2 Inhalt der Meldung

Absatz 2 enthält die Mindestanforderungen an eine Meldung an den Beauftragten. Der Verantwortliche muss zunächst die Art der Verletzung der Datensicherheit nennen, soweit ihm dies möglich ist. Dabei lassen sich vier Arten der Verletzung unterscheiden: die Vernichtung oder Löschung, der Verlust, die Veränderung und die Bekanntgabe von Daten an Unbefugte. Ebenfalls muss er die Folgen der Verletzung der Datensicherheit soweit als möglich umschreiben. Hierbei stehen die Folgen für die betroffene Person im Vordergrund; gemeint sind nicht diejenigen für den Verantwortlichen selbst. Schliesslich muss der Verantwortliche angeben, welche Massnahmen er aufgrund der Verletzung ergriffen hat bzw. welche Massnahmen er

für die Zukunft vorschlägt. Dabei geht es um Massnahmen, welche die Verletzung beseitigen oder deren Folgen mildern. Insgesamt soll die Meldung dem Beauftragten erlauben, möglichst zeitnah und wirksam zu intervenieren.

Abs. 3 Meldung durch den Auftragsbearbeiter

Eine Verletzung der Datensicherheit kann auch beim Auftragsbearbeiter auftreten. Daher ist dieser nach Absatz 3 verpflichtet, dem Verantwortlichen so rasch als möglich jede unbefugte Datenbearbeitung zu melden. Es ist am Verantwortlichen, anschliessend eine Risikoabschätzung vorzunehmen und darüber zu entscheiden, inwieweit eine Meldepflicht gegenüber dem Beauftragten und der betroffenen Person besteht.

Abs. 4 Information an die betroffene Person

Grundsätzlich muss die betroffene Person nicht benachrichtigt werden. Gemäss Absatz 4 muss sie jedoch über die Verletzung der Datensicherheit informiert werden, wenn es zu ihrem Schutz erforderlich ist oder wenn der Beauftragte es verlangt. Dabei besteht ein gewisser Ermessensspielraum. Bedeutsam ist insbesondere, ob durch die Information die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person reduziert werden können. Dies ist insbesondere der Fall, wenn die betroffene Person entsprechende Vorkehren zu ihrem Schutz treffen muss, zum Beispiel indem sie ihre Zugangsdaten oder Passwörter ändert.

Abs. 5 Einschränkung der Pflicht zur Information der betroffenen Person

Der Verantwortliche kann nach Absatz 5 die Information an die betroffenen Person einschränken, aufschieben oder darauf verzichten, wenn einer der Gründe von Artikel 24 Absatz 1 Buchstabe b oder Absatz 2 Buchstabe b E-DSG vorliegt oder eine gesetzliche Geheimhaltungspflicht dies verbietet (Bst. a.). Nach Absatz 5 Buchstabe b ist die Einschränkung ebenfalls zulässig, wenn die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert. Eine Information ist unmöglich, wenn der Verantwortliche gar nicht weiss, welche Personen von der Verletzung der Datensicherheit betroffen sind, beispielsweise weil die Logfiles, aus denen dies ersichtlich wäre, nicht mehr vorhanden sind. Ein unverhältnismässiger Aufwand würde beispielsweise vorliegen, wenn bei einer grossen Anzahl Betroffener diese einzeln informiert werden müssten und die dadurch verursachten Kosten im Verhältnis zum Informationsgewinn für die betroffene Person unverhältnismässig erschienen. Insbesondere in solchen Konstellationen kann Absatz 5 Buchstabe c zur Anwendung kommen, der dem Verantwortlichen erlaubt, die betroffenen Personen durch eine öffentliche Bekanntmachung zu informieren, wenn sie dadurch auf vergleichbare Weise informiert werden. Dies ist der Fall, wenn die Information der betroffenen Person durch eine individuelle Information nicht substantiell verbessert wird.

Abs. 6 Einverständnis des Meldepflichtigen

Die Meldepflicht nach Artikel 22 E-DSG kann in Konflikt geraten mit dem Grundsatz, dass sich niemand selbst belasten muss. Absatz 6 sieht für diese Konstellation vor, dass eine Meldung, die in Erfüllung der Meldepflicht nach Artikel 22 E-DSG erfolgt, in einem Strafverfahren gegen den Meldepflichtigen nur verwendet werden

darf, wenn dieser damit einverstanden ist. Die Bestimmung erfasst sowohl Verantwortliche als auch Auftragsbearbeiter, die eine Verletzung der Datensicherheit melden.

9.1.5 Rechte der betroffenen Person

Das 4. Kapitel regelt die Rechte der betroffenen Person. Spezifische Ansprüche gegenüber den privaten Verantwortlichen sind im 5. Kapitel festgelegt, solche gegenüber Bundesorganen im 6. Kapitel.

Art. 23 Auskunftsrecht

Das Auskunftsrecht ergänzt die Informationspflicht des Verantwortlichen und bildet die zentrale Grundlage dafür, dass die betroffene Person ihre Rechte nach diesem Gesetz überhaupt wahrnehmen kann. Das Auskunftsrecht ist ein subjektives höchstpersönliches Recht, das auch urteilsfähige handlungsunfähige Personen selbständig, ohne Zustimmung ihres gesetzlichen Vertreters, geltend machen können. Aus dem Charakter des höchstpersönlichen Rechts ergibt sich auch, dass niemand im Voraus auf das Auskunftsrecht verzichten kann (Art. 23 Abs. 5 E-DSG).

Abs. 1 Grundsatz

Nach Absatz 1 kann jede Person vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Die Bestimmung bleibt, abgesehen von redaktionellen Anpassungen, unverändert im Verhältnis zum bisherigen Recht.

Abs. 2 Mitzuteilende Informationen

Absatz 2 hält fest, dass die betroffene Person aufgrund eines Auskunftsbegehrens diejenigen Informationen erhält, die ihr auch aufgrund der Informationspflicht mitgeteilt werden müssen (vgl. Art. 17 Abs. 2 E-DSG). Dabei handelt es sich grundsätzlich um diejenigen Informationen, die erforderlich sind, damit die betroffene Person ihre Rechte nach dem Gesetz geltend machen kann und damit eine transparente Datenbearbeitung gewährleistet ist. Dies verdeutlicht den engen Zusammenhang von Auskunftsrecht und Informationspflicht. Zugleich wird auf diese Weise der zentrale Zweck des Auskunftsrechts hervorgehoben, wie ihn auch das Bundesgericht festgehalten hat, nämlich der betroffenen Person zu ermöglichen, ihre Rechte im Bereich des Datenschutzes geltend zu machen.[153] Die Präzisierung erfolgt vor dem Hintergrund der zahlreichen Stellungnahmen in der Vernehmlassung sowie in der Lehre, die kritisieren, dass das Auskunftsrecht häufig zu anderen, datenschutzfremden Zwecken verwendet werde.[154] Angesprochen sind insbesondere Fälle, in denen das Auskunftsrecht ausschliesslich zur Beschaffung von Beweismitteln für Zivilprozesse benutzt wird, die in keinem Zusammenhang mit dem Datenschutz stehen. Dadurch wird die Beschaffung von Beweismitteln, die zugleich als Perso-

153 BGE **138** III 425 E. 5.3.
154 Vgl. Rosenthal David, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, Jusletter 20. Februar 2017, N 54 ff.

nendaten nach dem DSG zu bezeichnen sind, in einer Form ermöglicht, wie sie im geltenden Verfahrensrecht nicht vorgesehen ist. Andere Beweismittel, die keine Personendaten darstellen, sind hingegen auf den üblichen prozessrechtlichen Wegen zu beschaffen. Daraus ergeben sich sachlich nicht gerechtfertigte Unterschiede in der Beweismittelbeschaffung.

Die Buchstaben a bis g enthalten eine Liste der Informationen, welche der betroffenen Person in jedem Fall mitzuteilen sind. Die nicht abschliessende Aufzählung erfasst grundsätzlich sämtliche Informationen, die der Verantwortliche der betroffenen Person mitteilen muss. Subsidiär erlaubt die Generalklausel im Einleitungssatz, gegebenenfalls weitere Informationen zu verlangen, wenn diese für die betroffene Person erforderlich sind, um ihre Rechte nach diesem Gesetz geltend zu machen und eine transparente Datenbearbeitung zu gewährleisten. Wenn er grosse Datenmengen über die betroffene Person bearbeitet, kann der Auskunftspflichtige gegebenenfalls verlangen, dass die betroffene Person präzisiert, auf welche Informationen oder welche Bearbeitungsvorgänge sich ihr Auskunftsgesuch bezieht.[155]

In jedem Fall erhält die betroffene Person zunächst Auskunft über die Identität und die Kontaktdaten des Verantwortlichen (Bst. a). Je nachdem wird sie diese Informationen bereits haben (z. B. aufgrund der Informationspflicht) und sie werden ihr bestätigt. Denkbar ist aber auch, dass die betroffene Person erst in diesem Zeitpunkt von einem Verantwortlichen erfährt, z. B. wenn es mehrere Verantwortliche gibt. Darüber hinaus müssen ihr die bearbeiteten Personendaten (Bst. b) und der Bearbeitungszweck (Bst. c) mitgeteilt werden. Ebenso erhält die betroffene Person Auskunft darüber, wie lange die Daten aufbewahrt werden, oder, wenn dies nicht möglich ist, nach welchen Kriterien sich die Aufbewahrungsdauer richtet (Bst. d). Diese Informationen erlauben ihr insbesondere nachzuvollziehen, ob der Verantwortliche die Daten entsprechend den Grundsätzen in Artikel 5 E-DSG bearbeitet. Da die Aufbewahrungsdauer aufgrund der Informationspflicht regelmässig nicht mitgeteilt werden muss, soll die betroffene Person sie im Rahmen des Auskunftsrechts in jedem Fall erhalten. Ebenfalls erhält die betroffene Person die verfügbaren Angaben über die Herkunft der Daten, soweit sie nicht bei ihr erhoben wurden (Bst. e). Gegebenenfalls wird der betroffenen Person mitgeteilt, ob eine automatisierte Einzelentscheidung vorliegt (Bst. f). In diesem Fall erhält sie ebenfalls Informationen über die Logik, auf der die Entscheidung beruht. Dabei müssen nicht unbedingt die Algorithmen mitgeteilt werden, die Grundlage der Entscheidung sind, weil es sich dabei regelmässig um Geschäftsgeheimnisse handelt. Vielmehr müssen die Grundannahmen der Algorithmus-Logik genannt werden, auf der die automatisierte Einzelentscheidung beruht. Das bedeutet beispielsweise, dass die betroffene Person Auskunft darüber erhält, dass sie aufgrund eines negativen Scoring-Resultats einen Vertrag zu schlechteren Konditionen abschliessen kann, als dies offeriert wurde. Darüber hinaus muss sie aber auch über die Menge und die Art der für das Scoring herangezogenen Informationen sowie deren Gewichtung informiert werden. Schliesslich erhält die betroffenen Person Informationen über die Empfänger oder die Kategorien von Empfängern, denen die Personendaten bekanntgegeben werden (Bst. g). Falls die Empfänger sich im Ausland befinden, nennt der Auskunftspflichtige zudem den

155 Vgl. hierzu auch die ähnlichen Ausführungen im Erwägungsgrund 63 der Verordnung (EU) 2016/679.

Staat, in den die Daten bekanntgegeben werden, sowie gegebenenfalls die Garantien nach Artikel 13 Absatz 2 E-DSG oder die Anwendung einer Ausnahme nach Artikel 14 E-DSG.

Abs. 3 und 4

Aus dem geltenden Recht unverändert übernommen wurde Absatz 3, wonach der Verantwortliche Informationen über die Gesundheit der betroffenen Person durch eine von dieser bezeichneten Gesundheitsfachperson mitteilen kann. Die Gesundheitsfachperson muss die Qualifikationen haben, die im fraglichen Fall erforderlich sind. Vorgesehen ist aber neu die Einwilligung der betroffenen Person, dass ihr die Daten über eine andere Person mitgeteilt werden. Dies verbessert die Wahlmöglichkeiten der betroffenen Person. Ebenfalls wird der Kreis der möglichen Personen erweitert, indem von einer Gesundheitsfachperson die Rede ist. Beide Ergänzungen erfolgen aufgrund der Vernehmlassung.

Satz 1 von Absatz 4 bleibt unverändert. Demnach ist grundsätzlich stets der Verantwortliche auskunftspflichtig, selbst wenn er die Bearbeitung an einen Auftragsbearbeiter delegiert. Richtet die betroffene Person ein Auskunftsgesuch versehentlich an den Auftragsbearbeiter, muss dieser ihr den Verantwortlichen nennen oder das Gesuch entsprechend weiterleiten. Der Auftragsbearbeiter muss in einem solchen Fall nicht selbst Auskunft geben, aber er darf die betroffene Person bei der Ausübung ihres Auskunftsrechts auch nicht behindern. Satz 2 der Bestimmung wird hingegen gestrichen.

Abs. 5

Diese Bestimmung entspricht dem bisherigen Artikel 8 Absatz 6 DSG.

Abs. 6

Absatz 6 gibt dem Bundesrat die Möglichkeit, in der Verordnung Ausnahmen von der Kostenlosigkeit vorzusehen. Diese Möglichkeit besteht schon im bisherigen Recht (vgl. Art. 2 VDSG). In der Vernehmlassungsvorlage wurde sie gestrichen, was erheblich kritisiert wurde, unter anderem mit der Begründung, dass Ausnahmen von der Kostenlosigkeit eine Möglichkeit seien, um Missbräuchen des Auskunftsrechts vorzubeugen. Aufgrund der Kritik in der Vernehmlassung wird diese Vorschrift nun beibehalten. Der Bundesrat wird dabei der Tatsache Rechnung tragen, dass gewisse Auskunftsersuchen für den Verantwortlichen mit einem grossen Aufwand verbunden sind.

Art. 24 Einschränkungen des Auskunftsrechts

Artikel 24 regelt die Einschränkungen des Auskunftsrechts. Sie wurden mit wenigen redaktionellen Anpassungen unverändert aus dem bisherigen Recht übernommen.

Abs. 1 Bst. c

Neu ist lediglich Artikel 24 Absatz 1 Buchstabe c. Demnach kann der Verantwortliche die Auskunft verweigern, einschränken oder aufschieben, wenn das Auskunftsgesuch offensichtlich unbegründet oder querulatorisch ist. Die Bestimmung wurde

aufgrund der Vernehmlassung aufgenommen. Sie orientiert sich inhaltlich an Artikel 12 Absatz 5 der Verordnung (EU) 2016/679, verwendet aber die schweizerische Terminologie, wie sie z. B. in Artikel 108 BGG sowie in Artikel 132 und 253 ZPO zu finden ist. Es handelt sich hierbei um eine schwere Grundrechtsbeschränkung, weshalb sie im Gesetz selbst und nicht in der Verordnung vorzusehen ist.

Die Ausnahme nach Absatz 1 Buchstabe c ist eng auszulegen. Dies gilt in zweifacher Hinsicht. Einerseits darf der Verantwortliche nicht leichthin annehmen, ein Auskunftsgesuch sei offensichtlich unbegründet oder aber querulatorisch. Andererseits hat er selbst für den Fall, dass ein solches Gesuch vorliegt, die für die betroffene Person günstigste Lösung zu wählen. Er muss daher soweit als möglich die Auskunft lediglich einschränken, darf sie allenfalls aufschieben und kann sie nur in den absolut eindeutigen, offensichtlichen, Fällen verweigern. In jedem Fall hat er die betroffene Person über die Verweigerung, die Einschränkung oder den Aufschub der Auskunft zu informieren (vgl. Abs. 3).

Das Auskunftsrecht kann ohne Nachweis eines Interesses und ohne eine Begründung geltend gemacht werden. Auch blosse Neugier reicht aus. Dies wird verdeutlicht durch die Bezugnahme auf eine transparente Datenbearbeitung in Artikel 23 Absatz 2 E-DSG. Der Verantwortliche darf daher grundsätzlich keine Begründung eines Auskunftsgesuchs fordern. Das Bundesgericht hielt jedoch fest, dass der Auskunftspflichtige eine Begründung für das Auskunftsbegehren verlangen kann, wenn im konkreten Fall eine rechsmissbräuchliche Nutzung des Auskunftsrechts in Frage steht.[156] Als möglicherweise rechtsmissbräuchlich erachtete das Bundesgericht insbesondere die Verwendung des Auskunftsrechts zu datenschutzwidrigen Zwecken, beispielsweise um sich die Kosten einer Beweisbeschaffung zu sparen, oder um eine mögliche Gegenpartei auszuforschen.[157] Bringt die betroffene Person, welche Auskunft verlangt, anschliessend einen Grund vor, der sich bereits ohne vertiefte Prüfung und ohne Zweifel als haltlos erweist, darf der Verantwortliche das Auskunftsrecht einschränken. Nur unter diesen Umständen kann ein offensichtlich unbegründetes Auskunftsgesuch vorliegen. Es muss mit anderen Worten offenkundig sein, dass das Auskunftsgesuch aus Gründen gestellt wurde, die mit seinem Zweck nach dem DSG nichts zu tun haben, oder dass dies in anderweitiger (z. B. betrügerischer) Absicht geschehen ist. Bestehen Zweifel, ob es sich um einen solchen Fall handelt, liegt kein offensichtlich unbegründetes Gesuch vor.

Querulatorisch sind Auskunftsgesuche, die beispielsweise ohne plausible Begründung häufig wiederholt werden, oder die sich an einen Verantwortlichen richten, von dem die Gesuchstellerin oder der Gesuchsteller bereits weiss, dass er keine Daten über sie oder ihn bearbeiten. Auch von einem querulatorischen Gesuch darf der Verantwortliche nicht leichthin ausgehen.

Insgesamt darf der Verantwortliche von der Einschränkung nach Absatz 1 Buchstabe c nicht bereits dann Gebrauch machen, wenn er lediglich seine eigenen Interessen wahren möchte. Hierfür müssen die Voraussetzungen nach Artikel 24 Absatz 2 Buchstabe a erfüllt sein. Vielmehr soll die Bestimmung in Absatz 1 Buchstabe c dem Verantwortlichen den vernünftigen Umgang mit Auskunftsgesuchen erlauben,

156 BGE **138** III 425 E. 5.4 f.; **123** II 534 E. 2e.
157 BGE **138** III 425 E. 5.5.

die offensichtlich völlig losgelöst vom Zweck erfolgen, dem das Auskunftsrecht dient.

Der Beauftragte ist der Ansicht, dass die in Artikel 24 Absatz 1 Buchstabe c E-DSG vorgesehene Ausnahme vom Auskunftsrecht mit dem Übereinkommen SEV 108 nicht vereinbar ist.

Abs. 3

Falls der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies mitteilen und gemäss Absatz 3 entsprechend begründen. Als Gründe kommen grundsätzlich nur die Voraussetzungen nach den Absätzen 1 und 2 in Frage. Bundesorgane müssen in diesem Fall eine anfechtbare Verfügung erlassen. Private Verantwortliche unterliegen hingegen keinen Formvorschriften. Aus Beweisgründen sollte die Begründung der betroffenen Person jedoch schriftlich zugestellt werden.

Auf der Basis der Begründung muss die betroffene Person überprüfen können, ob die Auskunft zu Recht verweigert, eingeschränkt oder aufgeschoben worden ist. Die Anforderungen an die Begründung können jedoch nicht allzu hoch sein, falls sie mit dem Grund für die Auskunftsverweigerung kollidieren.

Art. 25 Einschränkungen des Auskunftsrechts für Medienschaffende

Artikel 25 E-DSG übernimmt den aktuellen Artikel 10 DSG betreffend die Einschränkung des Auskunftsrechts für Medienschaffende. Es erfolgen keine materiellen Änderungen. Das Kriterium der Veröffentlichung im redaktionellen Teil eines Mediums bleibt bestehen. Dies bedeutet, dass alleine Daten darunter fallen, welche gesammelt werden im Hinblick auf die Publikation einer journalistischen Arbeit in jenem Teil eines Mediums, das für redaktionelle Beiträge reserviert ist.[158] Darüber hinaus muss es sich um ein periodisch erscheinendes Medium handeln. Darunter fallen insbesondere Zeitungen, Zeitschriften, Radio- und Fernsehsendungen, Presseagenturen und Online-Newsdienste, die kontinuierlich und mit einer dem Publikum bekannten Regelmässigkeit aktualisiert werden.[159]

9.1.6 Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Das 5. Kapitel regelt spezifische Ansprüche gegenüber privaten Verantwortlichen. Die Vorschriften zum Bearbeiten von Personendaten durch private Personen konkretisieren den Schutz der Persönlichkeit nach Artikel 28 ZGB in Bezug auf den Datenschutz und dienen damit der Verwirklichung der informationellen Selbstbestimmung unter Privaten (siehe Art. 35 Abs. 1 und 3 BV). Die drei Bestimmungen dieses Abschnitts sind gemeinsam zu lesen: Artikel 26 E-DSG konkretisiert Persönlichkeitsverletzungen im Bereich des Datenschutzes, Artikel 27 E-DSG definiert spezifische Rechtfertigungsgründe und Artikel 28 E-DSG regelt die Rechtsansprüche, die

158 Barrelet Denis/Werly Stéphane, Droit de la communication, 2. Aufl., Bern 2011, N 1769.
159 Barrelet Denis/Werly Stéphane, Droit de la communication, 2. Aufl., Bern 2011, N 1420.

aufgrund einer Persönlichkeitsverletzung durch Datenbearbeitung geltend gemacht werden können. Der vorliegende Entwurf behält die bestehende Regelung weitgehend bei. Es wurden jedoch einige redaktionelle Änderungen vorgenommen mit dem Ziel, die Bestimmungen insgesamt klarer und zugänglicher zu machen.

Die Evaluation hat zudem ergeben, dass die betroffenen Personen insbesondere im privaten Sekor ihre Rechte kaum wahrnehmen. Dies wird hauptsächlich auf die Kostenrisiken eines Prozesses zurückgeführt[160], welche durch Anpassungen bei der Kostenregelung im Zivilprozess aufgefangen werden sollen (vgl. Ziff. 9.2.15).

Art. 26 Persönlichkeitsverletzungen

Der Begriff der Persönlichkeitsverletzung ist in Artikel 28 ZGB nicht definiert. Artikel 26 des Entwurfs konkretisiert diesen Begriff für Verletzungen der Persönlichkeit durch die Bearbeitung von Personendaten.

Abs. 1 Grundsatz

Absatz 1 hält fest, dass durch eine Datenbearbeitung die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzt werden darf. Der Wortlaut bleibt unverändert. Das individuelle Verfügungsrecht über personenbezogene Daten, welches durch die informationelle Selbstbestimmung geschützt ist, wird durch Datenbearbeitungen rasch empfindlich eingeschränkt. Die Einhaltung der Grundsätze der Datenbearbeitung durch private Verantwortliche ist daher zentral zum Schutz der Persönlichkeit der betroffenen Person, zumal die private Bearbeitung einen grossen Anteil der Datenbearbeitungsvorgänge überhaupt ausmacht.

Abs. 2 Fälle von Persönlichkeitsverletzungen

Absatz 2 nimmt unter anderem Bezug auf die Einhaltung der Grundsätze der Datenbearbeitung und sieht vor, dass namentlich in drei Konstellationen eine Persönlichkeitsverletzung vorliegt.

Nach Buchstabe a liegt eine Persönlichkeitsverletzung vor, wenn Daten entgegen den Grundsätzen der Artikel 5 und 7 E-DSG bearbeitet werden.

Persönlichkeitsverletzend ist nach Buchstabe b zudem, wenn Daten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden. Diese Bestimmung gibt der betroffenen Person mithin das Recht, einem bestimmten Verantwortlichen explizit eine bestimmte Datenbearbeitung zu verbieten, ohne dass hierfür spezifische Voraussetzungen erfüllt sein müssten (Opting-out). Diese Möglichkeit bestand bereits nach dem bisherigen Recht und wird auch durch Artikel 8 Buchstabe d E-SEV 108 verlangt. Eine Willenserklärung ist «ausdrücklich», wenn sie durch geschriebene oder gesprochene Worte oder ein Zeichen erfolgt und der geäusserte Willen aus den verwendeten Worten oder dem Zeichen unmittelbar hervorgeht. Demnach muss die betroffene Person in Worten oder Zeichen unmittelbar zum Ausdruck bringen, dass sie mit einer bestimmten Datenbearbeitung nicht einverstanden ist. Die Willensäusserung als solche muss durch die Art und Weise, in

160 Vgl. S. 90 f. und 219 des Schlussberichts zur Evaluation des Bundesgesetzes über den Datenschutz vom 10. März 2011.

der sie erfolgt, bereits Klarheit über den Willen schaffen. Im vorliegenden Fall müsste die betroffene Person beispielsweise eine Dienstleistung, die mit einer Datenbearbeitung einhergeht, kündigen oder gegenüber einem Verantwortlichen eine mündliche oder schriftliche Erklärung abgeben, dass sie nicht will, dass er Daten über sie bearbeitet. Demgegenüber ist eine «stillschweigende» Willenserklärung im vorliegenden Fall nicht ausreichend (vgl. die Erläuterungen zu Artikel 5 Absatz 6 E-DSG in Ziff. 9.1.3.1). So wäre es beispielsweise nicht ausreichend, dass die betroffene Person eine Dienstleistung, die mit einer Datenbearbeitung einhergeht, nicht mehr benutzt.

Nach Buchstabe c liegt ebenfalls eine Persönlichkeitsverletzung vor, wenn besonders schützenswerte Daten an Dritte bekanntgegeben werden.

Die Aufzählung ist nicht abschliessend. Das heisst, eine Persönlichkeitsverletzung durch die Bearbeitung von Daten kann auch auf anderem Wege als durch die Verwirklichung dieser drei Tatbestände erfolgen. In Buchstaben b und c wurde die Bezugnahme auf den Rechtfertigungsgrund entfernt, wie dies bei der Revision im Jahre 2003 bereits für Buchstabe a erfolgte[161]. Auch dies dient lediglich der Klarheit und entspricht Artikel 28 ZGB, in dem die Verletzung der Persönlichkeit und die Rechtfertigungsgründe ebenfalls in zwei Teilbestimmungen behandelt werden. Im E-DSG werden die Rechtfertigungsgründe nun ausschliesslich in Artikel 27 geregelt.

Abs. 3 Keine Persönlichkeitsverletzung

Nach Absatz 3 liegt hingegen in der Regel keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und deren Bearbeitung nicht ausdrücklich untersagt hat (zur Ausdrücklichkeit vgl. den Kommentar oben zu Absatz 2 Buchstabe b). Diese Regelung, die identisch aus dem bisherigen Recht übernommen wurde, ist folgerichtig. Denn die individuelle Verfügungsfreiheit über personenbezogene Daten wird unter diesen Umständen prinzipiell nicht verletzt. Durch die Formulierung «in der Regel» wird ausgedrückt, dass es sich dabei um eine gesetzliche Vermutung und keine unumstössliche Fiktion handelt. Der betroffenen Person steht dadurch der Nachweis offen, dass im Einzelfall dennoch eine Persönlichkeitsverletzung vorliegen kann. Diese Möglichkeit ist sachgerecht und wichtig, weil die Abgrenzung zwischen Öffentlichkeit und Privatheit zunehmend schwierig ist.

Art. 27 Rechtfertigungsgründe

Artikel 27 konkretisiert die Rechtfertigungsgründe für persönlichkeitsverletzende Datenbearbeitungen. Die Norm bleibt abgesehen von kleineren Änderungen unverändert.

Abs. 1 Grundsatz

Absatz 1 hält den Grundsatz fest, wonach jede Persönlichkeitsverletzung – d. h. jede persönlichkeitsverletzende Datenbearbeitung – grundsätzlich widerrechtlich ist,

161 Vgl. hierzu BGE **136** II 508 E. 5.2.3.

ausser sie wäre durch Einwilligung der betroffenen Person, durch Gesetz oder ein überwiegendes privates oder öffentliches Interesse gerechtfertigt. Diese Bestimmung entspricht Artikel 28 Absatz 2 ZGB. Falls die Einwilligung der betroffenen Person oder ein gesetzlicher Rechtfertigungsgrund vorliegt, erfolgt grundsätzlich keine Interessenabwägung und die Abwägungsgründe nach Absatz 2 kommen nicht zum Zug. Zu den gesetzlichen Rechtfertigungsgründen gehören beispielsweise Bearbeitungs- oder Abklärungspflichten (z. B. Art. 28 ff. des Bundesgesetzes vom 23. März 2001[162] über den Konsumkredit, Art. 3 ff. des Geldwäschereigesetzes vom 10. Oktober 1997[163]) oder Aufbewahrungspflichten. Hingegen erfordert ein überwiegendes privates oder öffentliches Interesse eine Abwägung der sich gegenüberstehenden Interessen. Auf Seiten der betroffenen Person besteht u. a. das Interesse an der Wahrung ihrer Verfügungsfreiheit über ihre Daten. Auf Seiten des Verantwortlichen liegt ein Interesse an der Datenbearbeitung vor. Absatz 2 enthält in einer beispielhaften Aufzählung Bearbeitungen, bei welchen ein überwiegendes Interesse des Verantwortlichen in Betracht kommt. Nur wenn das Interesse an der Datenbearbeitung überwiegt gegenüber dem Interesse der betroffenen Person, ist die Persönlichkeitsverletzung gerechtfertigt.

Abs. 2 Überwiegende Interessen des Verantwortlichen

Absatz 2 konkretisiert, wann ein überwiegendes Interesse des Verantwortlichen in Betracht fällt. Die Formulierung, die unverändert beibehalten wurde, macht deutlich, dass es sich dabei nicht um absolute Rechtfertigungsgründe handelt. Massgebend ist vielmehr wie im bisherigen Recht letztlich die Interessenabwägung im Einzelfall. Anders als im bisherigen Recht ist nicht mehr von der bearbeitenden Person, sondern vom Verantwortlichen die Rede. Die Anpassung erfolgt aufgrund der Einführung des Begriffs des Verantwortlichen. Die Rechtfertigungsgründe nach Artikel 27 Absatz 2 sind auf Personen zugeschnitten, die als Verantwortliche über Zweck und Mittel der Datenbearbeitung entscheiden können. Andere Beklagte können Rechtfertigungsgründe nach Absatz 1 geltend machen. Aufgrund von Artikel 8 Absatz 4 E-DSG kann der Auftragsbearbeiter dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche. Auch die Passivlegitimation bleibt von der Änderung unbeeinflusst.

Die aufgeführten Gründe entsprechen weitgehend dem bisherigen Recht. Die Aufzählung ist nicht abschliessend, sodass auch andere Gründe, als die hier aufgeführten, als überwiegendes Interesse des Verantwortlichen herangezogen werden können. Die Aufzählung führt verschiedene Zwecke auf, welche die Bearbeitung von Daten rechtfertigen und gegenüber dem Interesse der betroffenen Person überwiegen können. Im Wesentlichen erfasst der Katalog drei Gruppen von Datenbearbeitungen: solche für bestimmte wirtschaftliche Tätigkeiten, solche für die Medien und Datenbearbeitungen zu nicht personenbezogenen Zwecken wie der Forschung. Bei einzelnen Bearbeitungszwecken reicht der angegebene Zweck alleine nicht aus, um die Persönlichkeitsverletzung zu rechtfertigen. Vielmehr muss die Bearbeitung zusätzlich bestimmte Voraussetzungen erfüllen, damit der Rechtfertigungsgrund des überwiegenden Interesses überhaupt geltend gemacht werden kann. Dies gilt na-

162 SR **221.214.1**
163 SR **955.0**

mentlich in Bezug auf die Buchstaben b, c, e und f. In diesen Fällen ist zunächst zu prüfen, ob die fragliche Bearbeitung die spezifischen Voraussetzungen erfüllt, bevor die Interessen des konkreten Einzelfalls gegeneinander abgewogen werden. Sind diese spezifischen Voraussetzungen nicht gegeben, ist die Datenbearbeitung nur gerechtfertigt, wenn ein Rechtfertigungsgrund nach Absatz 1 vorliegt. Kommentiert werden nachfolgend nur die Buchstaben c und e, bei denen der Gesetzestext geändert wurde.

Abs. 2 Bst. c Prüfung der Kreditwürdigkeit

In Bezug auf die Tätigkeit von Wirtschaftsauskunftsdiensten ist zunächst auf das kürzlich ergangene Urteil des Bundesverwaltungsgerichts A-4232/2015 vom 18. April 2017 (Moneyhouse) hinzuweisen. Die Moneyhouse AG ist ein Wirtschaftsauskunftsdienst und bezieht Daten in elektronischer Form von diversen öffentlichen privaten Quellen. Diese Vielzahl von Personendaten wird auf www.moneyhouse.ch publiziert und dazu verwendet, um verschiedene Dienstleistungen anzubieten, insbesondere eine Firmen- und Personensuche. Während dieser Dienst für das Publikum nach erfolgter Registrierung kostenlos ist, werden zusätzlich zahlungspflichtig für sogenannte «Premium User» Bonitäts- und Zahlweiseabonnemente, Details zu Zahlungsstörungen, Betreibungs-, Grundbuch-, Wirtschafts- und Steuerauskünfte sowie Dienstleistungen betreffend Firmenportraits angeboten. Für Zusatzangebote und um auf Daten natürlicher Personen, die nicht im Handelsregister oder in einem elektronischen Telefonverzeichnis eingetragen sind, zuzugreifen, müssen Interessensnachweise erbracht werden.[164] Bezüglich der kostenpflichtigen Premiumabonnemente kam das Bundesverwaltungsgericht zum Schluss, dass die Moneyhouse AG dabei teilweise ein biografisches Bild von Personen erstellt. Das Bundesverwaltungsgericht hielt fest, dass bei dieser Ausgangslage die Bearbeitung eines Persönlichkeitsprofils zu bejahen sei, weshalb der Rechtfertigungsgrund der Kreditüberprüfung nach Artikel 13 Absatz 2 Buchstabe c DSG nicht zur Anwendung gelange.[165] Für das Bundesverwaltungsgericht war als Rechtfertigungsgrund weder eine gesetzliche Grundlage ersichtlich noch konnte eine explizite Einwilligung der betroffenen Personen in die Erstellung eines Persönlichkeitsprofils belegt werden. Schliesslich ergab auch eine gesamthafte Interessenabwägung, dass das Interesse der betroffenen Personen an der Wahrung ihrer Persönlichkeitsrechte überwiegt. Im Ergebnis stellte das Bundesverwaltungsgericht eine rechtswidrige Bearbeitung von Persönlichkeitsprofilen fest und wies die Moneyhouse AG an, für solche Datenbearbeitungen die ausdrückliche Einwilligung der betroffenen Personen einzuholen, andernfalls die entsprechenden Daten, insoweit zu löschen seien, als sich Rückschlüsse auf wesentliche Teilaspekte der Persönlichkeit ziehen lassen.[166] Zudem verpflichtete das Gericht die Moneyhouse AG zu einer jährlichen Überprüfung ihres Datenbestands auf dessen Richtigkeit hin im Verhältnis von 5 % zu den auf der Plattform getätigten Abfragen.[167] Darüber hinaus wird der Bundesrat im Rahmen des Berichts für das Postulat Schwaab 16.3682 «Die Tätigkeiten von Wirt-

164 BVGer, A-4232/2015 vom 18. April 2017, Sachverhalt A.a.
165 BVGer, A-4232/2015 vom 18. April 2017, E. 5.3.
166 BVGer, A-4232/2015 vom 18. April 2017, E. 5.5.
167 BVGer, A-4232/2015 vom 18. April 2017, E. 7.3.2.

schaftsauskunfteien einschränken» spezifische Massnahmen in Bezug auf Wirtschaftsauskunftsdienste prüfen.

Der E-DSG trägt allerdings gewissen Anliegen in Bezug auf die Tätigkeit von Wirtschaftsauskunftsdiensten bereits Rechnung. So müssen vier Voraussetzungen erfüllt sein, damit die Prüfung der Kreditwürdigkeit als überwiegendes Interesse gelten kann. Die Bestimmung wird im Verhältnis zum bisherigen Recht leicht verschärft, insbesondere um dem hohen Risiko Rechnung zu tragen, das mit dieser Art der Datenbearbeitung einhergeht.

Die Ziffern 1 und 2 entsprechen dem geltenden Recht, wobei der Begriff des Persönlichkeitsprofils durch jenen des Profilings ersetzt wird. Ebenfalls unzulässig bleibt die Bearbeitung besonders schützenswerter Personendaten. Darunter fällt auch die Bearbeitung von Daten über strafrechtliche Verfolgungen und Sanktionen. Dies ist folgerichtig, da Dritte auch keine Einsicht in das Strafregister erhalten können. Das DSG soll, anders als von verschiedenen Vernehmlassungsteilnehmern angeregt, keine darüber hinausgehenden Rechte für Wirtschaftsauskunftsdienste enthalten.

Die Ziffern 3 und 4 wurden neu hinzugefügt.

Ziffer 3 setzt voraus, dass die Daten nicht älter als fünf Jahre sein dürfen. Eine solche Verstärkung wurde von verschiedenen Vernehmlassungsteilnehmern angeregt und erscheint berechtigt im Hinblick auf die Tragweite einer Kreditauskunft für die betroffene Person. Auch das Bundesverwaltungsgericht hielt fest, dass an die inhaltliche Qualität und damit auch an die Richtigkeit der bearbeiteten Daten umso höhere Anforderungen zu stellen sind, je grösser das Risiko einer Persönlichkeitsverletzung ist.[168] Die sehr niedrige Überprüfungsquote von 5 Prozent, welche das Bundesverwaltungsgericht der Moneyhouse AG auferlegt, zeigt zugleich die Schwierigkeiten auf, solche Datenbanken aktuell zu halten. Daher erachtet der Bundesrat eine generelle Regelung über die Dauer, während der Daten verwendet werden dürfen, als sinnvoll. Eine solche Einschränkung lässt sich insbesondere auch mit entsprechenden technischen Vorkehren (privacy by design, vgl. Art. 6 E-DSG und die Erläuterungen dazu) umsetzen, beispielsweise indem Daten nach Ablauf einer bestimmten Dauer automatisch gelöscht werden. Die Aufbewahrungsdauer von fünf Jahren stellt darauf ab, dass private Dritte gemäss Artikel 8*a* Absatz 4 SchKG lediglich bis fünf Jahre nach Abschluss des Verfahrens Einsicht in das Betreibungsregister erhalten können. Hier sollen die Rechte von Wirtschaftsauskunftsdiensten nicht weiter gehen.

Ziffer 4 setzt voraus, dass die betroffene Person volljährig ist. Diese Voraussetzung wird eingefügt, um den Schutz von Minderjährigen zu verbessern, was eines der Ziele der Revision ist. Die Tragweite dieser Änderung dürfte sich aufgrund der beschränkten Handlungsfähigkeit minderjähriger Personen in Grenzen halten.

Abs. 2 Bst. e Bearbeitung für Forschung, Planung oder Statistik

Leicht verschärft wird der Rechtfertigungsgrund der Bearbeitung zu nicht personenbezogenen Zwecken, insbesondere in der Forschung, Planung oder Statistik, in Buchstabe e. Die Verwendung von Daten zu diesen Zwecken ist neu nur zulässig,

168 BVGer, A-4232/2015 vom 18. April 2017, E. 7.1.

wenn die Voraussetzungen der Ziffern 1–3 erfüllt sind. Durch diese Regelung soll der Schutz besonders schützenswerter Personendaten verstärkt werden. Dies erfolgt insbesondere mit Blick auf die Möglichkeiten von Big Data und die zunehmende Digitalisierung des Alltags, die auch dazu führt, dass eine immer grössere Anzahl besonders schützenswerter Personendaten bearbeitet wird.

Nach Ziffer 1 müssen die Daten anonymisiert werden, sobald der Bearbeitungszweck es erlaubt. Wenn es zur Datenbearbeitung für Forschung, Planung oder Statistik nicht mehr erforderlich ist, über personenbezogene Daten zu verfügen, müssen diese anonymisiert werden. Diese Voraussetzung ist ebenfalls erfüllt, wenn die Weitergabe in pseudonomysierter Form erfolgt und der Schlüssel bei der weitergebenden Person verbleibt (faktische Anonymisierung).

Dies ergibt sich grundsätzlich bereits aus der Vorschrift in Artikel 5 Absatz 4 E-DSG. Ein Verstoss gegen dieselbe führt gemäss Artikel 26 Absatz 2 Buchstabe a E-DSG zu einer Persönlichkeitsverletzung, die sich durch einen der Gründe in Artikel 27 E-DSG rechtfertigen lässt. Durch die Vorschrift in Artikel 27 Absatz 2 Buchstabe e Ziffer 1 E-DSG ist es nun nicht mehr möglich, einen Verstoss gegen Artikel 5 Absatz 4 E-DSG mit der Bearbeitung zu Zwecken der Forschung, Planung oder Statistik zu rechtfertigen, ausser es gilt einer der Rechtfertigungsgründe nach Artikel 27 Absatz 1 E-DSG.

Wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden, muss dies so erfolgen, dass die betroffenen Personen nicht bestimmbar sind (Ziff. 2). Die Bekanntgabe besonders schützenswerter Personendaten an Dritte führt gemäss Artikel 26 Absatz 2 Buchstabe c E-DSG zu einer Persönlichkeitsverletzung, die sich durch einen der Gründe in Artikel 27 rechtfertigen lässt. Die Vorschrift in Ziffer 2 schliesst es nunmehr aus, die Bekanntgabe nicht anonymisierter, besonders schützenswerter Personendaben zu rechtfertigen mit der Begründung, diese erfolge zur Bearbeitung zu Zwecken der Forschung, Planung oder Statistik.

Schliesslich dürfen wie bisher die Ergebnisse nur so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind (Ziff. 3).

Art. 28 Rechtsansprüche

Artikel 28 regelt die Rechtsansprüche, welche die betroffene Person gegenüber privaten Personen geltend machen kann.

Abs. 1 Berichtigung

Absatz 1 hält fest, dass jede Person die Berichtigung unrichtiger Personendaten verlangen kann. Dieser Anspruch ist bislang in Artikel 5 Absatz 2 DSG enthalten. Er wird im E-DSG mit allen anderen Rechtsansprüchen in einer Bestimmung zusammengeführt. Die Berichtigung kann bedeuten, dass die fehlenden Daten ergänzt oder die falschen Daten gelöscht und gegebenenfalls durch neue, richtige Daten ersetzt werden.

Wie aus dem separaten Absatz deutlich wird, besteht der Berichtigungsanspruch unabhängig von einer Personlichkeitsverletzung nach Artikel 26 E-DSG. Ebenfalls können die Rechtfertigungsgründe von Artikel 27 E-DSG nicht geltend gemacht

werden. Vielmehr sieht Absatz 1 zwei eigenständige Ausnahmen vor, die eine Berichtigung ausschliessen.

Nach Buchstabe a ist die Berichtigung unrichtiger Daten ausgeschlossen, wenn eine gesetzliche Vorschrift die Änderung der Personendaten ausschliesst. Zu denken ist hierbei an gesetzliche Bearbeitungs- und Aufbewahrungspflichten, nach denen private Verantwortliche Daten unverändert belassen müssen.

Buchstabe b erlaubt eine Interessenabwägung in Bezug auf Daten Archivbeständen, die ausschliesslich zu diesem Zweck bearbeitet werden und bei denen ein überwiegendes öffentliches Interesse daran besteht, dass die Daten unverändert bestehen bleiben. Diese Ausnahme erfasst beispielsweise private Bibliotheken.

Abs. 2 Klagen

Absatz 2 enthält die Verweisung auf die Klagen nach Artikel 28 ff. ZGB, welche bereits im bisherigen Recht besteht. Analog zu Artikel 28*a* Absatz 1 ZGB hält dieser Absatz zudem einzelne spezifische Ansprüche fest, welche die betroffene Person geltend machen kann. Der Klarheit halber sind diese im Entwurf neu mit einer Aufzählung besser hervorgehoben. Diese Aufzählung konkretisiert insbesondere die Unterlassungs- und Beseitigungsklage nach Artikel 28*a* Absatz 1 Ziffer 1 und 2 ZGB in Bezug auf den Datenschutz. Nach Buchstabe a kann die betroffene Person verlangen, dass die Datenbearbeitung verboten wird. Nach Buchstabe b kann sie beantragen, dass die Bekanntgabe von Daten an Dritte untersagt wird. Gemäss Buchstabe c kann sie schliesslich die Löschung oder Vernichtung von Daten verlangen.

Obschon es sich implizit bereits aus dem bisherigen Recht ergibt, wird im E-DSG ausdrücklich ein Recht auf Löschung formuliert. Es entspricht den Anforderungen von Artikel 8 Buchstabe e E-SEV 108. Der Artikel 17 der Verordnung (EU) 2016/679 enthält eine ähnliche Regelung. Dieses Recht auf Löschung entspricht im Bereich des Datenschutzes dem «Recht auf Vergessenwerden», wie es generell aus dem zivilrechtlichen Persönlichkeitsschutz abgeleitet wird.[169] Demnach wäre auch in der Schweiz beispielsweise ein ähnlicher Entscheid möglich, wie ihn der Europäische Gerichtshof gegenüber Google gefällt hat.[170] Ein solches Recht auf Vergessenwerden gilt indessen nicht absolut.[171] Vielmehr wird in der Rechtsprechung zum Persönlichkeitsschutz grundsätzlich das Interesse der betroffenen Person abgewogen gegen die Meinungs- und Informationsfreiheit, aus denen sich regelmässig ein überwiegendes Interesse am Fortbestehen bzw. an der Verwendung der Information ergibt. Ein solches Interesse kann beispielsweise bestehen bei Archiven oder Bibliotheken, deren Aufgabe es ist, Dokumente unverändert zu sammeln, zu erschliessen, zu erhalten und zu vermitteln. Besteht ein überwiegendes Interesse, ist die Persönlichkeitsverletzung gerechtfertigt und ein allfälliger Anspruch auf Löschung entfällt. Die notwendige Interessenabwägung im Einzelfall ist aufgrund von Artikel 28 Absatz 2 E-DSG sowie der Verweisung auf die Klagen nach Artikel 28 f. ZGB möglich und erforderlich, sodass keine spezifischen Vorbehalte in den Gesetzestext

169 Vgl. hierzu insbesondere BGE **109** II 353; **111** II 209 sowie **122** III 449.
170 Vgl. Urteil Rs. C-131/12 (Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González) vom 13.5.2014, ECLI:EU:C:2014:317.
171 BGE **111** II 209 E. 3c.

eingefügt werden müssen.[172] Der Beauftragte hätte es vorgezogen, wenn ausdrücklich ein Auslistungsrecht («Recht auf Vergessenwerden») eingefügt worden wäre.

Abs. 3 Bestreitungsvermerk

Absatz 3 enthält den so genannten Bestreitungsvermerk, der unverändert aus dem bisherigen Recht übernommen wird. Demnach kann bei Daten ein entsprechender Vermerk angebracht werden, wenn weder die Richtigkeit noch die Unrichtigkeit der Daten festgestellt werden kann. Die Bestimmung ist vor dem Hintergrund zu betrachten, dass sich die Unrichtigkeit von Tatsachenbehauptungen, gerade wenn sie mit Werturteilen verknüpft sind, mitunter nicht ausreichend nachweisen lässt. Die betroffene Person erhält auf diese Weise zumindest einen teilweisen Rechtsschutz.

Abs. 4 Mitteilung an Dritte oder Veröffentlichung

Absatz 4 sieht wie das bisherige Recht vor, dass das Urteil, die Berichtigung, die Löschung oder Vernichtung, das Verbot der Bearbeitung bzw. der Bekanntgabe an Dritte oder der Bestreitungsvermerk Dritten mitgeteilt wird oder veröffentlicht wird. Diese Regelung konkretisiert Artikel 28*a* Absatz 2 ZGB im Bereich des Datenschutzes.

Aufgehoben wird hingegen die Bestimmung betreffend das vereinfachte Verfahren für Auskunftsbegehren. Diese Regelung ist mit Einführung der ZPO obsolet geworden, weil sämtliche Vorschriften zu zivilrechtlichen Verfahren nun in der ZPO enthalten sind. Diese regelt das anwendbare Verfahren (Art. 243 Abs. 2 Bst. d E-ZPO) sowie den Gerichtsstand (Art. 20 Bst. d E-ZPO).

9.1.7 Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane

Art. 29 Kontrolle und Verantwortung bei gemeinsamer Bearbeitung von Personendaten

Im Vergleich zu Artikel 16 DSG erfährt Artikel 29 E-DSG wenige Änderungen.

Artikel 16 Absatz 1 DSG wird aufgehoben. Die Verantwortlichkeit des Bundesorgans, das Personendaten bearbeitet oder bearbeiten lässt, ergibt sich aus der Definition des Begriffs «Verantwortlicher» (Art. 4 Bst. i E-DSG).

Mit Artikel 29 E-DSG wird ferner aus redaktionellen Gründen der Ausdruck «besonders regeln» von Artikel 16 Absatz 2 DSG weggelassen. Darüber hinaus soll der Bundesrat nicht nur die Möglichkeit haben, besondere Regeln über die Kontrolle und Verantwortung für den Datenschutz zu erlassen, wenn Bundesorgane Daten zusammen mit anderen Behörden oder Privatpersonen bearbeiten, sondern dazu verpflichtet sein. Mit dieser Änderung wird Artikel 21 der Richtlinie (EU) 2016/680 umgesetzt. Artikel 26 der Verordnung (EU) 2016/679 sieht eine analoge Regelung vor.

[172] Artikel 38 sieht die Möglichkeit einer solchen Abwägung nicht vor, weswegen dort ein Vorbehalt in Absatz 5 gemacht wird.

Art. 30 Rechtsgrundlagen

Um der Kritik in der Lehre betreffend die Abgrenzung der Ausnahmen in Artikel 17 Absatz 2 DSG und Artikel 19 Absatz 2 DSG Rechnung zu tragen, regelt der E-DSG in Artikel 30 Absatz 2 die gesetzliche Grundlage für bestimmte Datenbearbeitungen. In Absatz 4 sind die Ausnahmen zu den Anforderungen an die gesetzliche Grundlage vorgesehen.

Abs. 1 Gesetzliche Grundlage

Absatz 1 übernimmt den Grundatz von Artikel 17 Absatz 1 DSG, wonach die Bundesorgane Personendaten unter Vorbehalt bestimmter Ausnahmen nur bearbeiten dürfen, wenn hierfür eine gesetzliche Grundlage vorliegt.

Abs. 2 Grundlage in Gesetz im formellen Sinn

Wie nach geltendem Recht schreibt Absatz 2 Buchstabe a vor, dass für die Bearbeitung besonders schützenswerter Daten eine Grundlage in einem Gesetz im formellen Sinn erforderlich ist.

Nach Absatz 2 Buchstabe b sind die Bundesorgane ausschliesslich dann zum Profiling im Sinne von Artikel 4 Buchstabe f E-DSG befugt, wenn dies in einer Grundlage in einem Gesetz im formellen Sinn vorgesehen ist. Die Bestimmung ersetzt insofern Artikel 17 Absatz 2 DSG, nach welchem Persönlichkeitsprofile nur bearbeitet werden dürfen, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht. Aufgrund des Risikos eines Eingriffs in die Grundrechte der betroffenen Personen ist der Bundesrat der Meinung, dass die Rechtsgrundlage für das Profiling auf derselben Stufe bestehen muss wie im Fall der Bearbeitung besonders schützenswerter Daten. Wie in den Erläuterungen zu Absatz 3 dargelegt wird, gilt die Anforderung einer Grundlage in einem Gesetz im formellen Sinn für derartige Datenbearbeitungen nicht absolut. Es wird folglich dem Gesetzgeber obliegen, in jedem Bereich zu bestimmen, ob eine formell-gesetzliche Grundlage in einem bereichsspezifischen Gesetz geschaffen werden muss oder ob eine Grundlage in einem Gesetz im materiellen Sinn genügt. Es ist denkbar, dass ein Profiling in bestimmten Fällen keine besonderen Risiken für die Grundrechte der betroffenen Person birgt.

Nach Absatz 2 Buchstabe c ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich, wenn der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen kann. Dieser Fall ist in Artikel 17 Absatz 2 DSG nicht ausdrücklich festgehalten. Es handelt sich aber nicht um eine neue Anforderung, denn nach Artikel 36 Absatz 1 BV bedürfen schwerwiegende Einschränkungen von Grundrechten einer gesetzlichen Grundlage in einem Gesetz im formellen Sinn. Buchstabe c ist jedoch notwendig, da in mehreren Bundesgesetzen der Begriff «Persönlichkeitsprofil» und die entsprechenden Gesetzesgrundlagen aufgehoben werden. Denn aus Sicht des Bundesrates darf die Aufhebung des Begriffs «Persönlichkeitsprofil» nicht dazu führen, dass die Anforderungen an die Stufe der gesetzlichen Grundlage gesenkt werden.

Ein schwerwiegender Eingriff in die Grundrechte der betroffenen Person kann sich aus dem Zweck der Bearbeitung von Personendaten ergeben (erster Anwendungsfall

von Bst. c). Denn in bestimmten Bereichen müssen die Bundesorgane eventuell bestimmte Personendaten bearbeiten, damit sie beispielsweise die Gefährlichkeit, das Potenzial für eine Funktion, die Eignung für die Erfüllung einer gesetzlichen Pflicht oder die Lebensführung einer Person beurteilen können. Je nach Zweck, den das Bundesorgan mit der Bearbeitung verfolgt, kann diese – unabhängig von der Art der bearbeiteten Daten – die Grundrechte der betroffenen Person in schwerwiegender Weise einschränken. Wenn dies zutrifft, ist es gerechtfertigt, dass für die Bearbeitung der Personendaten auf der gleichen Stufe eine gesetzliche Grundlage bestehen muss wie für die Bearbeitung besonders schützenswerter Personendaten.

Ein schwerwiegender Eingriff in die Grundrechte der betroffenen Person kann sich ausserdem aus der Art und Weise der Datenbearbeitung ergeben (zweiter Anwendungsfall von Bst. c). Dies trifft insbesondere auf automatisierte Einzelentscheidungen nach Artikel 19 Absatz 1 E-DSG zu. Zwar birgt nicht jede automatisierte Einzelentscheidung ein schwerwiegendes Risiko für die Grundrechte der betroffenen Person, sodass für gewisse solcher Entscheidungen auch eine Grundlage in einem Gesetz im materiellen Sinn genügen kann. Eine Ermächtigung durch ein Gesetz im formellen Sinn ist grundsätzlich dann erforderlich, wenn die automatisierte Einzelentscheidung auf der Grundlage besonders schützenswerter Personendaten erfolgt. Damit wird auch den Anforderungen von Artikel 11 der Richtlinie (EU) 2016/680 Rechnung getragen.

Abs. 3 Ausnahmen von der Anforderung einer Grundlage in einem Gesetz im formellen Sinn

Diese Bestimmung ermächtigt den Bundesrat, für die Bearbeitung besonders schützenswerter Personendaten und das Profiling eine Grundlage in einem Gesetz im materiellen Sinn zu erlassen, wenn zwei Voraussetzungen kumulativ erfüllt sind. Nach Buchstabe a muss die Bearbeitung unentbehrlich sein für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe. Damit diese Voraussetzung erfüllt ist, muss auf Gesetzesebene die Natur der Aufgaben, welche die Bearbeitung von Personendaten erfordern, ausreichend konkretisiert sein. Die zweite Voraussetzung (Absatz 3 Buchstabe b) ist neu. Sie hat den Vorteil, dass sie die Tragweite von Absatz 3 auf präzisere Weise einschränkt als die aktuelle Regelung in Artikel 17 Absatz 2 Buchstabe a DSG. Letztere ist nur ausnahmsweise anwendbar, was auch dazu führen kann, dass der Ermessensspielraum dazu genutzt wird, Ausnahmefälle anzunehmen, wo gar keine vorliegen.

Die Senkung der Anforderungen an die Stufe der Gesetzesgrundlage ist insbesondere für besonders schützenswerte Personendaten angebracht, die ausnahmsweise in Bundesrats-, Departements- und Amtsgeschäften bearbeitet werden (z. B. Beschwerdeentscheide; Staatshaftungsfälle; Bundespersonalgeschäfte). Auch dies erfordert, streng genommen, nach dem geltenden Artikel 17 Absatz 1 DSG eine formell-gesetzliche Grundlage. Indessen soll nach Artikel 30 Absatz 3 E-DSG eine Grundlage in einem Gesetz im materiellen Sinn genügen, wenn die Bearbeitung für die Erfüllung einer formell-gesetzlich vorgesehenen Aufgabe unentbehrlich ist und der Bearbeitungszweck für die Grundrechte der betroffenen Person keine besonderen Risiken birgt. Soweit diese Kriterien erfüllt sind und der Zugriff auf diese Daten

stark eingeschränkt ist, wird künftig eine Grundlage in einem Gesetz im materiellen Sinn grundsätzlich genügen.

Abs. 4 Ausnahmen

Gemäss Absatz 4 kann von der Anforderung der gesetzlichen Grundlage (Abs. 1–3) abgewichen werden, wenn eine der Voraussetzungen nach den Buchstaben a bis c erfüllt ist.

Buchstabe a regelt den Entscheid des Bundesrates, der dem Bundesorgan ausnahmsweise erlaubt, Personendaten ohne gesetzliche Grundlage zu bearbeiten. Buchstabe a entspricht der Ausnahme nach Artikel 17 Absatz 2 Buchstabe b DSG.

Gemäss Buchstabe b können Bundesorgane Personendaten ohne gesetzliche Grundlage bearbeiten, wenn die betroffene Person im Einzelfall ihre Einwilligung gemäss Artikel 5 Absatz 6 E-DSG gibt oder wenn sie ihre Personendaten allgemein zugänglich gemacht und die Bearbeitung nicht ausdrücklich untersagt hat. Diese Bestimmung entspricht im Wesentlichen der Ausnahme nach Artikel 17 Absatz 2 Buchstabe c DSG.

Buchstabe c ist eine neue Ausnahme, die in Artikel 17 Absatz 2 DSG nicht enthalten ist. Sie entspricht Artikel 10 Buchstabe b der Richtlinie (EU) 2016/680 und Artikel 6 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679. Demnach ist die Bearbeitung ebenfalls zulässig, wenn sie notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, wenn es nicht möglich ist, die Einwilligung der betroffenen Person innert angemessener Frist einzuholen.

Art. 31 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen

Die vorliegenden Änderungen des aktuellen Artikels 17*a* DSG sollen nicht die Voraussetzungen abschwächen, unter denen ein Bundesorgan vor Inkrafttreten eines Gesetzes im formellen Sinn im Rahmen eines Pilotversuchs Daten automatisiert bearbeiten kann. Es soll lediglich die Regelungsdichte reduziert werden. Denn seit dem Inkrafttreten dieser Norm haben die Bundesorgane nur selten darauf zurückgegriffen. Gewisse Bestimmungen von Artikel 17*a* DSG können zudem in die künftigen Ausführungsverordnung aufgenommen werden.

Abgesehen davon, dass der Begriff «Persönlichkeitsprofile» durch «andere Datenbearbeitungen nach Artikel 30 Absatz 2 Buchstaben b und c» ersetzt wird, stimmen die Voraussetzungen nach den Absätzen 1 und 2 mit jenen von Artikel 17*a* Absatz 1 DSG weitgehend überein. Ausserdem wird in Buchstabe c präzisiert, dass eine Testphase «insbesondere aus technischen Gründen» erforderlich ist. Diese Änderung ist durch die Aufhebung von Artikel 17*a* Absatz 2 DSG begründet, der die Fälle aufzählt, in denen die praktische Umsetzung einer Datenbearbeitung zwingend eine Testphase erfordern kann. Aus den hiervor aufgeführten Gründen können diese Fälle in einer Ausführungsverordnung geregelt werden.

Die Absätze 3 und 4 bleiben, von der Aufhebung des Begriffs «Persönlichkeitsprofile» und einigen redaktionellen Änderungen abgesehen, im Vergleich zum geltenden Recht unverändert.

Art. 32 Bekanntgabe von Personendaten

Artikel 32 E-DSG behält den Grundsatz von Artikel 19 DSG bei, wonach Bundesorgane Personendaten im Prinzip nur bekannt geben dürfen, wenn dafür eine Rechtsgrundlage besteht. Er präzisiert aber, dass der Begriff der Rechtsgrundlage dem Begriff nach Artikel 30 Absätze 1–3 E-DSG entspricht. Aus dieser Präzisierung folgt, dass Artikel 32 nicht auf die in Artikel 30 Absatz 4 vorgesehenen Ausnahmen verweist. Dementsprechend sind die Fälle, in denen Bundesorgane befugt sind, Personendaten ohne gesetzliche Grundlage bekannt zu geben, in Artikel 32 Absatz 2 Buchstaben a–e E-DSG abschliessend aufgezählt. Mit dieser Änderung wird der Kritik in der Lehre betreffend die Abgrenzung der Ausnahmen in Artikel 17 Absatz 2 DSG und Artikel 19 Absatz 2 DSG Rechnung getragen.

Der Begriff der «Personendaten» in Absatz 1 umfasst auch besonders schützenswerte Personendaten. Verlangt Artikel 30 für die Bearbeitung einer bestimmten Kategorie von Personendaten (besonders schützenswerte Personendaten) oder bestimmte Bearbeitungen (Profiling, Bearbeitungen nach Art. 30 Abs. 2 Bst. c) eine Grundlage in einem Gesetz im formellen Sinn, so gilt dies auch betreffend die Vorschriften für die Bekanntgabe der fraglichen Personendaten. Die Bekanntgabe von Personendaten ist an sich ein besonders sensibler Vorgang, sodass in diesem Bereich nicht unerheblich sein kann, auf welche Weise die bekanntgegebenen Daten gewonnen werden. Erfolgt daher eine Bekanntgabe im Nachgang zu einer der besonders heiklen Bearbeitungsarten, ist dies in einem Gesetz im formellen Sinn vorzusehen. Die Ausnahmen von Absatz 2 gelten auch, wenn ein Bundesorgan beabsichtigt, diese Art von Daten bekannt zu geben.

Die Ausnahme nach Absatz 2 Buchstabe a wird erweitert. Bisher durften Bundesorgane Daten im Einzelfall ohne gesetzliche Grundlage bekannt geben, wenn die Bekanntgabe der Daten für den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich war. Neu dürfen sie es auch dann tun, wenn dies für sie selbst zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich ist.

Buchstabe c ist eine neue Ausnahme, die in Artikel 19 Absatz 1 DSG nicht vorgesehen ist. Sie wird auch in den Artikel 30 Absatz 4 Buchstabe c E-DSG eingefügt.

Artikel 32 Absatz 3 E-DSG entspricht mit Ausnahme einer punktuellen Änderung Artikel 19 Absatz 1bis DSG. Mit einer Anpassung des Wortlauts von Artikel 32 Absatz 3 soll die Koordination zwischen BGÖ und DSG verbessert werden. Dabei ist bezüglich der Voraussetzung des überwiegenden öffentlichen Interesses an der Datenbekanntgabe (Art. 32 Abs. 3 Bst. b E-DSG) klarzustellen, dass diese Voraussetzung nicht nur zusätzlich (alternativ), sondern auch selbstständig zu Artikel 32 Absätze 1 und 2 gilt. Vorgeschlagen wird, im Einleitungssatz von Artikel 32 Absatz 3 E-DSG den Ausdruck «auch» (für den es in der französischen Version keine Entsprechung gibt) durch ein «darüber hinaus/en outre» zu ersetzen, um deutlich zu machen, dass die Rechtsgrundlage nach Absatz 3 zu denen in den Absätzen 1 und 2 dazukommt.

Artikel 32 Absatz 4 bleibt im Vergleich zu Artikel 19 Absatz 2 DSG unverändert. Die Erläuterungen in der Botschaft des Bundesrates vom 23. März 1988[173] behalten ihre Gültigkeit.

Dagegen wird die gesetzliche Grundlage für «Abrufverfahren» (Art. 19 Abs. 3 DSG) bei Bundesorganen aufgehoben, weil sie im digitalen Zeitalter überholt erscheint. Diese Änderung führt nicht zu einer Schwächung des Schutzes der Personendaten, denn die Bekanntgabe muss immer im Rahmen der gesetzlichen Datenschutzvorschriften erfolgen. Die Anpassungen der bereichsspezifischen Datenschutzbestimmungen, die sich aus der Aufhebung von Artikel 19 Absatz 3 ergeben, erfolgen kontinuierlich im Rahmen von Revision der jeweiligen Erlasse.

Die Absätze 5 und 6 entsprechen den Absätzen 3bis und 4 von Artikel 19 DSG.

Art. 33 Widerspruch gegen die Bekanntgabe von Personendaten

Diese Bestimmung bleibt, von einigen redaktionellen Änderungen abgesehen, im Vergleich zum geltenden Recht (Artikel 20 DSG) unverändert. In der deutschen Fassung wird der Ausdruck «Sperrung der Bekanntgabe» in Anlehnung an die europäische Terminologie durch «Widerspruch gegen die Bekanntgabe» ersetzt.

Nach der Ansicht des Beauftragten müsste sich das Recht auf Widerspruch nicht nur auf die Datenbekanntgabe, sondern auch auf die Datenbearbeitung beziehen.

Art. 34 Angebot von Unterlagen an das Bundesarchiv

Diese Bestimmung entspricht Artikel 21 DSG. Sie bleibt materiell unverändert.

Art. 35 Bearbeiten für Forschung, Planung und Statistik

Diese Bestimmung entspricht weitgehend Artikel 22 DSG.

Darüber hinaus wird in Absatz 1 ein neuer Buchstabe b eingefügt, wonach Bundesorgane privaten Dritten besonders schützenswerte Personendaten so bekannt geben müssen, dass die betroffene Person nicht bestimmbar ist. Dies soll den Schutz besonders schützenswerter Personendaten stärken. Diese Voraussetzung ist ebenfalls erfüllt, wenn die Weitergabe in pseudonymisierter Form erfolgt und der Schlüssel bei der weitergebenden Person verbleibt (faktische Anonymisierung).

Absatz 2 wird zudem betreffend die Verweisungen auf die Artikel 5 Absatz 3, 30 Absatz 2 und 32 Absatz 1 E-DSG geändert.

Art. 36 Privatrechtliche Tätigkeit von Bundesorganen

Diese Bestimmung entspricht Artikel 23 Absatz 1 DSG. Artikel 23 Absatz 2 DSG kann aufgehoben werden, da im E-DSG für private Personen und Bundesorgane dasselbe Aufsichtssystem vorgesehen ist.

173 BBl **1988** II 471

Art. 37 Ansprüche und Verfahren

Im Vergleich mit Artikel 25 DSG erfährt Artikel 37 E-DSG einige Änderungen, die nachfolgend erklärt werden.

Abs. 1 Begehren

Diese Bestimmung regelt die Begehren, die die betroffenen Personen an Bundesorgane richten können. Im Vergleich mit Artikel 25 Absatz 1 DSG wird sie nicht geändert.

Abs. 2 Weitere Begehren

Heute ergibt sich der Anspruch der betroffenen Person, die Löschung ihrer Daten zu verlangen, implizit aus Artikel 25 DSG. Um die Anforderungen von Artikel 8 Buchstabe e E-SEV 108 und von Artikel 16 der Richtlinie (EU) 2016/680 zu berücksichtigen, wird dieser Anspruch nun ausdrücklich in Artikel 37 Absatz 2 Buchstaben a und b genannt. Artikel 17 der Verordnung (EU) 2016/679 sieht seinerseits das Recht der betroffenen Person vor, unter bestimmten Bedingungen die Löschung der sie betreffenden Daten zu verlangen («Recht auf Vergessenwerden»). Derselbe Anspruch wird in Artikel 28 E-DSG eingeführt, sodass die Regelung gegenüber privaten und öffentlichen Verantwortlichen übereinstimmt (vgl. Ziff. 9.1.6). An der konkreten Rechtslage ändert sich indessen nichts.

In Absatz 2 Buchstabe a wird im Vergleich zu Artikel 25 Absatz 3 Buchstabe 3 DSG der letzte Teilsatz betreffend die Sperrung der Bekanntgabe an Dritte gelöscht, weil der Widerspruch gegen die Bekanntgabe von Daten abschliessend durch Artikel 33 E-DSG geregelt ist.[174] Der Widerspruch nach Artikel 33 E-DSG ist nicht an die widerrechtliche Bearbeitung gebunden, was bei den Ansprüchen nach Artikel 37 der Fall ist.

Beibehalten wird allerdings in Buchstabe b dieser Bestimmung die Möglichkeit, dass die betroffene Person vom Bundesorgan verlangen kann, den Entscheid über den Widerspruch gegen die Bekanntgabe nach Artikel 33 zu veröffentlichen. Artikel 33 sieht dies nicht vor, aber es erscheint sinnvoll, dass die betroffene Person dies zumindest im Falle der widerrechtlichen Bekanntgabe verlangen kann.

Abs. 3 Einschränkung der Bearbeitung

In Absatz 3 ist eine Massnahme vorgesehen, die weniger radikal ist als die Löschung oder Vernichtung der bestrittenen Personendaten: die Einschränkung der Bearbeitung.

Diese Regelung entspricht Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680, nach dem der Verantwortliche die Bearbeitung einschränken kann, anstatt die bestrittenen Daten zu löschen, wenn die betroffene Person die Richtigkeit der Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann oder wenn Daten für Beweiszwecke weiter aufbewahrt werden müssen.

174 Vgl. hierzu Bangert Jan, Kommentar zu Art. 25/25bis DSG, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Auflage, Basel 2014, N 62 f.

Artikel 18 der Verordnung (EU) 2016/679 geht weiter, da die betroffene Person gemäss dieser Bestimmung einen Anspruch hat, die Einschränkung der Bearbeitung zu verlangen.

Im E-SEV 108 hingegen ist die Einschränkung der Bearbeitung nicht enthalten.

Absatz 3 ist in dem Sinne auszulegen, dass die Daten weiter bearbeitet werden dürfen, jedoch nur zu bestimmten Zwecken. Es geht nicht darum, jegliche Art der Datenbearbeitung auszuschliessen. Gemäss dem Erwägungsgrund 47 der Richtlinie (EU) 2016/680 ist die Einschränkung der Bearbeitung so zu verstehen, dass das Bundesorgan die betreffenden Daten nur zu dem Zweck bearbeiten darf, der ihrer Löschung entgegenstand. Absatz 3 sieht dafür vier Konstellationen vor.

Nach Absatz 3 Buchstabe a muss das Bundesorgan die Bearbeitung der Personendaten einschränken, wenn die betroffene Person die Richtigkeit der Personendaten bestreitet und weder deren Richtigkeit noch Unrichtigkeit festgestellt werden kann. In diesem Fall bedeutet die Einschränkung der Bearbeitung, dass das Bundesorgan die bestrittenen Daten ausschliesslich zum Zweck bearbeiten darf, deren Richtigkeit oder Unrichtigkeit festzustellen. Sobald die Richtigkeit der Daten feststeht, darf das Bundesorgan die Bearbeitung ohne Einschränkungen fortsetzen. Erweisen sich die Personendaten jedoch als unrichtig, so muss das Bundesorgan sie löschen oder vernichten, sofern im betreffenden Fall nicht Buchstabe b oder c anwendbar ist.

Absatz 3 Buchstabe b schreibt vor, dass das Bundesorgan die Bearbeitung einschränken muss, wenn überwiegende Interessen eines Dritten dies erfordern, zum Beispiel wenn die Löschung oder Vernichtung bestimmter Daten eine dritte Person daran hindern könnte, ihre Rechte vor Gericht auszuüben. Das bedeutet, dass die Daten weiter bearbeitet werden dürfen, jedoch nur, damit der betroffene Dritte seine Rechte ausüben kann. Jede Bearbeitung zu einem anderen Zweck ist ausgeschlossen.

Nach Absatz 3 Buchstabe c muss das Bundesorgan die bestrittenen Daten nicht löschen oder vernichten, wenn dies ein überwiegendes öffentliches Interesse, namentlich die innere oder äussere Sicherheit der Schweiz, gefährden könnte.

Absatz 3 Buchstabe d schliesslich hält fest, dass das Bundesorgan die Daten nicht löschen oder vernichten muss, wenn dies eine Ermittlung, Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden kann. In diesem Fall darf das Bundesorgan die Personendaten weiterhin bearbeiten, jedoch ausschliesslich zu dem Zweck, der ihrer Löschung entgegenstand, d. h. zur Fortsetzung einer Ermittlung, einer Untersuchung oder eines Verfahrens.

Die Einschränkung der Bearbeitung bedeutet, dass die bestrittenen Daten gekennzeichnet werden, damit ihre künftige Bearbeitung ausschliesslich zum Zweck erfolgt, der ihrer Löschung oder Vernichtung entgegenstand. Die Kennzeichnung muss klar sein. Sie kann in der Praxis bedeuten, dass die bestrittenen Daten vorübergehend in ein anderes Bearbeitungssystem verschoben werden oder dass den Benutzerinnen und Benutzern der Zugriff auf die Daten verunmöglicht wird. In Systemen für eine automatisierte Datenbearbeitung sollte die Einschränkung der Bearbeitung grundsätzlich mit technischen Mitteln gewährleistet werden, sodass die Daten nicht zu anderen Zwecken als jenen nach Absatz 3 weiter bearbeitet oder verändert werden können.

Abs. 4 Bestreitungsvermerk

Diese Bestimmung enthält den sogenannten Bestreitungsvermerk, der unverändert aus dem bisherigen Recht (Art. 25 Abs. 2 DSG) übernommen wurde. Demnach kann bei Daten ein entsprechender Vermerk angebracht werden, wenn weder die Richtigkeit noch die Unrichtigkeit der Daten endgültig festgestellt werden kann.

Abs. 5 Bestände öffentlicher Gedächtnisinstitutionen

Nach Absatz 5 kann die Berichtigung, Löschung oder Vernichtung von Daten nicht verlangt werden in Bezug auf die Bestände von öffentlich zugänglichen Bibliotheken, Bildungseinrichtugen, Museen, Archiven oder anderen öffentlichen Gedächtnisinstitutionen. Die Ausnahme hat insofern eine beschränkte Tragweite, als viele dieser Insitutionen unter das kantonale Datenschutzrecht fallen. Die Bestimmung bezieht sich auf öffentliche Institutionen, deren Tätigkeit insbesondere darin besteht, Dokumente aller Art (auch digitale) zu sammeln, zu erschliessen, zu erhalten und zu vermitteln. Diesem spezifischen Bearbeitungszweck würde eine Berichtigung, Löschung oder Vernichtung entgegenstehen, soweit sie sich auf die Archivbestände solcher Institutionen bezieht. Auch der Bestreitungsvermerk nach Absatz 4 dieses Artikels kommt nicht zur Anwendung. Denn diese Bestände sollen mittels Dokumenten einen Moment in der Vergangenheit abbilden, was nur möglich ist, wenn diese Dokumente originalgetreu und damit unverändert im Archiv enthalten sind. Daran besteht ein erhebliches öffentliches Interesse, das sich aus der Informationsfreiheit (Art. 16 Abs. 3 BV) ergibt.

Der zweite Satz in Absatz 5 ermöglicht es jedoch der betroffenen Person, zu verlangen, dass die fragliche Institution den Zugang zu den umstrittenen Daten beschränkt. Hierfür muss die betroffene Person jedoch ein überwiegendes Interesse glaubhaft machen. Diese Ausnahme ist insbesondere im Hinblick auf die zunehmende Tendenz zu betrachten, umfangreiche Bestände öffentlich zugänglicher Gedächtnisinstitutionen für jedermann im Internet zugänglich zu machen. Dadurch reduziert sich der Aufwand für gezielte Recherchen, während gleichzeitig der Kreis der Personen, die auf den fraglichen Bestand zugreifen können, erheblich erweitert wird. Das Gesetz muss daher für solche Fälle eine differenzierte Interessenabwägung erlauben. Dabei stehen sich das öffentliche Interesse an einem unverfälschten und uneingeschränkten Zugang zu Dokumenten und das Interesse der betroffenen Person gegenüber, dass unwahre oder persönlichkeitsverletzende Informationen über sie nicht allgemein zugänglich sind. Wie sich aus Satz 1 von Absatz 5 ergibt, geht in Bezug auf Archive und ähnliche Institutionen das öffentliche Interesse am freien und unverfälschten Zugang grundsätzlich vor. Ein überwiegendes Interesse der betroffenen Person ist hingegen nur anzunehmen, wenn ihr aufgrund des freien Zugangs erhebliche persönliche Nachteile erwachsen, die sie auch in der Zukunft wesentlich einschränken können (z. B. in ihrem beruflichen Fortkommen). Diese Nachteile sind zudem in Beziehung zu setzen zum archivarischen Wert der umstrittenen Daten, der sich beispielsweise aus der historischen Bedeutung, der Art oder dem Inhalt des Dokuments ergeben kann. Ein überwiegendes Interesse auf Seiten der betroffenen Person ist namentlich dann anzunehmen, wenn der archivarische Wert der Daten und damit auch die Bedeutung des uneingeschränkten öffentlichen Zugangs als gering erscheint im Verhältnis zu den erheblichen Einschränkungen der betroffenen

Person. In diesem Fall kann die betroffene Person verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt. Die Beschränkung ist im Einzelfall so auszugestalten, dass sie im Hinblick auf die in Frage stehenden Interessen verhältnismässig erscheint. So kann es häufig bereits ausreichen, dass ein Dokument nicht im Internet, sondern nur in physischen Archiven zugänglich ist. In Einzelfallen wäre auch denkbar, den Zugang zu einem Dokument lediglich Personen zu gewähren, die ihn für ihre wissenschaftliche oder journalistische Tätigkeit benötigen.

Nicht unter Absatz 5 fallen hingegen Datenbearbeitungen solcher Institutionen, die nicht im Zusammenhang mit den Beständen stehen und zu anderen Zwecken erfolgen, wie beispielsweise Benutzerkonten der Bibliotheken oder Personaldossiers. Für diese Bearbeitungen stehen der betroffenen Person die Ansprüche in Artikel 37 uneingeschränkt offen.

Art. 38 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten

Diese Bestimmung entspricht Artikel 25bis DSG. Sie bleibt materiell unverändert.

9.1.8 Beauftragte oder Beauftragter

9.1.8.1 Organisation

Art. 39 Ernennung und Stellung

Abs. 1 Ernennungsverfahren

Das Ernennungsverfahren der oder des Beauftragten bleibt nach Absatz 1 unverändert, weil es mit den Anforderungen der Richtlinie (EU) 2016/680 und des E-SEV 108 übereinstimmt. Der E-SEV 108 enthält keine Bestimmung zum Modus für die Wahl oder Ernennung der Aufsichtsbehörde. Artikel 43 der Richtlinie (EU) 2016/680 verpflichtet die Schengen-Staaten zur Regelung des Ernennungsverfahrens, lässt ihnen jedoch die Wahl zwischen einer Ernennung durch das Parlament, die Regierung, das Staatsoberhaupt oder durch eine unabhängige Stelle. In Artikel 53 der Verordnung (EU) 2016/679 ist für die Mitgliedsttaaten der Europäischen Union dieselbe Lösung vorgesehen.

Der Bundesrat hat den Vorschlag verschiedener Vernehmlassungsteilnehmer, eine Wahl durch das Parlament einzuführen, geprüft. Aus folgenden Gründen ist er zum Schluss gekommen, dass diese Änderung nicht angemessen ist. Das aktuelle Verfahren bietet hinreichende Garantien für die Unabhängigkeit der oder des Beauftragten gegenüber der Exekutive. Denn die Bundesversammlung kann die Zustimmung zur Ernennung des Bundesrates verweigern. Der Bundesrat ist auch nicht überzeugt, dass eine Wahl durch das Parlament die Unabhängigkeit der oder des Beauftragten stärken würde. Denn sie könnte durch Interessengruppen beeinflusst werden. Ausserdem bietet die Ernennung durch den Bundesrat unter Vorbehalt der Genehmigung durch das Parlament die Möglichkeit, dass die oder der Beauftragte administrativ weiterhin der Bundeskanzlei angegliedert bleiben kann. Das wäre bei einer Wahl

durch das Parlament nicht mehr möglich. Sollte die oder der Beauftragte nicht mehr Teil der Bundesverwaltung sein, ist nicht ausgeschlossen, dass es für sie oder ihn schwieriger wäre, die Aufsicht über die Bundesorgane wahrzunehmen und sie bei einer Untersuchung zur Mitwirkung zu bewegen. Wenn die oder der Beauftragte durch das Parlament gewählt würde, müsste sie oder er schliesslich auch finanziell unabhängig sein, so wie beispielsweise die Eidgenössische Finanzkontrolle.

Abs. 3 Stellung

Absatz 3 erster Satz konkretisiert die Unabhängigkeit der oder des Beauftragten mit der Präzisierung, dass sie oder er keine Weisungen einer Behörde oder eines Dritten einholen oder erhalten darf. Diese Änderung berücksichtigt die Anforderungen von Artikel 12bis Absatz 4 E-SEV 108 und von Artikel 42 Absätze 1 und 2 der Richtlinie (EU) 2016/680, der denselben Wortlaut hat wie Artikel 52 Absätze 1 und 2 der Verordnung (EU) 2016/679.

Abs. 2, 4 und 5

Diese Bestimmungen bleiben im Verhältnis zum aktuellen Recht (Art. 26 Abs. 2, 4 und 5 DSG) materiell unverändert.

Der Beauftragte ist der Ansicht, dass die Regelung seines Budgets aufgrund seiner Aufsichtsfunktion der Regelung für die Eidgenössische Finanzkontrolle anzugleichen wäre.

Art. 40 Wiederernennung und Beendigung der Amtsdauer

Gegenwärtig kann die oder der Beauftragte für eine unbeschränkte Zahl von Amtsdauern wiedergewählt werden. Dieser Grundsatz wird in Absatz 1 zur Umsetzung der Anforderungen von Artikel 44 Absatz 1 Buchstabe e der Richtlinie (EU) 2016/680 geändert. Dieser sieht vor, dass die Schengen-Staaten regeln müssen, ob und wenn ja wie oft das Mitglied oder die Mitglieder der Aufsichtsbehörde wiederernannt werden können. Gemäss dieser Bestimmung haben die Schengen-Staaten also die Wahl, ob und wie oft eine Wiederernennung der Aufsichtsbehörde möglich ist. Artikel 54 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 enthält eine ähnliche Regelung.

Entsprechend dem Handlungsspielraum, den Artikel 44 der Richtlinie (EU) 2016/680 gewährt, schlägt der Bundesrat vor, dass die oder der Beauftragte zwei Mal wiederernannt werden kann. Diese bzw. dieser kann daher für höchstens zwölf Jahre im Amt bleiben. Durch diese Massnahme soll die Unabhängigkeit der oder des Beauftragten als Behörde gestärkt werden. Sie oder er soll nicht aus Furcht, nicht wiedergewählt zu werden, in der Erfüllung des gesetzlichen Auftrags zurückgehalten werden. Wenn die oder der Beauftragte während der Amtsdauer das Pensionsalter erreicht, endet das Arbeitsverhältnis automatisch bei Erreichen des Alters nach Artikel 21 des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG)[175] (Art. 10 Abs. 1 des Bundespersonalgesetzes vom 24. März 2000 (BPG)[176] in Verbindung mit Art. 14 Abs. 1 BPG).

175 SR **831.10**
176 SR **172.220.1**

Die Absätze 2, 3 und 4 bleiben im Verhältnis zu Artikel 26*a* DSG materiell unverändert.

Art. 41 Nebenbeschäftigung

In Artikel 41 werden die Voraussetzungen für die Ausübung einer Nebenbeschäftigung durch die Beauftragte oder den Beauftragten verschärft. Mit dieser Bestimmung werden die Anforderungen von Artikel 42 Absatz 3 der Richtlinie (EU) 2016/680 umgesetzt, die denselben Wortlaut hat wie Artikel 52 Absatz 3 der Verordnung (EU) 2016/679. Die Bestimmung gilt nur für die oder den Beauftragen. Die Stellvertreterin oder der Stellvertreter sowie das Sekretariat unterstehen dem BPG.

Nach Artikel 26*b* DSG ist lediglich vorgesehen, dass der Bundesrat der oder dem Beauftragten gestatten kann, eine andere Beschäftigung auszuüben, wenn dadurch deren oder dessen Unabhängigkeit und Ansehen nicht beeinträchtigt werden. Artikel 41 Absatz 1 erster Satz hält hingegen den Grundsatz fest, wonach die oder der Beauftragte keine zusätzliche Erwerbstätigkeit ausüben darf. Der zweite Satz präzisiert, dass sie oder er auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden darf. Der Begriff des Kantons ist in einem weiten Sinne zu verstehen und erfasst auch die Gemeinden, Bezirke, Kreise und Körperschaften des öffentlichen Rechts. Absatz 1, zweiter Satz schreibt darüber hinaus vor, dass die oder der Beauftragte auch nicht als Mitglied der Geschäftsleitung, des Verwaltungsrats, oder der Aufsichts- oder Revisionsstelle eines Handelsunternehmens tätig sein darf. Dies gilt unabhängig davon, ob eine solche Tätigkeit vergütet würde oder nicht.

Absatz 2 beschränkt die Tragweite von Absatz 1. Er sieht vor, dass der Bundesrat der oder dem Beauftragten unter bestimmten Voraussetzungen erlauben kann, eine Nebenbeschäftigung auszuüben. Der Entscheid des Bundesrates wird veröffentlicht.

Art. 42 Selbstkontrolle des Beauftragten

Diese Bestimmung verpflichtet den Beauftragten, geeignete Kontrollmassnahmen zu treffen, insbesondere in Bezug auf die Sicherheit der Personendaten und den rechtskonformen Vollzug der bundesrechtlichen Datenschutzvorschriften. Der Bundesrat wird die zu ergreifenden Massnahmen in der künftigen Verordnung konkretisieren.

9.1.8.2 Untersuchung von Verstössen gegen Datenschutzvorschriften

Art. 43 Untersuchung

Nach geltendem Recht unterscheidet sich das Verfahren je nach dem, ob es die Aufsichtstätigkeit des Beauftragten im privaten Sektor oder im öffentlichen Sektor betrifft. Während Artikel 27 DSG dem Beauftragten die Aufgabe überträgt, die Datenbearbeitung durch Bundesorgane zu überwachen, bestimmt Artikel 29 Absatz 1 Buchstaben a–c DSG, dass dieser eine Untersuchung gegen eine Privatperson eröffnet, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen, Datensammlungen gemäss Artikel 11*a* DSG registriert werden müssen oder eine Informationspflicht nach Artikel 6 Absatz 3 besteht. Die Überwachungskompetenzen des Beauftragten gegenüber dem Privatsektor erfüllen derzeit nicht die Anforderungen des E-SEV 108. So sieht deren Artikel 12bis keine Begrenzung der Ermittlungs- und Eingriffsbefugnisse der Aufsichtsbehörde gegenüber den Verantwortlichen vor.

Abs. 1 Eröffnung der Untersuchung

Gemäss Artikel 43 Absatz 1 E-DSG eröffnet der Beauftragte von Amtes wegen oder auf Anzeige hin eine Untersuchung, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Die Anzeige kann durch einen Dritten oder durch die betroffene Person erfolgen. Die Person, die Anzeige erstattet, hat im Verfahren jedoch keine Parteistellung (Art. 46 Abs. 2 e contrario). Falls hingegen die betroffene Person Anzeige erstattet hat, muss der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung informieren (Abs. 4). Die betroffene Person muss ihre Rechte mit den anwendbaren Rechtsmitteln geltend machen, d. h. sie kann bei einem Zivilgericht Klage erheben, wenn der Verantwortliche eine private Person ist, oder sie kann gegen den Entscheid des verantwortlichen Bundesorgans Beschwerde erheben. Dies entspricht dem geltenden Recht.

Abs. 2 Verzicht auf die Eröffnung einer Untersuchung

Der Beauftragte kann von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist. Das wäre etwa der Fall, wenn ein Sport- oder Kulturverein allen seinen Mitgliedern eine E-Mail-Nachricht sendet, ohne die Identität der Empfängerinnen und Empfänger zu verbergen. Absatz 2 kann auch zur Anwendung gelangen, wenn der Beauftragte der Auffassung ist, dass die Beratung des Verantwortlichen ausreicht, um eine an sich kaum problematische Situation zu beseitigen.

Abs. 3 Mitwirkungspflichten

Absatz 3 regelt die Mitwirkungspflichten der privaten Person und des Bundesorgans, indem die Regelung nach den Artikeln 27 Absatz 3 und 29 Absatz 2 DSG übernommen wird. Die Verfahrenspartei hat dem Beauftragten sämtliche Auskünfte zu erteilen und alle Unterlagen zur Verfügung zu stellen, welche dieser für die Untersuchung benötigt. In Absatz 3 zweiter Satz ist festgehalten, dass sich das Auskunfts-

verweigerungsrecht nach den Artikeln 16 und 17 VwVG richtet. Artikel 16 Absatz 1 VwVG verweist auf Artikel 42 Absätze 1 und 3 des Bundesgesetzes vom 4. Dezember 1947[177] über den Bundeszivilprozess. Nach dieser Bestimmung können die befragten Personen das Zeugnis verweigern, wenn die Beantwortung der Frage sie der Gefahr der strafgerichtlichen Verfolgung aussetzen kann. Dabei geht es um die Personen, die die Geheimnisse nach den Artikeln 321, 321bis und 321ter StGB wahren müssen. So können Ärztinnen und Ärzte beispielsweise verweigern, dem Beauftragten Personendaten über ihre Patientinnen und Patienten zu liefern, falls diese dem nicht zustimmen. Dasselbe gilt für die Rechtsanwältinnen und Rechtsanwälte und ihre Kundschaft. Artikel 90 der Verordnung (EU) 2016/679 sieht ebenfalls vor, dass die Mitgliedstaaten die Befugnisse der Aufsichtsbehörden gegenüber den Verantwortlichen oder den Auftragsbearbeitern, die nach innerstaatlichem Recht dem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen, regeln.

Art. 44 Befugnisse

Diese Bestimmung erfüllt die Anforderungen von Artikel 12bis Absatz 2 Buchstabe a E-SEV 108, wonach die Aufsichtsbehörde über Ermittlungs- und Eingriffsbefugnisse verfügen muss. Auch Artikel 47 Absatz 1 der Richtlinie (EU) 2016/680 bestimmt, dass die Schengen-Staaten wirksame Untersuchungsbefugnisse für die Aufsichtsbehörde vorzusehen haben, namentlich die Befugnis, vom Verantwortlichen Zugang zu allen Daten, die verarbeitet werden, und zu allen für die Erfüllung ihrer Aufgaben notwendigen Informationen zu erhalten. Die Verordnung (EU) 2016/679 wiederum sieht in Artikel 58 Absatz 1 Buchstaben e und f eine analoge Regelung vor.

Abs. 1 Untersuchungsmassnahmen

Die Massnahmen nach Absatz 1 dürfen nur angeordnet werden, wenn eine Untersuchung eröffnet worden ist und soweit die private Person oder das Bundesorgan ihren Mitwirkungspflichten nicht nachkommen. Der Beauftragte kann die Massnahmen nach den Buchstaben a–d mit anderen Worten nur anordnen, wenn er vergeblich versucht hat, die Mitwirkung des Verantwortlichen einzuholen.

Der Katalog der Massnahmen nach Absatz 1 gleicht jenem nach Artikel 12 VwVG. Es handelt sich um eine nicht abschliessende Liste. Der Beauftragte ist unter anderem befugt, Zugang zu allen Auskünften, Unterlagen, Bearbeitungsverzeichnissen und Personendaten verlangen, die für die Untersuchung erforderlich sind (Bst. a) oder Zugang zu Räumlichkeiten und Anlagen zu verlangen (Bst. b). Wie alle Bundesbehörden muss er die geltenden Rechtsvorschriften beachten, namentlich jene zum Datenschutz und zur Wahrung von Fabrikations- und Geschäftsgeheimnissen. Er untersteht ausserdem dem Amtsgeheimnis nach Artikel 22 BPG. Folglich ist die vertrauliche Behandlung der Personendaten gewährleistet, zu denen er in Ausübung seiner Aufsichtsaufgaben Zugang erhält , namentlich wenn er die Person, die Anzeige erstattet hat, über das Ergebnis einer allfälligen Untersuchung informiert

177 SR **273**

(Art. 43 Abs. 4) oder wenn er seinen Tätigkeitsbericht nach Artikel 51 E-DSG veröffentlicht.

Abs. 2 Vorsorgliche Massnahmen

Diese Bestimmung verleiht dem Beauftragten die Befugnis, für die Dauer der Untersuchung vorsorgliche Massnahmen anzuordnen und sie durch eine Bundesbehörde oder die kantonalen oder kommunalen Polizeiorgane vollstrecken zu lassen. Der aktuell geltende Artikel 33 Absatz 2 DSG sieht vor, dass der Beauftragte dem Präsidenten der für den Datenschutz zuständigen Abteilung des Bundesverwaltungsgerichts vorsorgliche Massnahmen beantragen kann, wenn er bei einer Untersuchung gegen eine private Person oder gegen ein Bundesorgan feststellt, dass den betroffenen Personen ein nicht leicht wiedergutzumachender Nachteil droht. Da Artikel 45 E-DSG dem Beauftragten Verfügungskompetenzen erteilt, braucht es das Bundesverwaltungsgericht für die Anordnung vorsorglicher Massnahmen nicht mehr und die entsprechende Bestimmung kann demzufolge gestrichen werden. Das Verfahren für Beschwerden gegen vorsorgliche Massnahmen richtet sich nach Artikel 44 ff. VwVG. Die aufschiebende Wirkung der Beschwerde wird durch Artikel 55 VwVG geregelt.

Die neuen Untersuchungsbefugnisse des Beauftragten sind im Hinblick auf Artikel 45 der Verordnung (EU) 2016/679 ein entscheidendes Element, um sicherzustellen, dass die Europäische Kommission den Angemessenheitsbeschluss gegenüber der Schweiz erneuert bzw. aufrechterhält.

Art. 45 Verwaltungsmassnahmen

Artikel 45 E-DSG setzt Artikel 47 Absatz 2 der Richtlinie (EU) 2016/680 um und erfüllt die Empfehlungen der Schengen-Evaluatoren, dem Beauftragten Verfügungskompetenzen zu erteilen. Artikel 58 Absatz 2 der Verordnung (EU) 2016/679 zählt alle Massnahmekompetenzen auf, über welche die Aufsichtsbehörde verfügen sollte. Neben den Massnahmen gemäss Artikel 47 Absatz 2 der Richtlinie (EU) 2016/680 sind dies laut Verordnung namentlich das Verhängen von Verwaltungsbussen (Art. 58 Abs. 2 Bst. i) und die Anordnung, die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation auszusetzen (Bst. j).

Artikel 45 E-DSG entspricht weitgehend den Anforderungen von Artikel 12bis Absatz 2 Buchstabe c und Absatz 6 E-SEV 108.

Allerdings schlägt der Bundesrat vor, dem Beauftragten keine Kompetenz zu geben, Verwaltungssanktionen auszusprechen, sondern ihm vielmehr die Kompetenz zu verleihen, bestimmte Verwaltungsmassnahmen anzuordnen, deren Missachtung strafrechtlich geahndet werden kann (Art. 57 E-DSG).

Artikel 45 E-DSG lässt dem Beauftragten einen grossen Handlungsspielraum. Denn es handelt sich um eine Kann-Bestimmung und er ist nicht verpflichtet, Verwaltungsmassnahmen zu ergreifen. Die Bestimmung umfasst zwei Kategorien von Massnahmen.

Die erste Kategorie besteht aus einer Reihe von Massnahmen gegen Datenbearbeitungen, die gegen die Datenschutzvorschriften verstossen (Abs. 1, 2 und 4). Die

Massnahmen reichen von einer einfachen Verwarnung (Abs. 4) über die Verfügung, Personendaten zu vernichten (Abs. 1) bis hin zum Verbot, Personendaten ins Ausland bekannt zu geben (Abs. 2). Grundsatz dieser Regelung ist die Wahrung der Verhältnismässigkeit. So kann der Beauftragte, anstatt den Abbruch der Bearbeitung anzuordnen, deren Änderung anordnen und die Massnahme nur auf den problematischen Teil der Bearbeitung beschränken. Wenn die Partei des Untersuchungsverfahrens während der Untersuchung die erforderlichen Massnahmen getroffen hat, um die Einhaltung der Datenschutzvorschriften wiederherzustellen, kann der Beauftragte sich auch darauf beschränken, eine Verwarnung auszusprechen (Abs. 4).

Die zweite Massnahmenkategorie betrifft die Fälle, in denen Ordnungsvorschriften oder Pflichten gegenüber der betroffenen Person nicht beachtet werden (Abs. 3). Der Beauftragte kann unter anderem verfügen, dass das Bundesorgan oder die private Person eine Datenschutz-Folgenabschätzung nach Artikel 20 vornimmt (Bst. d) oder der betroffenen Person die Auskünfte nach Artikel 23 erteilt (Bst. g). Die Liste unter Absatz 3 ist nicht abschliessend.

Der Beauftragte informiert ausschliesslich die Parteien des Untersuchungsverfahrens über seinen Entscheid. Gegebenenfalls informiert er gemäss Artikel 51 Abs. 2 E-DSG die Öffentlichkeit. Die ergriffene Massnahme muss ausreichend begründet werden. Der Verantwortliche muss insbesondere in der Lage sein, zu bestimmen, welche Datenbearbeitungen unter den Beschluss des Beauftragten fallen. Die beteiligten Parteien sind berechtigt, gemäss den allgemeinen Bestimmungen über die Bundesrechtspflege Beschwerde zu erheben (vgl. Art. 46). Gegebenenfalls kann der Beauftragte die gegenüber dem Verantwortlichen verfügte Massnahme mit einer Strafdrohung versehen (Art. 57).

Art. 46 Verfahren

Nach Absatz 1 unterstehen das Untersuchungsverfahren sowie jenes zum Erlass der Massnahmen nach den Artikeln 44 und 45 dem Verwaltungsverfahrensgesetz. Die private Person oder das Bundesorgan, die oder das in der Untersuchung Partei ist, hat Anspruch auf Gewährung des rechtlichen Gehörs (Art. 29 ff. VwVG).

Absatz 2 präzisiert, dass nur das Bundesorgan oder die private Person, gegen das bzw. die eine Untersuchung eröffnet wurde, Verfahrenspartei sein kann. Dementsprechend können lediglich diese gegen Verfügungen und Massnahmen, die der Beauftragte gegen sie ergriffen hat, Beschwerde erheben. Die betroffene Person ist nicht Partei, auch wenn der Beauftragte die Untersuchung auf deren Anzeige hin eröffnet hat. Möchte sie Rechtsansprüche gegen einen privaten Verantwortlichen geltend machen, muss sie dies gemäss Artikel 28 E-DSG tun, d. h. vor dem zuständigen Zivilgericht. Im öffentlichen Sektor muss die betroffene Person gegen das verantwortliche Bundesorgan vorgehen (Art. 37), indem sie dessen Entscheid bei der zuständigen Beschwerdeinstanz anficht. Dies bleibt unverändert zum geltenden Recht.

Nach Absatz 3 kann der Beauftragte Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten, wie er dies bereits aktuell gemäss Artikel 27 Absatz 6 und 29 Absatz 4 DSG tun kann.

Art. 47 Koordination

Gewisse Bundesbehörden beaufsichtigen Private oder ausserhalb der Bundesverwaltung stehende Organisationen. Dies ist etwa der Fall des Bundesamts für Gesundheit in Bezug auf die Krankenversicherungen oder der Eidgenössischen Finanzmarktaufsicht (FINMA) in Bezug auf die Banken oder andere Finanzdienstleisterinnen. Der Begriff «Organisationen ausserhalb der Bundesverwaltung» entspricht der in Artikel 1 Absatz 2 Buchstabe e VwVG verwendeten Bezeichnung.

Im Rahmen eines Aufsichtsverfahrens, das allenfalls zu einem Entscheid der zuständigen Behörde führen kann, können sich datenschutzrechtliche Fragen stellen. Um dieser Problematik Rechnung zu tragen, sieht Absatz 1 vor, dass die Aufsichtsbehörde den Beauftragten zur Stellungnahme einlädt. Hat der Beauftragte ebenfalls ein Verfahren nach Artikel 43 E-DSG gegen die selbe Partei eröffnet, müssen sich die Aufsichtsbehörde und der Beauftragte auf zwei Ebenen koordinieren (Abs. 2): Einerseits zur Abklärung, ob die beiden Verfahren parallel geführt werden können oder ob eines der Verfahren suspendiert oder eingestellt werden soll und andererseits für den Inhalt ihres jeweiligen Entscheids, falls die Verfahren parallel geführt werden. Im Fall von Kompetenzkonflikten entscheidet der Bundesrat (Art. 9 Abs. 3 VwVG). Die Koordination muss auf einfache und schnelle Weise sichergestellt werden. Die betroffenen Einheiten müssen über den Ausgang dieser Koordination und die anwendbare Gesetzgebung informiert werden, damit sie möglichst schnell über ihre Rechte und Pflichten im Klaren sind.

9.1.8.3 Amtshilfe

Art. 48 Amtshilfe zwischen schweizerischen Behörden

Diese neue Bestimmung regelt die Amtshilfe zwischen dem Beauftragten sowie den Behörden des Bundes und der Kantone. Der derzeit geltende Artikel 31 Absatz 1 Buchstabe c DSG beschränkt sich darauf, den Beauftragten zur Zusammenarbeit mit den Schweizer Datenschutzbehörden zu verpflichten.

In Absatz 1 des neuen Artikels wird der Grundsatz festgelegt, dass die schweizerischen und kantonalen Behörden dem Beauftragten die Informationen und persönlichen Daten mitzuteilen haben, welche für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Es handelt sich um eine Standardbestimmung zur Amtshilfe, die sich auch in vielen anderen Bundesgesetzen findet.

Absatz 2 bestimmt, dass der Beauftragte Informationen und Daten den für den Datenschutz zuständigen kantonalen Behörden (Bst. a), den zuständigen Strafbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 59 Absatz 2 E-DSG geht (Bst. b), und den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss den Artikeln 44 Absatz 2 und 45 E-DSG (Bst. c) bekannt zu geben hat.

Die in den Absätzen 1 und 2 genannte Bekanntgabe von Informationen kann spontan oder auf Anfrage erfolgen.

Art. 49 Amtshilfe gegenüber ausländischen Behörden

Diese neue Bestimmung regelt die Amtshilfe zwischen dem Beauftragten und den ausländischen Datenschutzbehörden. Der derzeit geltende Artikel 31 Absatz 1 Buchstabe c DSG beschränkt sich darauf, den Beauftragten zur Zusammenarbeit mit den ausländischen Datenschutzbehörden zu verpflichten.

Die neue Bestimmung überträgt Artikel 50 der Richtlinie (EU) 2016/680 ins Schweizer Recht. Sie erfüllt zudem die Anforderungen von Artikel 15 und 16 E-SEV 108. Die Verordnung (EU) 2016/679 sieht in Artikel 61 eine analoge Regelung vor.

Der Beauftragte hätte eine Ergänzung der Bestimmung befürwortet, wonach er ermächtigt würde, die Modalitäten der Zusammenarbeit mit den ausländischen Datenschutzbehörden im Rahmen einer Vereinbarung zu regeln. Der Bundesrat zieht es dagegen vor, sich an die Kompetenzdelegation gemäss Artikel 61 E-DSG zu halten.

Abs. 1 Voraussetzungen

Gemäss dieser Bestimmung kann der Beauftragte unter bestimmten Voraussetzungen (Bst. a–e) mit ausländischen Behörden, die für den Datenschutz zuständig sind, für die Erfüllung ihrer jeweiligen gesetzlich vorgesehenen Aufgaben im Bereich des Datenschutzes Informationen oder Personendaten austauschen.

Nach der ersten Voraussetzung (Bst. a) muss zwischen der Schweiz und dem ausländischen Staat die Gegenseitigkeit der Amtshilfe im Datenschutzbereich sichergestellt sein. Zweitens dürfen die ausgetauschten Informationen und Personendaten nach dem Spezialitätsgrundsatz nur für das fragliche Datenschutzverfahren verwendet werden, das dem Amtshilfeersuchen zugrunde liegt (Bst. b). Wenn die Daten anschliessend in einem Strafverfahren verwendet werden sollen, gelten die Grundsätze der internationalen Rechtshilfe in Strafsachen. Die dritte und die vierte Voraussetzung gewährleisten die Wahrung der Berufsgeheimnisse sowie der Geschäfts- und Fabrikationsgeheimnisse (Bst. c) und verbieten, dass die Informationen und Personendaten ohne vorgängige Genehmigung der Behörde, die sie übermittelt hat, bekannt gegeben werden (Bst. d). Schliesslich muss die empfangende Behörde die Auflagen und Einschränkungen der Behörde einhalten, die ihr die Informationen und Personendaten übermittelt hat (Bst. e).

Der Beauftragte kann das Amtshilfeersuchen einer ausländischen Behörde beispielsweise ablehnen, wenn die Voraussetzungen von Artikel 13 E-DSG nicht eingehalten sind oder wenn einer der in Artikel 32 Absatz 6 E-DSG vorgesehenen Gründe einer Bekanntgabe von Personendaten entgegensteht.

Abs. 2 Bekanntgabe von Personendaten

Absatz 2 Buchstaben a–g bestimmt, welche Informationen der Beauftragte der ausländischen Behörde bekannt geben darf, um sein Amtshilfegesuch zu begründen oder dem Ersuchen einer ausländischen Behörde Folge zu leisten. Um die Identität der betroffenen Personen weiterleiten zu dürfen, benötigt der Beauftragte die Einwilligung jeder einzelnen Person (Bst. c). Für die Einwilligung gelten die Anforderungen von Artikel 5 Absatz 6 E-DSG (Abs. 2 Bst. c Ziff. 1). Ohne Einwilligung darf

die Identität nur bekannt gegeben werden, wenn dies für die Erfüllung der gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde unentbehrlich ist (Abs. 2 Bst. c Ziff. 2). Diese Voraussetzungen entsprechen jenen nach Artikel 32 Absatz 2 Buchstaben a und b E-DSG.

Abs. 3 Stellungnahme

Bevor der Beauftragte in einem Amtshilfeverfahren einer ausländischen Behörde, die für den Datenschutz zuständig ist, Informationen bekannt gibt, die Berufs-, Geschäfts- oder Fabrikationsgeheimnisse enthalten können, informiert er die betroffenen Personen und lädt sie zur Stellungnahme ein. Von dieser Pflicht ist er jedoch entbunden, wenn die Information nicht möglich ist oder einen unverhältnismässigen Aufwand erfordert.

9.1.8.4 Andere Aufgaben des Beauftragten

Art. 50 Register

Die Bestimmung sieht vor, dass der Beauftragte ein Register der ihm von den Bundesorganen gemeldeten Datenbearbeitungstätigkeiten (Art. 11 Abs. 4) führt. Dieses Register soll wie heute veröffentlicht werden.

Art. 51 Information

Abgesehen davon, dass der Beauftragte der Bundesversammlung und dem Bundesrat neu jährlich einen Tätigkeitsbericht unterbreiten muss, entspricht Absatz 1 dem geltenden Artikel 30 Absatz 1 DSG.

Absatz 2 verstärkt die aktive Information durch den Beauftragten. Dieser informiert die Öffentlichkeit über seine Feststellungen und Verfügungen, wenn ein allgemeines öffentliches Interesse dafür besteht. Artikel 30 Absatz 2 zweiter Satz DSG wird aufgehoben. Als unabhängige Instanz muss der Beauftragte selbst bestimmen können, worüber er die Öffentlichkeit informiert. Daten müssen anonymisiert werden, es sei denn, es besteht ein überwiegendes öffentliches Interesse an deren Bekanntgabe (Art. 32 Abs. 3 und 5 E-DSG). Zudem gelten die Voraussetzungen von Artikel 32 Absatz 6 E-DSG.

Die Pflicht der Aufsichtsbehörde zur Erstellung eines Tätigkeitsberichts ist in Artikel 49 der Richtlinie (EU) 2016/680 und in Artikel 12bis Absatz 5bis E-SEV 108 vorgesehen. Die Verordnung (EU) 2016/679 enthält in Artikel 59 eine analoge Regelung.

Art. 52 Weitere Aufgaben

Um Artikel 46 Absatz 1 Buchstaben d und e der Richtlinie (EU) 2016/680 umzusetzen, wird die Liste der Kompetenzen des Beauftragten gegenüber dem geltenden Recht (Art. 31 DSG) ergänzt. Die neuen Aufgaben entsprechen zudem den Anforderungen von Artikel 12bis Ziffer 2 Buchstabe e E-SEV 108.

Nach Absatz 1 hat der Beauftragte insbesondere die Aufgabe, die Bundesorgane sowie private Personen in Datenschutzfragen zu informieren, zu schulen und zu beraten. Hierzu gehören auch entsprechende Informationsveranstaltungen oder Weiterbildungen, namentlich für Verantwortliche im öffentlichen Sektor (Bst. a). Eine weitere Aufgabe besteht darin, die Öffentlichkeit, insbesondere schutzbedürftige Personen wie Minderjährige oder ältere Menschen, für den Datenschutz zu sensibilisieren (Bst. c). Ausserdem erteilt er auf Anfrage den betroffenen Personen Auskunft, wie sie ihre Rechte ausüben können (Bst. d).

Gemäss Buchstabe e muss der Beauftragte zu sämtlichen Vorlagen über Erlasse und Massnahmen des Bundes, welche die Datenbearbeitung betreffen, konsultiert werden und nicht nur zu jenen, welche den Datenschutz in erheblichem Masse betreffen. Diese Änderung entspricht der aktuellen Praxis.

In Buchstabe g ist vorgesehen, dass der Beauftragte ausserdem Leitfäden und Arbeitsinstrumente zuhanden der Verantwortlichen, Auftragsbearbeiter und betroffenen Personen erarbeitet. Diese Aufgabe nimmt er heute bereits im Rahmen seiner Beratungstätigkeit wahr (Art. 28, 30 und 31 DSG).[178] Es wird ferner präzisiert, dass er die Besonderheiten der einzelnen Datenbearbeitungsbereiche berücksichtigt sowie das erhöhte Schutzbedürfnis besonders verletzlicher Personen wie Minderjähriger, Behinderter oder älterer Menschen.

Absatz 2 entspricht Artikel 31 Absatz 2 DSG.

Aufhebung von Art. 33 DSG

Diese Bestimmung kann aufgehoben werden. Absatz 1, wonach der Rechtsschutz sich nach den allgemeinen Bestimmungen über die Bundesrechtspflege richtet, hat lediglich deklaratorische Bedeutung. Absatz 2 wiederum ist aufgrund von Artikel 44 Absatz 2 E-DSG überflüssig.

9.1.8.5 Gebühren

Art. 53

Nach Artikel 33 Absatz 1 VDSG wird für die Gutachten des Beauftragten für private Personen eine Gebühr erhoben. Die Bestimmungen der Allgemeinen Gebührenverordnung vom 8. September 2004[179] (AllgGebV) sind anwendbar.

Gemäss Absatz 1 wird auf Gesetzesstufe der Grundsatz verankert, wonach der Beauftragte für bestimmte Dienstleistungen gegenüber privaten Personen eine Gebühr erheben muss. Darunter fallen die Stellungnahme zu einem Verhaltenskodex (Bst. a), die Genehmigung von Standarddatenschutzklauseln und verbindlichen unternehmensinternen Datenschutzvorschriften (Bst. b), die Konsultation aufgrund

178 Z. B. der Leitfaden für die Bearbeitung von Personendaten im medizinischen Bereich, der Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung oder der Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich.

179 SR **172.041.1**

einer Datenschutz-Folgenabschätzung (Bst. c), die Massnahmen nach Artikel 44 Absatz 2 und 45 E-DSG (Bst. d) sowie Beratungen in Fragen des Datenschutzes (Bst. e). Im Umkehrschluss ergibt sich aus Absatz 1, dass für eine Untersuchung, die ohne Anordnung von vorsorglichen Massnahmen oder Verwaltungsmassnahmen abgeschlossen wird, keine Gebühr erhoben wird.

In Absatz 2 wird der Bundesrat beauftragt, die Höhe der Gebühren zu bestimmen. Entsprechend den Anforderungen von Artikel 46*a* Absatz 1 RVOG darf er ausschliesslich für die Verrichtungen nach Artikel 53 Absatz 1 E-DSG Gebühren erheben. Zudem muss er die Höhe der Gebühren so festlegen, dass sie die Kosten für die Verrichtungen decken (Kostendeckungsprinzip). Es ist also nicht vorgesehen, die gesamte Tätigkeit des Beauftragten durch Gebühren zu finanzieren. Es sollen ausschliesslich die Kosten für die Verrichtungen nach Absatz 1 gedeckt werden. Bei der Regelung des Tarifs kann der Bundesrat je nach Dienstleistung einen Pauschaltarif oder einen Stundenansatz festlegen.

Nach Absatz 3 kann der Bundesrat darüber hinaus die Fälle festlegen, in denen es möglich ist, auf die Erhebung einer Gebühr zu verzichten oder sie zu reduzieren. So kann auf eine Gebührenerhebung beispielsweise verzichtet werden, wenn an der Dienstleistung ein überwiegendes öffentliches Interesse besteht und sie zur Beachtung des Datenschutzes beiträgt. Artikel 3 Absatz 2 Buchstabe a AllgGebV enthält eine ähnliche Lösung. Der Beauftragte kann die Gebühr auch stunden, herabsetzen oder erlassen, wenn es sich beim Verantwortlichen oder Auftragsbearbeiter um eine natürliche Person oder ein kleines oder mittleres Unternehmen handelt.

Gebühren werden nur gegenüber privaten Personen erhoben. In Bezug auf die Beratung der Kantonsbehörden ist Artikel 3 Absatz 1 AllgGebV anwendbar: Die Bundesverwaltung erhebt keine Gebühren von interkantonalen Organen, Kantonen und Gemeinden, soweit diese Gegenrecht gewähren. Die Dienstleistungen für Organe des Bundes und der Kantone werden kostenlos erbracht.

9.1.9 Strafbestimmungen

Aufgrund zahlreicher kritischer Stellungnahmen zum Vorentwurf hat der Bundesrat die Strafbestimmungen grundlegend überarbeitet.

In der Vernehmlassung wurde (unter Hinweis auf die Verordnung [EU] 2016/679) die Einführung von finanziellen Verwaltungssanktionen gefordert. Finanzielle Verwaltungssanktionen mit strafendem Charakter sind in der Schweiz aber eine Ausnahme. Sie gehören klassischerweise in Bereiche, in denen Unternehmen einer verwaltungsrechtlichen Aufsicht unterstehen, weil sie eine wirtschaftliche Aktivität ausüben, für die sie eine Konzession oder Bewilligung benötigen oder für die sie staatliche Subventionen erhalten (z. B. im Postwesen oder für Geldspiele). Sie wurden ausserdem im Kartellrecht eingeführt, als es im StGB noch keine Unternehmensstrafbarkeit gab. Solche finanziellen Verwaltungssanktionen haben Strafcharakter, weshalb gewisse strafprozessuale Garantien einzuhalten sind. Das grundsätzlich anwendbare Verwaltungsverfahren regelt diese Fragen jedoch nicht. Es geht bei solchen Sanktionen zudem um eine direkte Zurechnung fremden Verschuldens an ein Unternehmen. Dies hat der Gesetzgeber mit der Unternehmensstrafbarkeit nach

Artikel 102 StGB aber abgelehnt: Die Verantwortlichkeit nach Artikel 102 StGB ist keine Kausal- oder Gefährdungshaftung[180], sondern verlangt ein spezifisches Organisationsverschulden. Mit der Einführung von pönalen Verwaltungssanktionen im DSG würde dieser strafrechtliche Grundsatzentscheid durch die Hintertür des Verwaltungsrechts stark relativiert.

Im Bereich des Datenschutzes wären solche Verwaltungssanktionen zudem besonders heikel. Der persönliche Geltungsbereich des DSG ist deutlich breiter als derjenige von Gesetzen in Bereichen, in denen klassischerweise finanzielle Verwaltungssanktionen zu finden sind und in denen die wirtschaftliche Tätigkeit durch Unternehmen ausgeübt wird. Das DSG richtet sich zwar auch an Grossunternehmen, erfasst aber ebenso KMU und natürliche Personen. Weil kein kodifiziertes Prozessrecht für Verwaltungssanktionen mit pönalem Charakter existiert, bestünde unter anderem die Gefahr, dass die verfahrensrechtliche Stellung von natürlichen Personen ausgehöhlt würde. Dies gilt insbesondere, weil zwischen juristischen und natürlichen Personen im Nebenstrafrecht verfahrensrechtliche Unterschiede bestehen.[181] Zusammenfassend würde die Einführung von finanziellen Verwaltungssanktionen im DSG damit eine grosse Rechtsunsicherheit erzeugen, was (nicht nur im Bereich des Datenschutzes) kaum vertretbar ist.

Der Bundesrat will deshalb an etablierte Strukturen mit gefestigter Praxis anknüpfen. In der Schweiz wird die Einhaltung grundlegender verwaltungsrechtlicher Pflichten mit dem Verwaltungsstrafrecht bzw. dem Nebenstrafrecht sichergestellt. Normadressaten sind natürliche Personen. Obschon die verwaltungsrechtliche Pflicht dem Unternehmen obliegt, wird ihre Verletzung den Leitungspersonen zugerechnet (vgl. Art. 29 StGB und Art. 6 VStR[182]). Die in der Vernehmlassung geäusserte Sorge, dass jeder beliebige Angestellte eines Unternehmens bestraft werden könnte, erweist sich deshalb als unbegründet. Die Sanktionierung mit strafrechtlichen Mitteln bedeutet auch, dass Gewinne, die aus DSG-Straftaten stammen, und Deliktswerkzeuge somit nach den Bestimmungen des StGB eingezogen werden können (Art. 69 ff. StGB). Der Beauftragte soll zudem nicht strafrechtliche Sanktionen aussprechen, weil sonst die Organisation des Beauftragten grundlegend verändert und deutlich ausgebaut werden müsste. Der Bundesrat zieht daher das bestehende Strafverfolgungssystem vor.

Das strafrechtliche Dispositiv des DSG muss im Vergleich zum geltenden Recht verstärkt werden. Die Sanktionen müssen abschreckend sein, wie vom E-SEV 108 (Art. 10) und der Richtlinie (EU) 2016/680 (Art. 57) verlangt. Ein zu mildes Strafsystem kann zur Folge haben, dass die EU die schweizerische Regelung als nicht mehr angemessen erachtet. Das vorgeschlagene Sanktionensystem sieht in den Grundzügen nun wie folgt aus:

180 Botschaft StGB AT, BBl **1999** II 1979 ff., Ziff. 217.421 und BGE **142** IV 333.
181 Zu nemo tenetur bei juristischen Personen im Nebenstrafrecht vgl. BGE **142** IV 207, 215 f., 222 f. und BGE **140** II 384, 393.
182 Dazu BGE **142** IV 315.

- Auf die Pönalisierung von fahrlässigen Pflichtverletzungen wird in Übereinstimmung mit den jüngsten Entscheiden des Parlaments verzichtet (vgl. z. B. den Entwurf zum Geldspielgesetz[183]). Der Beauftragte hätte dagegen bevorzugt, dass auch die Fahrlässigkeit strafbar wäre.
- Die verwaltungsrechtlichen Pflichten wurden konkretisiert und die Pönalisierung auf wesentliche Pflichten beschränkt.
- Zur Kompensation erhält der Beauftragte die Kompetenz, die Einhaltung der DSG-Pflichten zu verfügen und mit einer Ungehorsams-Strafdrohung zu verbinden. Dieses Modell ist im Nebenstrafrecht weit verbreitet (z. B. im Bundesgesetz vom 22. Juni 2007[184] über die Eidgenössische Finanzmarktaufsicht [FINMAG]) und entspricht dem Mechanismus von Artikel 292 StGB. Falls erforderlich, kann sich der Beauftragte in kantonalen Strafverfahren als Privatkläger beteiligen.
- Die Bussenobergrenze wird vom Bundesrat auf maximal 250 000 Franken festgelegt. Die Erhöhung erfolgt insbesondere um das schweizerische Recht der Verordnung (EU) 2016/679 anzunähern. Es wäre jedoch fragwürdig, die Bussenobergrenze gegen natürliche Personen noch höher anzusetzen mit der Begründung, Unternehmen würden durch tiefe Bussen nicht abgeschreckt. Die Strafbestimmungen des E-DSG richten sich primär an natürliche Personen, hier insb. an Leitungspersonen (vgl. Artikel 29 StGB und Artikel 6 VStrR). Es ist anzumerken, dass etwa im FINMAG fahrlässige Pflichtverletzungen mit Busse bis zu 250 000 Franken bedroht sind (Art. 44 ff. FINMAG), das Missachten einer Verfügung jedoch mit Busse bis zu 100 000 Franken (Art. 48 FINMAG). Der Beauftragte ist dagegen der Ansicht, die Bussen seien nicht ausreichend abschreckend, namentlich was deren Höhe betrifft.
- Die Verletzung der beruflichen Schweigepflicht ist wie bisher eine Übertretung.
- Soweit Daten durch ein Unternehmen bearbeitet werden, obliegen die aus dem DSG abgeleiteten Pflichten in der Regel dessen Leitungspersonen. Diese sind gesetzlich verpflichtet, die Einhaltung dieser Pflichten im Unternehmen sicherzustellen.[185] Die Verletzung von Pflichten oder der Ungehorsam gegen eine Verfügung des Beauftragten, die sich an das Unternehmen richtet, werden daher in Anwendung von Art. 29 StGB und Art. 6 VStR den Leitungspersonen im Unternehmen und nicht den bloss ausführenden Mitarbeitern angelastet.
- Soweit die Busse 50 000 Franken nicht übersteigt, können Unternehmen in Anwendung von Art. 7 VStrR direkt gebüsst werden. Dies trägt auch der in der Vernehmlassung vorgebrachten Kritik Rechnung.

183 Vgl. BBl **2015** 8535
184 SR **956.1**
185 BGE **142** IV 315.

Art. 54 Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten

Artikel 54 E-DSG übernimmt Artikel 34 DSG, mit Ausnahme von Artikel 34 Absatz 2 Buchstabe a DSG, weil die dort geregelten Pflichten im E-DSG nicht mehr enthalten sind. Im Gegenzug bezieht sich die Norm aber auch auf die neue Informationspflicht bei einer automatisierten Einzelentscheidung (Art. 19 E-DSG).

Absatz 1 Buchstabe a umfasst das vorsätzliche Erteilen einer falschen Auskunft, aber auch das vorsätzliche Erteilen einer unvollständigen Auskunft, während der Eindruck erweckt wird, dass die Auskunft vollständig sei. Das gänzliche Verweigern einer Auskunft ist dagegen nicht nach Buchstabe a, sondern gegebenenfalls nach Buchstabe b strafbar. Die private Person, welche wahrheitswidrig vorgibt, über keine Informationen zur betroffenen Person zu verfügen, macht sich indessen nach Absatz 1 Buchstabe a strafbar.

Absatz 1 Buchstabe b kommt in Fällen zur Anwendung, in welchen eine private Person es vollständig unterlässt, die betroffene Person nach den Artikeln 17 Absatz 1 und 19 Absatz 1 zu informieren oder ihr die Angaben nach Artikel 17 Absatz 2 zu liefern. Nicht strafbar ist dagegen die private Person welche unter Berufung auf Artikel 18 oder 25 behauptet, dass sie nicht zur Information verpflichtet sei. In einem solchen Fall weiss die betroffene Person nämlich, dass eine Datenbearbeitung stattfindet. Sie ist deshalb in der Lage, ihre Rechte geltend zu machen und ein zivilrechtliches Verfahren einzuleiten, in welchem darüber entschieden werden kann, ob die Verweigerung oder Einschränkung des Auskunftsrechts oder der Informationspflicht gerechtfertigt ist.[186]

Absatz 2 übernimmt Art. 34 Absatz 2 Buchstabe b DSG, welcher das Erteilen falscher Auskünfte oder die Verweigerung der Mitwirkung im Rahmen einer Untersuchung des Beauftragten für strafbar erklärt.

Die Verletzung dieser Pflichten soll weiterhin eine Übertretung sein, aber die dafür vorgesehene Bussenobergrenze ist deutlich anzuheben und auf 250 000 Franken zu erhöhen. Die tatsächliche Strafe wird unter Berücksichtigung der wirtschaftlichen Lage des Täters (Art. 106 Abs. 3 StGB in Verbindung mit Art. 47 StGB) festgelegt. In Bagatellfällen kann anstelle der verantwortlichen Person das Unternehmen zur Bezahlung der Busse verurteilt werden. Ferner kann gemäss Artikel 52 StGB bei geringfügigen Fällen von einer Strafverfolgung oder Bestrafung abgesehen werden.

Art. 55 Verletzung von Sorgfaltspflichten

Diese Bestimmung ist neu. Sie ist notwendig, weil der E-DSG neue elementare Pflichten vorsieht, die von den geltenden Strafbestimmungen nicht abgedeckt werden. Ein wirksamer Schutz der Persönlichkeit der betroffenen Personen ist dann möglich, wenn die Verantwortlichen und die Auftragsbearbeiter ihren Pflichten gerecht werden. Um sie zur Einhaltung des DSG anzuhalten, schlägt der Bundesrat diese Ergänzung der Strafbestimmungen vor.

186 Siehe auch BBl **1988** II 413, 484.

Die Bestimmung dürfte sich ihrer Natur nach primär an Personen mit Weisungsbefugnissen richten, weil die Entscheidkompetenz für die Erfüllung dieser Pflichten eine Leitungsaufgabe ist (vgl. auch Art. 29 StGB).

Art. 56 Verletzung der beruflichen Schweigepflicht

Seit Inkrafttreten des DSG hat sich die Informations- und Kommunikationstechnologie immens weiter entwickelt und deren Bedeutung hat markant zugenommen. Nicht zuletzt aufgrund der massenhaften Verbreitung von Smartphones werden immer mehr Daten von immer mehr Menschen auf immer mehr Systemen gespeichert und bearbeitet. Vor diesem Hintergrund ist es angezeigt, den Geheimnisschutz auf alle Arten von Personendaten auszudehnen. Massgebend ist, dass es sich um geheime Daten handelt. Dies entspricht Artikel 320 und 321 StGB, die ebenfalls alleine darauf abstellen, ob die fragliche Information geheim ist oder nicht. Es gilt somit der materielle Geheimnisbegriff des Strafrechts[187]. Ein strafrechtlich geschütztes Geheimnis liegt dann vor, wenn die Tatsache nicht allgemein bekannt oder zugänglich ist, wenn der Geheimnisherr ein schutzwürdiges Interesse an der beschränkten Bekanntheit hat und er auch den Willen dazu hat. Nicht jede Offenbarung von Personendaten erfüllt damit diesen Tatbestand. Der Begriff «offenbaren» entspricht demjenigen bei Artikeln 320 und 321 StGB und schafft hinsichtlich der Tathandlung Kohärenz.[188]

Mit Artikel 56 werden Lücken geschlossen, die durch den eingeschränkten Täterkreis der Artikel 320 und 321 StGB (Sonderdelikte) entstehen. Artikel 56 E-DSG sieht deshalb eine Schweigepflicht auch für Personen vor, die nicht unter Artikel 320 oder 321 StGB fallen. Die Verletzung der beruflichen Schweigepflicht ist eine Übertretung (Antragsdelikt) und wird mit einer Busse von bis zu 250 000 Franken bestraft.

Absatz 2 erweitert die Strafbarkeit auf Hilfspersonen (Auftragsdatenbearbeiter) und Auszubildende. Die Erweiterung entspricht dem geltenden DSG und in der Sache auch der Regelung in Artikel 321 StGB («Hilfspersonen»). Der Bundesrat hat dem Parlament mit der Verabschiedung der Botschaft zum Informationssicherheitsgesetz[189] eine entsprechende Änderung von Artikel 320 StGB vorgeschlagen.

Die Offenbarung kann durch die Einwilligung des Berechtigten gerechtfertigt sein. Die allgemeinen Regeln und die im Rahmen von Artikel 321 Ziffer 2 StGB von Rechtsprechung und Dogmatik entwickelten Grundsätze[190] gelten sinngemäss.

In der Praxis können sich Konkurrenzfragen insb. hinsichtlich Artikel 320 StGB (Bundesbeamte) und Art. 321 StGB (Anwälte, Ärzte etc.) stellen. Allerdings ist dies bereits im aktuellen Recht der Fall, weshalb dieser Umstand keine besonderen Probleme bieten sollte.

187 Stefan/Jean-Richard-dit-Bressel Marc, in: Trechsel/Pieth (Hrsg.), Schweizerisches Strafgesetzbuch Praxiskommentar, Zürich/St. Gallen 2013, Art. 162 StGB N 2.
188 Trechsel Stefan/Vest Hans, in: Trechsel/Pieth (Hrsg.), Schweizerisches Strafgesetzbuch Praxiskommentar, Zürich/St. Gallen 2013, Art. 320 StGB N 8 und Art. 321 StGB N 23 f.
189 BBl **2017** 2953, 3001 f. und 3077 ff.
190 Trechsel Stefan/Vest Hans, in: Trechsel/Pieth (Hrsg.), Schweizerisches Strafgesetzbuch Praxiskommentar, Zürich/St. Gallen 2013, Art. 321 StGB N 28.

Art. 57 Missachten von Verfügungen

Artikel 57 hat der Bundesrat nach der Vernehmlassung neu eingefügt. Analoge Bestimmungen sind im Nebenstrafrecht des Bundes weit verbreitet. Der Artikel dient einerseits als Kompensation für den Wegfall von zahlreichen Strafbestimmungen im Vergleich zum VE-DSG. Andererseits werden mit dieser Bestimmung die Fragen in Bezug auf den Grundsatz nulla poena sine lege, wie sie in der Vernehmlassung häufig vorgebracht wurden, berücksichtigt. Dieselben Fragen hätten sich auch im Zusammenhang mit Verwaltungssanktionen gestellt, weil diese strafrechtlichen Charakter haben. Die vorliegende Lösung erlaubt es, die entsprechenden Bestimmungen des E-DSG weiterhin in einer hinreichend allgemeinen Form auszugestalten, ohne zugleich in Konflikt mit den strafrechtlichen Anforderungen an die Präzision einer gesetzlichen Regelung zu geraten. Ausserdem erleichtert dieses Modell die Arbeit der zuständigen Strafverfolgungsbehörden und trägt damit den Bedenken Rechnung, die in der Vernehmlassung teilweise geäussert wurden.

Der Beauftragte hat mit Artikel 57 E-DSG die Möglichkeit, die Einhaltung von Pflichten nach dem E-DSG zu verfügen (siehe Art. 45 Abs. 3 E-DSG) und mit einer Strafandrohung zu verbinden. Ein Vorteil dieses Modells ist, dass die Pflicht in der Verfügung soweit konkretisiert werden kann, dass für den Adressaten kein Zweifel besteht, was er zu tun oder zu lassen hat. Dies erleichtert auch die Arbeit der kantonalen Strafverfolgungsbehörde, die im Falle der Missachtung auf Anzeige des Beauftragten hin den Sachverhalt ermitteln und ein Urteil fällen bzw. einen Strafbefehl erlassen muss.

Wenn sich die Verfügung des Beauftragten an ein Unternehmen richtet, tritt die Strafbarkeit kraft Artikel 29 StGB bei einer Leitungsperson ein: Die strafbegründende Pflicht, die dem Unternehmen obliegt, wird der natürlichen Person zugerechnet. Dies trägt auch der in der Vernehmlassung teilweise vorgebrachten Kritik Rechnung.

Art. 58 Widerhandlungen in Geschäftsbetrieben

Mit Artikel 58 werden Artikel 6 und 7 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht (VStrR) übernommen. Eine ausdrückliche Verweisung ist erforderlich, weil das VStrR in der Sache grundsätzlich nicht anwendbar ist.

Artikel 6 Absatz 2 VStrR ermöglicht die Geschäftsherrenhaftung auch im Bereich des DSG. Die Pflichten des DSG dürften sich nämlich regelmässig an den Geschäftsherrn richten.[191] Artikel 6 Absatz 2 VStrR erfüllt damit eine ähnliche Funktion wie Artikel 29 StGB und adressiert eine strafrechtliche Verantwortung an die Leitungsebene des Unternehmens, also an Führungspersonen, die Entscheidungs- und Weisungsbefugnisse haben. Dies ermöglicht eine sachgerechte Zuweisung der strafrechtlichen Verantwortung in Unternehmen.

Der Bussenbetrag, bis zu dessen Obergrenze es möglich ist, nach Artikel 7 VStrR ein Unternehmen an Stelle einer natürlichen Person zur Bezahlung einer Busse zu verurteilen, wird auf 50 000 Franken erhöht. Diese Anpassung ist erforderlich, weil

[191] Vgl. BGE **142** IV 315.

die Bussenobergrenze im DSG nicht bei 10 000 Franken liegt (Art. 106 Abs. 1 StGB), sondern bei 250 000 Franken.

Art. 59 Zuständigkeit

Die Verfolgung und Beurteilung der strafbaren Handlungen obliegt wie heute grundsätzlich den Kantonen.

Der Beauftragte hat ein Anzeigerecht und kann sich im kantonalen Strafverfahren als Privatkläger beteiligen (Art. 118 ff. StPO). Er kann somit Einstellungsverfügungen anfechten und Rechtsmittel gegen kantonale Urteile ergreifen, wenn dies im Interesse einer einheitlichen Anwendung des DSG geboten scheint. Gegen Strafbefehle und das Strafmass kann er hingegen kein Rechtsmittel ergreifen, was hinsichtlich seiner Aufgaben aber auch nicht erforderlich scheint.

Art. 60 Verfolgungsverjährung

Die Verjährungsfrist für Übertretungen beträgt nach Artikel 109 StGB drei Jahre. Datenschutzuntersuchungen erfordern technologisches Wissen und können aufwendig sein. Damit Strafverfahren im Datenschutzbereich somit nicht an zu kurzen Verjährungsfristen scheitern, sieht der Bundesrat eine Erhöhung auf fünf Jahre vor.

9.1.10 Abschluss von Staatsverträgen

Art. 61

Diese Bestimmung ersetzt Artikel 36 Absatz 5 DSG, der unter Berücksichtigung der geltenden Grundsätze in Bezug auf die Kompetenzdelegation zu unbestimmt ist. Gemäss Artikel 61 E-DSG kann der Bundesrat in zwei Fällen Staatsverträge mit einem oder mehreren Völkerrechtssubjekten (Staat, internationale Organisation) abschliessen. Nach Buchstabe a kann der Bundesrat Staatsverträge abschliessen, welche die internationale Zusammenarbeit zwischen Datenschutzbehörden betreffen. Diese Bestimmung bezieht sich etwa auf Kooperationsabkommen nach dem Modell des Abkommens vom 17. Mai 2013[192] zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Union über die Zusammenarbeit bei der Anwendung ihres Wettbewerbsrechts. Nach Buchstabe b kann der Bundesrat ausserdem Staatsverträge über die gegenseitige Anerkennung eines angemessenen Schutzniveaus für die grenzüberschreitende Bekanntgabe von Daten abschliessen.

Die übrigen Absätze von Artikel 36 DSG werden aufgehoben. Die Absätze 1 und 4 sind insofern überflüssig, als die Praxis, ausdrücklich festzuhalten, dass der Bundesrat Ausführungsbestimmungen erlassen muss, aufgegeben wurde. Absatz 3, wonach der Bundesrat für die Auskunftserteilung durch diplomatische und konsularische Vertretungen der Schweiz im Ausland Abweichungen von den Artikeln 8 und 9 vorsehen kann, kann ebenfalls aufgehoben werden. Absatz 6 wiederum ist obsolet,

192 SR **0.251.268.1**. Zu erwähnen ist, dass in diesem Fall die Kompetenz nicht dem Bundesrat übertragen war.

da der Bundesrat seine Kompetenz, zu regeln, wie Datensammlungen zu sichern sind, deren Daten im Kriegs- oder Krisenfall zu einer Gefährdung von Leib und Leben der betroffenen Personen führen können, nie wahrgenommen hat.

9.1.11 Schlussbestimmungen

Aufhebung von Art. 37 DSG

Die Vernehmlassung hat ergeben, dass Artikel 37 DSG überflüssig ist und aufgehoben werden muss. Heute verfügen sämtliche Kantone über Datenschutzvorschriften, die im Hinblick auf die Anforderungen des Übereinkommens SEV 108 und des entsprechenden Zusatzprotokolls einen angemessenen Schutz gewährleisten.

Art. 62 Aufhebung und Änderung anderer Erlasse

Die Aufhebung und Änderung anderer Erlasse wird unter Ziffer 9.2 kommentiert.

Art. 63 Übergangsbestimmungen betreffend die Pflichten des Verantwortlichen

Nach Absatz 1 richtet sich die Informationspflicht bei der Beschaffung von Personendaten während zwei Jahren nach Inkrafttreten dieses Gesetzes nach dem bisherigen Recht. Private Verantwortliche müssen demnach während zwei Jahren weiterhin lediglich bei der Beschaffung von besonders schützenswerten Personendaten informieren (vgl. Art. 14 DSG). Die Informationspflicht bei der Beschaffung von Persönlichkeitsprofilen, welche nach altem Recht besteht, entfällt, weil es nach neuem Recht keine Persönlichkeitsprofile mehr gibt. Bundesorgane müssen die betroffene Person weiterhin nach altem Recht über die Beschaffung von Personendaten informieren (vgl. Art. 18 DSG), ausser Artikel 63 Absatz 2 E-DSG ist anwendbar.

Nach Absatz 2 gelten die Artikel 6, 17–21 E-DSG während zwei Jahren nach Inkrafttreten dieses Gesetzes nur für Datenbearbeitungen im Sinne von Artikel 1 und Artikel 2 der Richtlinie (EU) 2016/680. Für private Verantwortliche und Bundesorgane, die ausserhalb des Anwendungsbereichs der Richtlinie (EU) 2016/680 Daten bearbeiten, treten diese Artikel damit erst zwei Jahre nach Inkrafttreten dieses Gesetzes in Kraft. Diese Regelung gilt, um den Verantwortlichen genügend Zeit zu geben, um sich auf die Erfüllung dieser neuen Pflichten vorzubereiten. Für den Anwendungsbereich der Richtlinie (EU) 2016/680 gelten diese Artikel hingegen bereits im Zeitpunkt des Inkrafttretens des Gesetzes.

Art. 64 Übergangsbestimmungen betreffend Bearbeitungen

Artikel 64 enthält verschiedene Übergangsregeln betreffend Bearbeitungen.

Abs. 1

Absatz 1 betrifft Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens dieses Gesetzes abgeschlossen sind. Hierbei handelt es sich um Datenbearbeitungen, die vollständig nach altem Recht erfolgt sind und die nach dem Inkrafttreten auch nicht mehr fortdauern. Solche Bearbeitungen richten sich weiterhin vollständig nach dem bisherigen Recht. So können beispielsweise abgeschlossene Bearbeitungen, die nach bisherigem Recht rechtmässig sind, nicht durch Inkrafttreten des neuen Rechts widerrechtlich werden. Dies gilt jedoch nicht für das Auskunftsrecht (Art. 23–25); nach Inkrafttreten des neuen Rechts richtet sich dieses ausschliesslich nach neuem Recht, und zwar auch bezüglich Daten und Datenbearbeitungen, die vollständig nach altem Recht erfolgt sind.

Abs. 2

Absatz 2 betrifft Datenbearbeitungen, die nach bisherigem Recht begonnen wurden und nach Inkrafttreten des Gesetzes fortdauern, bei denen aber das neue Recht die Voraussetzungen verschärft hat. Zu denken ist beispielsweise an den Fall, dass nach neuem Recht eine Persönlichkeitsverletzung vorliegt, weil die Anforderungen an den Rechtfertigungsgrund geändert wurden. Solche Bearbeitungen dürfen grundsätzlich während 2 Jahren ohne weitere Anpassungen fortgeführt werden. In dieser Zeit muss der Verantwortliche dafür sorgen, dass diese Bearbeitungen in einen rechtmässigen Zustand nach neuem Recht übergeführt werden.

Absatz 2 betrifft dabei nicht die Pflichten nach den Artikeln 6, 20 und 21, die durch den Absatz 3 erfasst werden.

Abs. 3

Absatz 3 betrifft Datenbearbeitungen, die nach bisherigem Recht begonnen wurden und nach Inkrafttreten des Gesetzes fortdauern. Für solche Bearbeitungen gelten die Artikel 6, 20 und 21 nicht, wenn der Bearbeitungszweck unverändert bleibt und keine neuen Daten beschafft werden. In diesem Fall dürfen die Bearbeitungen weitergeführt werden, ohne dass sie den Anforderungen von Artikel 6 genügen. Ebenfalls muss für diese Bearbeitungen nicht nachträglich eine Datenschutz-Folgeabschätzung erstellt werden. Diese Regelung liegt insbesondere darin begründet, dass die Pflichten in Artikel 6 und 20 f. primär im Vorfeld einer Datenbearbeitung zu erfüllen sind. Die Verantwortlichen sollen nicht dazu verpflichtet werden, diese Pflichten nachträglich und damit rückwirkend zu erfüllen.

Sind die Voraussetzungen von Absatz 3 nicht erfüllt, gelten die Pflichten nach Artikel 6, 20 und 21 auch für Bearbeitungen, die nach bisherigem Recht begonnen wurden und nach Inkrafttreten des Gesetzes fortdauern. Mit Ausnahme des Anwendungsbereichs der Richtlinie (EU) 2016/680 treten diese Bestimmungen allerdings erst zwei Jahre nach Inkrafttreten des Gesetzes in Kraft, sodass eine zweijährige Übergangsfrist besteht, um diese Pflichten zu erfüllen.

Abs. 4

Absatz 4 betrifft alle Datenbearbeitungen, die nicht unter die Absätze 1 bis 3 fallen. Dazu gehören insbesondere Datenbearbeitungen, die erst nach Inkrafttreten des Gesetzes begonnen wurden, aber auch solche, die sowohl nach bisherigem als auch nach neuem Recht rechtmässig sind. Für diese Datenbearbeitungen gilt das neue Recht ab dem Zeitpunkt des Inkrafttretens der fraglichen Bestimmungen.

Art. 65 Übergangsbestimmung betreffend laufende Verfahren

Zur Gewährleistung der Rechtssicherheit und Einhaltung des Grundsatzes von Treu und Glauben schreibt diese Bestimmung vor, dass Untersuchungen des Beauftragten, die im Zeitpunkt des Inkrafttretens des künftigen DSG hängig sind, sowie Beschwerden gegen hängige erstinstanzliche Entscheide dem bisherigen Recht unterstehen. Dies betrifft sowohl die materiellen Datenschutzvorschriften als auch die Befugnisse des Beauftragten und die weiteren anwendbaren Verfahrensvorschriften.

Art. 66 Übergangsbestimmung betreffend Daten juristischer Personen

Die Aufhebung des Schutzes der Daten juristischer Personen im E-DSG sowie die Beschränkung des Begriffs der Personendaten in Artikel 4 Buchstabe a E-DSG auf Angaben, die sich auf eine bestimmte oder bestimmbare *natürliche Person* beziehen, hat verschiedene Auswirkungen auf die Datenbearbeitung durch Bundesorgane. Insbesondere führt diese Neuerung dazu, dass die bundesrechtlichen Gesetzesgrundlagen, mit denen Bundesorgane zur Bearbeitung und Bekanntgabe von Personendaten ermächtigt werden, inskünftig nicht mehr anwendbar sind, wenn Daten *juristischer Personen* bearbeitet bzw. bekannt gegeben werden. Aufgrund des in Artikel 5 Absatz 1 BV verankerten Legalitätsprinzips bedarf jedoch jedes staatliche Handeln – und damit auch jede staatliche Datenbearbeitung bzw. Datenbekanntgabe – einer gesetzlichen Grundlage (vgl. auch Artikel 13 Abs 2, Artikel 27 und Artikel 36 BV). Der Gesetzesentwurf führt deshalb im RVOG für die Bundesorgane eine Reihe von Bestimmungen ein, welche deren Umgang mit Daten juristischer Personen regeln (vgl. Ziff. 9.2.8). Zu erwähnen sind insbesondere Artikel 57*r* E-RVOG, welcher eine allgemeine gesetzliche Grundlage für die Bearbeitung von Daten juristischer Personen durch Bundesorgane schafft, sowie Artikel 57*s* E-RVOG, welcher – analog zu Artikel 32 E-DSG betreffend die Bekanntgabe von Personendaten – die Anforderungen an die Rechtsgrundlagen für die Bekanntgabe von Daten juristischer Personen enthält. Anders als Artikel 57*r* E-RVOG stellt Artikel 57*s* E-RVOG damit keine gesetzliche Grundlage für spezifische Datenbekanntgaben durch Bundesorgane dar, weshalb sich eine Bekanntgabe von Daten juristischer Personen auch inskünftig immer auf eine spezialgesetzliche Rechtsgrundlage stützen können muss. Eine Anpassung sämtlicher bisheriger Rechtsgrundlagen (welche aufgrund der Anpassungen im E-DSG grösstenteils nur noch auf natürliche Personen anwendbar sein werden) wäre im Rahmen dieser Vorlage nicht zweckmässig, würden der Gesetzesentwurf und die Botschaft dadurch doch erheblich verlängert. Dem Bundesrat erscheint es daher zielführender, die spezialgesetzlichen Datenschutzbestimmungen nach den parlamentarischen Beratungen dieser Vorlage gründlich durchzusehen und

zu prüfen, welche Vorschriften, die sich heute auf den Umgang von Bundesorganen mit Daten juristischer Personen beziehen, weiterhin beibehalten werden sollen oder angepasst bzw. aufgehoben werden müssen. Damit in der Zwischenzeit keine Rechtslücken entstehen, wird für Bundesorgane in Artikel 66 E-DSG eine Übergangsbestimmung eingeführt, welche die Weitergeltung solcher spezialgesetzlicher Bundesvorschriften (sowohl in Gesetzen im formellen als auch im materiellen Sinn) betreffend die Daten juristischer Personen während fünf Jahren nach Inkrafttreten des E-DSG für Bundesorgane vorsieht. Insbesondere sollen sich Bundesorgane während dieser Zeit für die Bekanntgabe von Daten juristischer Personen auf die bisherigen Rechtsgrundlagen zur Bekanntgabe von Personendaten stützen können.

Nur ganz vereinzelt, wo dies aus Gründen der Praktikabilität und der Rechtssicherheit bereits heute angezeigt ist, werden spezialgesetzliche Bestimmungen im Rahmen dieser Vorlage betreffend die Daten juristischer Personen überprüft und angepasst. Dies betrifft die folgenden Erlasse:

- das BGÖ (vgl. Ziff. 9.2.7: Art. 3 Abs. 2, 9, 11, 12 Abs. 2 und 3, 15 Abs. 2 Bst. b);
- das RVOG (vgl. Ziff. 9.2.8: Art. 57*h*bis, 57*h*ter, 57*i*, 57*j*, 57*k* Einleitungssatz, 57*l* Sachüberschrift und Einleitungssatz, 57*r*, 57*s* und 57*t*);
- das Revisionsaufsichtsgesetz vom 16. Dezember 2005[193] (vgl. Ziff. 9.2.12: Art. 15*b*);
- das Bundesstatistikgesetz vom 9. Oktober 1992[194] (vgl. Ziff. 9.2.24: Art. 5 Abs. 2 Bst. a und Abs. 4 Bst. a, 14 Abs. 1, 14*a* Abs. 1, 15 Abs. 1, Art. 16 Abs. 1 und 19 Abs. 2);
- das Bundesgesetz vom 17. Juni 2005[195] gegen die Schwarzarbeit (vgl. Ziff. 9.2.56: Art. 17 Sachüberschrift, Abs. 1, 2 und 4 sowie Art. 17*a*);
- das Nationalbankgesetz vom 3. Oktober 2003[196] (vgl. Ziff. 9.2.66: Art. 16 Abs. 5 und Art. 49*a*);
- das Bundesgesetz vom 19. März 1976[197] über die internationale Entwicklungszusammenarbeit und humanitäre Hilfe (vgl. Ziff. 9.2.69: Art. 13*a* Abs. 1);
- das Energiegesetz vom 30. September 2016[198] (vgl. Ziff. 13.7: Art. 56 Abs. 1, 58 Sachüberschrift, Abs. 1 und 3 sowie Art. 59 Sachüberschrift, Abs. 1 und 2) sowie das durch das Energiegesetz vom 30. September 2016 zu ändernde Stromversorgungsgesetz[199] (vgl. Ziff. 13.7: Art. 17*c* Abs. 1 und 27 Abs. 1)

193 SR **221.302**
194 SR **431.01**
195 SR **822.41**
196 SR **951.11**
197 SR **974.0**
198 BBl **2016** 7683
199 SR **734.7**; vgl. BBl **2016** 7683

Art. 67 Übergangsbestimmung betreffend die Zertifizierung

Gemäss Artikel 12 Absatz 2 E-DSG erlässt der Bundesrat Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Diese Bestimmung wird aus dem geltenden Artikel 11 Absatz 2 DSG entnommen. Der Bundesrat wird hauptsächlich die bisherigen Erlasse anpassen, namentlich die Verordnung vom 28. September 2007 über die Datenschutzzertifizierungen[200] und die Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996[201]. Angesichts des technischen Charakters dieser Verordnungen und der knappen Zeit, die zur Erarbeitung sämtlicher Vollzugsvorschriften zur Verfügung steht, erachtet es der Bundesrat als sinnvoll, eine Übergangsfrist von zwei Jahren vorzusehen. Während dieser Frist findet das bisherige Recht Anwendung.

9.2 Erläuterungen zu den Änderungen anderer Bundesgesetze

Die Aufhebung und Änderung anderer Bundesgesetze ist im Anhang des E-DSG geregelt. Diese Änderungen erfolgen aufgrund des E-DSG.

9.2.1 Aufhebung des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz

Da es sich beim E-DSG um eine Totalrevision handelt, muss das aktuelle DSG aufgehoben werden.

9.2.2 Änderung der Terminologie in Bundesgesetzen

Aufgrund der Aufhebung des Begriffs «Datensammlung» im E-DSG müssen die Bundesgesetze, in denen dieser verwendet wird, ebenfalls angepasst werden. Mit dem E-DSG wird ferner der Begriff «Inhaber der Datensammlung» durch «Verantwortlicher» ersetzt.

Im E-DSG wird zudem der Begriff «Persönlichkeitsprofil» durch den Begriff «Profiling» abgelöst. Wie in den Erläuterungen zu Artikel 4 Buchstabe f E-DSG dargelegt, überschneiden sich diese beiden Begriffe nicht ganz. Beim Profiling werden bestimmte Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, namentlich mittels Algorithmen, bewertet.

Da der Begriff «Persönlichkeitsprofil» aufgehoben wird, müssen auch die Gesetzesgrundlagen in einer Reihe von Gesetzen, mit denen die Bundesorgane zur Bearbeitung von Persönlichkeitsprofilen ermächtigt werden, angepasst werden.

200 SR **235.13**
201 SR **946.512**

In einigen Bundesgesetzen genügt es, den Verweis auf das Persönlichkeitsprofil einfach zu streichen. Denn es hat sich gezeigt, dass die Gesetzesgrundlagen für die Bearbeitung von Persönlichkeitsprofilen durch die Bundesorgane nie angewendet worden sind. In anderen Gesetzen muss der Begriff «Persönlichkeitsprofil» demgegenüber – wie im Folgenden erläutert – unter Berücksichtigung der neuen Anforderung nach Artikel 30 Absatz 2 Buchstaben b und c E-DSG entweder durch den Begriff «Profiling» ersetzt oder angepasst werden.

9.2.3 Ausländergesetz vom 16. Dezember 2005[202]

Art. 101

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Vgl. die Erläuterungen unter Ziffer 9.2.2.

Art. 104 Abs. 4

Der Verweis auf den E-DSG wird angepasst.

Art. 105 Abs. 1

Gestützt auf diese Bestimmung können Personendaten ins Ausland bekannt gegeben werden, wenn der betreffende Staat oder die betreffende Organisation für einen Datenschutz Gewähr bietet, der dem schweizerischen gleichwertig ist. Die Voraussetzungen für derartige Bekanntgaben müssen im Bundesrecht einheitlich sein. Deshalb ist ein Verweis auf Artikel 13 E-DSG erforderlich.

Art. 111d Abs. 1 und 2

Diese Bestimmung regelt die Bekanntgabe von Personendaten im Rahmen der Schengen-Assoziierungsabkommen. Absatz 1 regelt die Bekanntgabe von Personendaten an die zuständigen Behörden eines Drittstaats durch Verweis auf die Artikel 13 und 14 E-DSG. Die Anpassungen der Ausnahmen nach Absatz 2 tragen dem neuen Wortlaut von Artikel 14 Abs. 1 Bst. a, c und d E-DSG Rechnung.

Art. 111f zweiter Satz

Diese Bestimmung kann aufgehoben werden, da die Pflicht des Verantwortlichen, der betroffenen Person Auskunft über die Herkunft der Daten zu erteilen, in Artikel 23 Absatz 2 Buchstabe e E-DSG festgehalten ist.

202 SR **142.20**

9.2.4 Asylgesetz vom 26. Juni 1998[203]

Art. 96 Abs. 1, Art. 99a Abs. 2 Bst. a, Art. 100 Abs. 2 und Art. 102 Abs. 1 dritter Satz und Abs. 2

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Vgl. die Erläuterungen unter Ziffer 9.2.2.

Art. 98 Abs. 1

Siehe die Erläuterungen zu Artikel 105 E-AuG unter Ziffer 9.2.3.

Art. 99 Abs. 6

Der Begriff des «Inhabers der Datensammlung» wird durch den «Verantwortlichen» ersetzt und der Verweis auf den E-DSG angepasst.

Art. 102c Abs. 1 und 2

Vgl. den Kommentar zu Artikel 111*d* Absatz 1 und 2 E-AuG (Ziff. 9.2.3).

Art. 102e zweiter Satz

Siehe die Erläuterungen zu Artikel 111*f* zweiter Satz E-AuG (Ziff. 9.2.3).

9.2.5 Bundesgesetz vom 20. Juni 2003[204] über das Informationssystem für den Ausländer- und den Asylbereich

Art. 4 Abs. 2

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 6 und 7 Abs. 2

Die Verweise auf den E-DSG werden angepasst.

Art. 15 Bekanntgabe ins Ausland

In dieser Bestimmung müssen die Verweise auf die Artikel 13 und 14 E-DSG angepasst werden.

203 SR **142.31**
204 SR **142.51**

Art. 16 Aufsichtspflicht der kantonalen Datenschutzbehörden

Diese Bestimmung muss angepasst werden, da Artikel 37 DSG aufgehoben wird.

9.2.6 Archivierungsgesetz vom 26. Juni 1998[205]

Art. 11 Abs. 1

Der Begriff «Persönlichkeitsprofil» wird aus den unter Ziffer 9.2.2 genannten Gründen gestrichen. Die Schutzfrist von fünfzig Jahren gilt nur mehr für Archivgut, das nach Personennamen erschlossen ist und besonders schützenswerte Personendaten enthält. Für die übrigen Personendaten gilt eine Schutzfrist von dreissig Jahren.

Art. 15 Sachüberschrift und Abs. 1

Die Bestimmung muss angepasst werden, weil das Archivierungsgesetz in Bezug auf das Auskunftsrecht vollständig auf das DSG verweist. Die Anpassung stellt sicher, dass die Ansprüche nach Artikel 16 E-DSG ebenfalls von diesem Verweis erfasst sind.

9.2.7 Öffentlichkeitsgesetz vom 17. Dezember 2004[206]

Art. 3 Abs. 2

Da der E-DSG inskünftig nur noch für die Daten natürlicher Personen gilt, drängt sich aus Gründen der Rechtssicherheit eine entsprechende Präzisierung des Verweises in Absatz 2 auf den E-DSG auf, indem – in Einklang mit der Terminologie von Artikel 4 Buchstabe a – der Ausdruck «persönliche Daten» durch den Begriff der Personendaten ersetzt wird.

Art. 9 Schutz von Personendaten und von Daten juristischer Personen

Aufgrund der Aufhebung des Schutzes der Daten juristischer Personen im E-DSG sowie der Beschränkung des Begriffs der Personendaten in Artikel 4 Buchstabe a E-DSG auf Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, ist in Artikel 9 E-BGÖ aus Gründen der Rechtssicherheit klarzustellen (vgl. die Erläuterungen in Ziff. 9.1.11), dass auch amtliche Dokumente, welche Daten juristischer Personen enthalten, nach Möglichkeit vor der Einsichtnahme zu anonymisieren sind (Absatz 1). Aus demselben Grund ist der Verweis in Absatz 2 insofern zu präzisieren, als Zugangsgesuche zu nicht anonymisierten Dokumenten für Personendaten nach Artikel 32 E-DSG und für Daten juristischer Personen nach Artikel 57*s* E-RVOG zu beurteilen sind.

205 SR **152.1**
206 SR **152.3**

Art. 11 Anhörung

Artikel 11 Absatz 1 BGÖ sieht vor, dass die Behörde die betroffene Person konsultiert und ihr Gelegenheit zur Stellungnahme gibt, wenn ein Gesuch amtliche Dokumente betrifft, die Personendaten enthalten. Aufgrund des neuen Anwendungsbereichs des E-DSG ist die Anhörungspflicht der Behörde nicht mehr gewährleistet. Es ist daher erforderlich, Artikel 11 Absatz 1 BGÖ anzupassen, damit das rechtliche Gehör juristischer Personen gewährleistet bleibt, falls die Behörde erwägt, nach Artikel 7 Absatz 2 BGÖ Zugang zu gewähren (vgl. auch die Erläuterungen in Ziff. 9.1.11).

Der neue Wortlaut von Artikel 11 Absatz 1 hält fest, dass die Behörde verpflichtet ist, betroffene Dritte anzuhören, wenn sie in Erwägung zieht, den Zugang zu einem amtlichen Dokument zu gewähren, durch dessen Herausgabe die Privatsphäre dieser Dritten beeinträchtigt werden kann. Der Begriff der Privatsphäre gilt auch für juristische Personen, sodass die Behörde verpflichtet ist, diese zu konsultieren, wenn der beabsichtigte Zugang zu einem Dokument die Privatsphäre juristischer Personen beeinträchtigen kann (z. B. ihren guten Ruf).

Die Beschränkung der Pflicht zur Anhörung von Personen, deren Personendaten in einem amtlichen Dokument enthalten sind, auf Fälle, in denen die Zugänglichmachung der Daten die Privatsphäre dieser Personen beeinträchtigen kann, betrifft auch natürliche Personen. Damit wird der aktuellen bundesgerichtlichen Rechtsprechung Rechnung getragen, wonach die Behörde auf die Anhörung Dritter verzichten kann, wenn offensichtlich nicht die Gefahr besteht, dass durch die Zugänglichmachung von Personendaten (oder von Daten juristischer Personen) die Privatsphäre der betroffenen Person beeinträchtigt wird.[207]

Die Änderung von Artikel 11 Absatz 2 ist rein redaktionell.

Art. 12 Abs. 2 zweiter Satz und Abs. 3

Aufgrund der Anpassung von Artikel 11 Absatz 1 E-BGÖ ist es nötig, Artikel 12 Absatz 2 zweiter Satz und Absatz 3 zu ändern und auf amtliche Dokumente zur Anwendung zu bringen, durch deren Zugänglichmachung die Privatsphäre Dritter beeinträchtigt werden kann.

Art. 15 Abs. 2 Bst. b

Aus den bereits erwähnten Gründen ist es erforderlich, Artikel 15 Absatz 2 Buchstaben b zu ergänzen, wonach die Behörde eine Verfügung erlassen muss, wenn sie entgegen der Empfehlung des Beauftragten den Zugang zu einem amtlichen Dokument gewähren will, durch dessen Zugänglichmachung die Privatsphäre Dritter beeinträchtigt werden kann.

Art. 18 Einleitungssatz

Der Verweis auf den E-DSG wird angepasst.

207 Vgl. das Urteil des Bundesgerichts 1C_50/2015 vom 2. Dezember 2015, E. 6.3.

9.2.8 Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997[208]

Vorbemerkungen zu Art. 57h bis Art. 57h^ter

Ausgangslage: Rechtsgrundlagen der Geschäftsverwaltungssysteme

Artikel 57*h* RVOG ist die formell-gesetzliche Grundlage für die GEVER-Systeme der einzelnen Verwaltungseinheiten. Gestützt auf dessen Absatz 3 hat der Bundesrat die GEVER-Verordnung vom 30. November 2012[209] erlassen.

Mit dem neuen GEVER-System Acta Nova der Bundesverwaltung, welches zurzeit als Bundesstandard entwickelt wird und schrittweise bis Anfang 2020 in der zentralen Bundesverwaltung und in einzelnen Einheiten der dezentralen Bundesverwaltung (z. B. EDÖB) eingeführt wird (Programm GENOVA), soll es möglich sein, dass die einzelnen Verwaltungseinheiten für die Abwicklung überdepartementaler Prozesse (z. B. Ämterkonsultationen, Bundesratsgeschäfte) Zugriff auf die GEVER-Systeme anderer Verwaltungseinheiten erhalten. So können Prozesse vereinfacht und Medienbrüche vermieden werden: So sollen beispielsweise Unterlagen der Ämterkonsultation (ÄK) nicht mehr per Mail versandt werden müssen. Künftig wird etwa ein Verweis auf das ÄK-Dossier verschickt werden, und die eingeladenen Verwaltungseinheiten können direkt auf einem Masterdokument arbeiten. Nebst dem Ämterkonsultationsprozess sollen künftig auch weitere verwaltungseinheitsübergreifende Geschäftsprozesse über GEVER abgewickelt werden (z. B. Beschaffungen, Legislaturplanung, Ziele des Bundesrats, Geschäftsbericht). Die im Zuge der WTO-Beschaffung beschaffte Lizenz erlaubt die Einführung und den Betrieb des neuen GEVER-Systems in der zentralen, aber auch dezentralen Bundesverwaltung.

Nebst dem Zugriff anderer Verwaltungseinheiten sollen auch kantonale, kommunale und private Stellen (Unternehmen, Bürger) im Rahmen von E-Government-Lösungen punktuellen und klar begrenzten Zugang zum neuen GEVER-System erhalten können. Für das neue GEVER-System wurde vor diesem Hintergrund eine Lizenz beschafft, welche solche Zugriffe ohne weitere Lizenzkosten unbegrenzt erlauben würde.

Erforderlichkeit einer Anpassung der Rechtsgrundlagen

In der Botschaft vom 25. August 1999 über die Schaffung und die Anpassung gesetzlicher Grundlagen für die Bearbeitung von Personendaten[210] zu Artikel 57*h* RVOG wurde Folgendes ausgeführt: «Die vorgeschlagene Bestimmung erstreckt sich *nicht* auf die Registratursysteme, die von verschiedenen Bundesorganen gemeinsam geführt werden und Personendaten enthalten, zu denen verschiedene Bundesorgane Zugang haben. Für diese Systeme ist eine *besondere gesetzliche Grundlage erforderlich*, namentlich für die Bekanntgabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen über Abrufverfahren nach Artikel 19 Absätze 1 und 3 DSG.»

208 SR **172.010**
209 SR **172.010.441**
210 BBl **1999** 9005, 9009

Nach Artikel 19 Absatz 3 erster Satz DSG dürfen Bundesorgane Personendaten durch ein Abrufverfahren zugänglich machen, wenn dies ausdrücklich vorgesehen ist. Nach dessen zweitem Satz dürfen *besonders schützenswerte Personendaten* sowie *Persönlichkeitsprofile* nur durch ein Abrufverfahren zugänglich gemacht werden, wenn ein Gesetz *im formellen Sinn* es ausdrücklich vorsieht. Diese Bestimmung wird im Rahmen der Revision des DSG gestrichen.

Im Rahmen der allgemeinen überdepartementalen bzw. verwaltungseinheitsübergreifende Querschnittprozesse (Ämterkonsultationsverfahren, Abwicklung von Bundesratsgeschäften, Planungsprozesse, Beschaffungsprojekte) werden besonders schützenswerte Daten nur in sehr wenigen Ausnahmefällen bearbeitet (Beispiele für Bundesratsgeschäfte: Beschwerdeentscheide; Staatshaftungsfälle; Entscheide und Berichte über Tätigkeitsverbote nach dem Bundesgesetz vom 21. März 1997[211] über Massnahmen zur Wahrung der inneren Sicherheit (BWIS); Personalgeschäfte). Auch dies erfordert, streng genommen, nach dem geltenden Artikel 17 Absatz 2 DSG eine formell-gesetzliche Grundlage. Indessen soll künftig auch eine Verordnung genügen, wenn die Bearbeitung unentbehrlich ist für die Erfüllung einer formell-gesetzlich vorgesehenen Aufgabe und keine besonderen Risiken für die Grundrechte der betroffenen Personen bestehen (vgl. Artikel 30 Absatz 3 E-DSG).

Die eigentliche Rechtsgrundlage für die Bearbeitung von Personendaten muss sich bereits heute generell aus dem Spezialrecht ergeben. Der geltende Artikel 57*h* RVOG stellt lediglich die Rechtsgrundlage dar, die aufgrund des (aufzuhebenden) Artikels 19 Absatz 3 DSG nötig ist, um besonders schützenswerte Personendaten per Abrufverfahren bekanntzugeben.

Da Artikel 57*h* RVOG einen engen Zusammenhang mit dem allgemeinen Datenschutzrecht aufweist und dieses in einem für die Datenbearbeitung durch die Bundesverwaltung wichtigen Bereich konkretisiert, ist eine Anpassung im Rahmen der Revision des DSG gleichwohl geboten. Der grundsätzliche Wechsel vom Silo-Prinzip zu einem prozessorientierten Ansatz der Datenbearbeitung im Rahmen der GEVER-Systeme sollte aus Gründen der Transparenz in einer entsprechend angepassten Rechtsgrundlage ersichtlich gemacht werden.

Aufgrund der Aufhebung des Schutzes der Daten juristischer Personen im E-DSG sowie der Beschränkung des Begriffs der Personendaten in Artikel 4 Buchstabe a E-DSG auf Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, ist in den Artikeln 57*h*^{bis} und 57*h*^{ter} aus Gründen der Rechtssicherheit klarzustellen, dass diese Bestimmungen auch auf Daten juristischer Personen Anwendung finden (vgl. die Erläuterungen in Ziff. 9.1.11).

Art. 57h Führen von Geschäftsverwaltungssystemen

Der geltende Artikel 57*h* soll auf drei Bestimmungen aufgeteilt werden. Die geltende Bestimmung enthält sowohl Bestimmungen die das Führen von Geschäftsverwaltungssystemen betreffen, als auch Bestimmungen über die Bearbeitung von Personendaten in diesen Systemen. Diese beiden Elemente sind zu trennen und separat zu regeln.

211 SR **120**

Absatz 1: Die Führung von elektronischen Geschäftsverwaltungssystemen (GEVER-Systemen) ist heute für die zentrale Bundesverwaltung eine zwingende Vorgabe (vgl. namentlich Artikel 1 Absatz 1 der GEVER-Verordnung vom 30. November 2012[212]). Die GEVER-Systeme dienen insbesondere der rechtskonformen, prozessorientierten und transparenten Geschäftsabwicklung (Artikel 1 Absatz 2 GEVER-Verordnung). Die vorliegende Bestimmung soll daher gegenüber dem bisherigen Wortlaut leicht erweitert werden. In diesen Systemen werden nicht nur Geschäfte im prozeduralen Sinn bearbeitet, sondern auch Dokumente längerfristig gespeichert (z. B. im Hinblick auf den Nachweis der Verwaltungstätigkeit nach Artikel 22 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[213] [RVOV] und die spätere Archivierung). Künftig kann diese Dokumentationsfunktion der GEVER-Systeme allenfalls noch ausgeweitet werden.

Auch das System EXE-BRC, welches insbesondere der Abwicklung von Bundesratsgeschäften dient, ist ein Geschäftsverwaltungssystem im Sinne dieser Bestimmung.

Bei den angesprochenen Einheiten der Bundesverwaltung handelt es sich grundsätzlich um Ämter. Allerdings verfügt das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) aufgrund seiner organisatorischen Struktur über ein einziges GEVER-System für das gesamte Departement.

Absatz 2 hält fest, dass die für die jeweiligen GEVER-Systeme verantwortlichen Einheiten der zentralen oder dezentralen Bundesverwaltung anderen Bundesbehörden (z. B. anderen Einheiten der zentralen oder dezentralen Bundesverwaltung, den Parlamentsdiensten oder den eidgenössischen Gerichten) sowie bundesexternen Stellen (z. B. kantonalen Stellen oder interkantonalen Konferenzen) einen beschränkten Zugriff auf ihre Geschäftsverwaltungssysteme gewähren können. Damit soll es möglich werden, eine Anzahl von Geschäftsprozessen in diesen Systemen abzuwickeln, z. B. Ämterkonsultationen, Bundesratsgeschäfte, aber auch Beschaffungen oder Reporting-Prozesse (vgl. oben). Weiter soll so die interdepartementale Zusammenarbeit vereinfacht werden können.

Damit wird es sich in Zukunft in vielen Fällen erübrigen, Dokumente via E-Mail zu schicken. Die Prozesse und die zugrundeliegenden Informationen dürften sich so besser gegen unbefugte Zugriffe schützen lassen.

*Art. 57h^bis^* Bearbeitung von Personendaten und von Daten juristischer Personen

Absatz 1 entspricht im Wesentlichen dem geltenden Artikel 57*h* Absatz 1, letzter Satz, RVOG. Diese Bestimmung hält fest, zu welchen Zwecken in den Geschäftsverwaltungssystemen Personendaten und Daten juristischer Personen bearbeitet

212 SR **172.010.441**. Artikel 1 Absatz 1 der GEVER-Verordnung lautet: «Die Bundesverwaltung bearbeitet ihre geschäftsrelevanten Dokumente grundsätzlich in elektronischen Geschäftsverwaltungssystemen (GEVER-Systeme). Als geschäftsrelevant gelten die Dokumente, die für den Nachweis der Verwaltungstätigkeit im Sinne von Artikel 22 der Regierungs- und Verwaltungsverordnung vom 25. November 1998 (RVOV) notwendig sind.». Vgl. dazu auch die Ausführungen in der Botschaft des Bundesrates zur Finanzierung der Realisierung und der Einführung eines standardisierten GEVER-Produkts in der zentralen Bundesverwaltung vom 11. September 2015, BBl **2015** 6963.

213 SR **172.010.1**

werden können. Damit wird diese datenschutzrechtlich notwendige Konkretisierung beibehalten. Sie leitet sich aus Artikel 4 Absatz 3 und 17 Absatz 1 DSG ab (vgl. die Art. 5 Abs. 3 und 30 Abs. 1 E-DSG). Die Rechtsgrundlage für die Bearbeitung (insbesondere die Beschaffung und die Bekanntgabe) der jeweiligen Personendaten bzw. Daten juristischer Personen muss sich indessen in jedem Fall aus dem Spezialrecht ergeben. Die vorliegende Bestimmung erlaubt die Bearbeitung in prozessorientierter Hinsicht.

Mit dem Verweis auf die gesetzlichen Grundlagen für die Bekanntgabe in *Absatz 2* wird ausdrücklich klargestellt, dass diese im Spezialrecht vorhanden sein müssen. Ist das der Fall, kann eine Bekanntgabe mittels Gewährung des (entsprechend beschränkten) Zugriffs auf das GEVER-System der hauptzuständigen Verwaltungseinheit umgesetzt werden.

Absatz 3 entspricht dem bisherigen Artikel 57*h* Absatz 1, zweiter Satz, RVOG. Die Bestimmung wird redaktionell leicht angepasst. Mit der Revision des DSG soll der Begriff der Persönlichkeitsprofile gestrichen werden; die Streichung ist hier nachzuvollziehen. Aufgrund der Aufhebung des Schutzes der Personendaten juristischer Personen im E-DSG ist hier zudem ausdrücklich festzuhalten, dass die Geschäftsverwaltungssysteme auch besonders schützenswerte Daten juristischer Personen (d.h. Daten betreffend verwaltungs- und strafrechtliche Verfolgungen und Sanktionen oder Berufs-, Geschäfts- und Fabrikationsgeheimnisse; vgl. Art. 57*r* Abs. 2) enthalten können (vgl. auch die Erläuterungen in Ziff. 9.1.11).

Absatz 4: Diese Bestimmung ist an sich deklaratorisch; der Grundsatz, dass der Zugang zu beschränken ist, ergibt sich unmittelbar aus dem Verhältnismässigkeitsgebot (Art. 5 Abs. 2 BV, Art. 4 Abs. 2 DSG bzw. Art. 5 Abs. 2 E-DSG). Die Verantwortung für die Zugangsbeschränkung liegt beim verantwortlichen Bundesorgan. Die diesbezüglich absolute Formulierung des geltenden Artikel 57*h* Absatz 2 RVOG, die den Zugang «ausschliesslich» auf Mitarbeiterinnen und Mitarbeiter des betreffenden Bundesorgans beschränkt, ist indessen nicht adäquat. Die prozessorientierten Zugriffsmöglichkeiten werden regelmässig bedingen, dass von «aussen» etwa auch auf Metadaten zugegriffen werden kann, die z. B. Namen, Telefonnummern und Mailadressen von Verwaltungsmitarbeitenden enthalten.

Die künftigen GEVER-Systeme sehen Möglichkeiten zur rollenbasierten Regelung von Zugriffen sowie eine systematische Datenverschlüsselung vor und bieten so hinreichende Möglichkeiten, diese Bestimmung in der Praxis umzusetzen. Einzelheiten werden auf Verordnungsstufe zu regeln sein (vgl. die heutigen Art. 6 ff. GEVER-Verordnung). Dort können gegebenenfalls auch die Sicherheitsanforderungen geregelt werden, welche diejenigen Personen und Organisationen ausserhalb der Bundesverwaltung zu treffen haben, denen ein Systemzugriff gewährt wird.

*Art. 57h^ter^* Ausführungsbestimmungen

Artikel 57*h*^ter^ entspricht im Wesentlichen dem bisherigen Artikel 57*h* Absatz 3 RVOG. Die Delegationsbestimmung umfasst auch die Befugnis, für die Einheiten der dezentralen Bundesverwaltung hinsichtlich der Vorgaben für die zu verwendenden Systeme besondere Regeln vorzusehen.

Indessen hat der Bund mit der neu beschafften Bundeslizenz Acta Nova das Recht erworben, auch die dezentralen Einheiten der Bundesverwaltung mit dem neuen GEVER-System auszustatten, ohne dass zusätzliche Lizenzkosten anfallen. Mittel- und langfristig ist daher anzustreben, dass auch diese Einheiten mit dem Bundesstandard arbeiten, um so Kosten zu sparen und die elektronische, verwaltungseinheitsübergreifende Zusammenarbeit zu vereinfachen.

Art. 57i Verhältnis zu anderem Bundesrecht

In Artikel 57*i* ist aus Gründen der Rechtssicherheit klarzustellen, dass sich der in dieser Bestimmung vorgesehene Vorbehalt anderer Bundesgesetz auch auf die Bearbeitung von Daten juristischer Personen bezieht (vgl. die Erläuterungen in Ziff. 9.1.11).

Art. 57j Grundsätze

Auch in Artikel 57*j* Absatz 1 und 2 ist aufgrund der Aufhebung des Schutzes der Daten juristischer Personen im E-DSG sowie der Beschränkung des Begriffs der Personendaten in Artikel 4 Buchstabe a E-DSG auf Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, aus Gründen der Rechtssicherheit festzuhalten, dass diese Bestimmungen auf Daten juristischer Personen Anwendung finden (vgl. oben die Erläuterungen in Ziff. 9.1.11). Zu den besonders schützenswerten Daten juristischer Personen gemäss Absatz 2 gehören Daten über verwaltungs- und strafrechtliche Verfolgungen und Sanktionen oder Berufs-, Geschäfts- und Fabrikationsgeheimnisse (vgl. Art. 57*r* Abs. 2).

In Absatz 2 wird ausserdem der Begriff «Persönlichkeitsprofil» gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 57k Einleitungssatz

Der Begriff der «Personendaten» wird um «Daten juristischer Personen» ergänzt. Siehe dazu die vorangehenden Erläuterungen sowie die Erläuterungen unter Ziff. 9.1.11.

Art. 57l Sachüberschrift, Einleitungssatz und Bst. b Ziff. 4

Der Begriff der «Personendaten» in der Sachüberschrift und im Einleitungssatz wird um «Daten juristischer Personen» ergänzt. Siehe dazu die vorangehenden Erläuterungen sowie die Erläuterungen unter Ziffer 9.1.11.

Der Begriff «Datensammlung» in Buchstabe b Ziffer 4 wird durch «elektronische Infrastruktur» ersetzt. Siehe die Erläuterungen unter Ziffer 9.1.11.

Art. 57r Bearbeitung von Daten juristischer Personen

Aufgrund des Verzichts auf den Schutz der Personendaten juristischer Personen gelten die bundesrechtlichen Gesetzesgrundlagen für die Bearbeitung von Personendaten durch Bundesorgane nicht mehr, wenn diese Daten juristischer Personen bearbeiten. Nach Artikel 5 BV ist das Recht die Grundlage staatlichen Handelns.

Ausserdem müssen die Bundesorgane jede Aufgabe, die die Privatsphäre einer juristischen Person verletzen (Art. 13 BV) oder deren Wirtschaftsfreiheit einschränken (Art. 27 BV) kann, unter Beachtung der Voraussetzungen nach Artikel 36 BV erfüllen (Vorliegen einer gesetzlichen Grundlage sowie eines überwiegenden öffentlichen Interesses und Beachtung des Grundsatzes der Verhältnismässigkeit). Der Bundesrat ist demnach der Ansicht, dass eine allgemeine gesetzliche Grundlage geschaffen werden muss, mit der die Bundesorgane ermächtigt werden, Daten juristischer Personen, einschliesslich besonders schützenswerter Daten, zu bearbeiten, soweit die Erfüllung ihrer Aufgaben dies erfordert und diese Aufgaben in einem Gesetz im formellen Sinn umschrieben sind (Abs. 1). Für den Begriff der «Bundesorgane» ist auf die Legaldefinition in Artikel 4 Buchstabe h E-DSG abzustellen, weshalb beispielsweise auch die dezentralisierten Verwaltungseinheiten darunter fallen.

In Absatz 2 der Bestimmung wird der Begriff der besonders schützenswerten Daten juristischer Personen definiert. Dabei handelt es sich um Daten über verwaltungs- und strafrechtliche Verfolgungen und Sanktionen (Bst. a) oder Daten über Berufs-, Geschäfts- und Fabrikationsgeheimnisse (Bst. b).

Art. 57s Bekanntgabe von Daten juristischer Personen

Abs. 1 Bekanntgabe von Daten juristischer Personen

In dieser Bestimmung ist der Grundsatz verankert, wonach Bundesorgane Daten juristischer Personen bekannt geben dürfen, wenn eine Rechtsgrundlage es vorsieht. Diese kann in einem völkerrechtlichen Vertrag, einem Gesetz im formellen Sinn oder in einer Verordnung vorgesehen sein. Der allgemeine Grundsatz entspricht jenem in Artikel 32 Absatz 1 E-DSG über die Bekanntgabe von Personendaten.

Abs. 2 Voraussetzung einer Grundlage in einem Gesetz im formellen Sinn

Gemäss dieser Bestimmung dürfen Bundesorgane besonders schützenswerte Daten juristischer Personen, d.h. Daten über verwaltungs- und strafrechtliche Verfolgungen und Sanktionen oder Berufs-, Geschäfts- und Fabrikationsgeheimnisse, ausschliesslich bekannt geben, wenn ein Gesetz im formellen Sinn es vorsieht. Denn die Bekanntgabe solcher Informationen kann eine schwerwiegende Einschränkung der Grundrechte einer juristischen Person im Sinne von Artikel 36 Absatz 1 zweiter Satz BV darstellen. Es ist folglich eine Grundlage in einem Gesetz im formellen Sinn erforderlich.

Abs. 3 Ausnahmen

Nach Absatz 3 kann von der Anforderung einer gesetzlichen Grundlage gemäss den Absätzen 1 und 2 abgewichen werden, wenn eine der Voraussetzungen nach den Buchstaben a–c erfüllt ist. Die Bestimmung entspricht den Ausnahmen nach Artikel 32 Absatz 2 Buchstaben a, b und e E-DSG.

Die Absätze 4–6 entsprechen der Regelung nach Artikel 32 Absätze 3, 5 und 6 E-DSG.

Art. 57t Rechte der juristischen Personen

Der Bundesrat ist der Ansicht, dass die Rechte der juristischen Personen, wie sie sich aus Artikel 13 Absatz 2 BV ergeben, durch das anwendbare Verfahrensrecht hinreichend gewährleistet sind und nicht ausdrücklich ein typisch datenschutzrechtliches Auskunfts- oder Berichtigungsrecht eingeführt werden muss. So können die juristischen Personen in einem erstinstanzlichen Verwaltungsverfahren nach Artikel 26 ff. VwVG die Akten einsehen, ihren Anspruch auf rechtliches Gehör nach Artikel 29 ff. VwVG geltend machen und gegebenenfalls gegen die Verfügung der zuständigen Behörde Beschwerde erheben. Die juristischen Personen können sich auch auf Artikel 25*a* VwVG berufen. Nach dieser Bestimmung kann jede Person, die ein schutzwürdiges Interesse hat, von der Behörde, die für Realakte zuständig ist, die sich auf öffentliches Recht des Bundes stützen und Rechte oder Pflichten berühren, verlangen, dass sie eine beschwerdefähige Verfügung erlässt. Auf diese Weise könnten juristische Personen ein Recht auf Berichtigung bzw. Vernichtung ihrer Daten erlangen.

9.2.9 Bundespersonalgesetz vom 24. März 2000[214]

Art. 27 Abs. 2 Einleitungssatz und Bst. b

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Es wird darauf hingewiesen, dass Artikel 27 durch die Revision vom 16. Juni 2017 des Bundesgesetzes über die Anstalt zur Verwaltung der Ausgleichsfonds von AHV, IV und EO[215] geändert wurde. Die Koordinationsbestimmungen (vgl. Ziff. 13.7) berücksichtigen den neuen Wortlaut dieser Bestimmung und die Aufhebung des Begriffs «Persönlichkeitsprofil».

Art. 27d Abs. 2 Einleitungssatz und 4 Einleitungssatz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.10 Verwaltungsgerichtsgesetz vom 17. Juni 2005[216]

Art. 35 Bst. b

Diese Bestimmung kann aufgehoben werden, da der E-DSG dem Beauftragten die Verfügungskompetenz zuspricht (Art. 44 und 45 E-DSG).

214 SR **172.220.1**
215 BBl **2017** 4219
216 SR **173.32**

9.2.11 Zivilgesetzbuch[217]

Art. 45a Abs. 3 Ziff. 3

In Artikel 45*a* Absatz 3 Ziffer 3 E-ZGB[218] wird der Bundesrat beauftragt, unter Mitwirkung der Kantone die Aufsicht über das elektronische Zivilstandsregister zu regeln. Es geht insbesondere darum, Artikel 83 der Zivilstandsverordnung vom 28. April 2004[219] anzupassen. Dies kann beispielsweise in Anlehnung an Artikel 55 Absatz 1 der N-SIS-Verordnung vom 8. März 2013[220] erfolgen, wonach die kantonalen Datenschutzbehörden und der Beauftragte im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammenarbeiten und für eine koordinierte Aufsicht über die Bearbeitung von Personendaten sorgen. In Bezug auf die Aufsicht über das elektronische Zivilstandsregister dürfen der Beauftragte und die kantonalen Datenschutzbehörden nicht in die Kompetenz der Gerichte zur Änderung streitiger Daten eingreifen (Art. 42 ZGB).

Es wird darauf hingewiesen, dass Artikel 45*a* ZGB im Rahmen der Revision des Bundesrates vom 16. April 2014[221] geändert wurde. Die Koordinationsbestimmungen (vgl. Ziff. 13.7) berücksichtigen den neuen Wortlaut dieser Bestimmung und sehen die nötigen Änderungen vor.

9.2.12 Revisionsaufsichtsgesetz vom 16. Dezember 2005[222]

Art. 15b Bearbeitung von Personendaten und von Daten juristischer Personen

Die Eidgenössische Revisionsaufsichtsbehörde (RAB) bearbeitet in Erfüllung ihrer gesetzlichen Aufgaben eine Vielzahl von Daten natürlicher und juristischer Personen. Sie erhebt diese insbesondere im Rahmen der gesetzlichen Auskunfts- und Herausgabepflichten (Art. 15*a* des Revisionsaufsichtsgesetzes [RAG]), im Rahmen ihrer Überprüfungen (Art. 16 RAG) und auf dem Weg der Amtshilfe (Art. 22 ff. RAG). Dazu gehören allgemeine Daten wie Kontakt- und Identifikationsdaten einer Gesuchstellerin oder eines Gesuchstellers bzw. einer Zulassungsträgerin oder eines Zulassungsträgers, aber auch konkrete zulassungs- und aufsichtsrelevante Daten, z. B. zu Ausbildungen und beruflichem Werdegang, Auszüge aus dem Strafregister, Daten im Zusammenhang mit relevanten Straf- oder Verwaltungsstrafverfahren und Verfahren der zivil- oder verwaltungsrechtlichen Verantwortlichkeit oder Informationen zur Organisation und zum Betrieb von Revisionsunternehmen und zur Durchführung von Revisionsdienstleistungen. Aus Gründen der Rechtssicherheit wird in Artikel 15*b* E-RAG klargestellt, dass die RAB zur Erfüllung all ihrer gesetzlichen Aufgaben Personendaten und Daten juristischer Personen, einschliesslich besonders

217 SR **210**
218 Vgl. die Botschaft des Bundesrates vom 16. April 2014 betreffend die Änderungen des Zivilgesetzbuches (Beurkundung des Personenstands und Grundbuch), BBl **2014** 3551.
219 SR **211.112.2**
220 SR **362.0**
221 BBl **2014** 3587
222 SR **221.302**

schützenswerter Daten, bearbeiten kann. Zu den besonders schützenswerten Daten juristischer Personen gehören namentlich Daten über die vorerwähnten Verfahren sowie über Berufs-, Geschäfts- und Fabrikationsgeheimnisse (vgl. auch die Erläuterungen in Ziff. 9.2.8).

9.2.13 Bundesgesetz vom 24. März 2000[223] über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten

Art. 1 zweiter Satz

Die Bestimmung ist überflüssig. Sie kann aufgehoben werden.

Art. 2 Abs. 1 und Abs. 2 erster Satz

Da der Begriff «Datensammlung» aufgehoben wird, muss Absatz 1 angepasst werden. Die Rechtsgrundlage für die Bearbeitung von Personendaten durch die zuständigen Dienste des EDA ändert sich jedoch nicht.

Absatz 2 wird in zwei Punkten geändert. Erstens wird der Begriff «Datensammlungen» gestrichen. Zweitens wird der Begriff «Persönlichkeitsprofile» durch «Personendaten zur Beurteilung der Eignung von Personen für Einsätze nach Absatz 1» ersetzt.

Art. 5 Abs. 1 Einleitungssatz und Abs. 3

Der Begriff «Datensammlungen» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2. In der deutschen Fassung wird der Begriff «administrative und strafrechtliche Massnahmen» an die Terminologie von Artikel 4 Buchstabe c Ziffer 5 E-DSG angepasst.

Art. 6 Bst. a

Der Begriff «Datensammlungen» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Es wird darauf hingewiesen, dass sich das Bundesgesetz vom 24. März 2000 über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten in Revision befindet. Die Vernehmlassung zum Vorentwurf des Bundesrates vom 28. Juni 2017 endet am 20. Oktober 2017. Gegebenenfalls müssen gewisse Begriffe dieses Gesetzes an die neuen Begrifflichkeiten des künftigen DSG angepasst werden.

223 SR **235.2**

9.2.14 Bundesgesetz vom 19. Dezember 1986[224] gegen den unlauteren Wettbewerb

Art. 22 Abs. 2 zweiter Satz

Der Verweis auf Artikel 6 DSG muss an die neue Nummerierung des E-DSG (Art. 13 und 14) angepasst werden.

9.2.15 Zivilprozessordnung[225]

Die vorgeschlagenen Änderungen der Zivilprozessordnung (ZPO) wurden in der Vernehmlassung grundsätzlich begrüsst.

Art. 20 Bst. d Gerichtsstand

Artikel 20 ZPO regelt neu den Gerichtsstand für sämtliche zivilrechtlichen Begehren nach dem DSG. Diese sind namentlich das Einsichts- und Löschungsrecht nach Artikel 16 E-DSG, das Auskunftsrecht nach Artikel 23 E-DSG und die verschiedenen Klagen nach Artikel 28 E-DSG.

Befreiung von den Gerichtskosten

Die Evaluation des DSG hat ergeben, dass die betroffenen Personen ihre Rechte kaum wahrnehmen bzw. auf dem Rechtsweg durchsetzen, insbesondere im privaten Sektor.[226] Dies liegt gerade im Kostenrisiko für die betroffene Person begründet und verringert die Wirksamkeit des DSG erheblich. Zudem fehlt es als Konsequenz davon im Bereich des DSG an einer differenzierten Gerichtspraxis, welche die Normen konkretisiert und dadurch mehr Rechtssicherheit gibt.

Als zentrale Massnahme zur Erleichterung der prozessualen Durchsetzung der datenschutzrechtlichen Ansprüche der betroffenen Personen sollen daher zivilrechtliche Verfahren nach dem DSG neu von den Gerichtskosten befreit werden, wie dies bereits für andere Verfahren und Bereiche vorgesehen ist (z. B. Verfahren nach dem Gleichstellungsgesetz oder arbeitsrechtliche Streitigkeiten bis zu einem Streitwert von 30 000 Franken sowie Streitigkeiten nach dem Mitwirkungsgesetz vom 17. Dezember 1993[227]). Damit wird das Kostenrisiko für betroffene Personen in einem wichtigen Punkt verringert. Da die Mehrheit der datenschutzrechtlichen Ansprüche nicht vermögensrechtliche Streitigkeiten sind, erscheint eine Streitwertgrenze wie im Arbeitsrecht nicht sinnvoll. Aufgrund der bisherigen Fallzahlen ist es unwahrscheinlich, dass durch die Änderung die Anzahl der Verfahren sprunghaft ansteigen würde oder solche leichtfertig angestrengt würden. Dies gilt insbesondere als die betroffene Person im Unterliegensfall nach wie vor eine Parteientschädigung leisten und ihre Parteikosten selbst tragen muss und bei bös- oder mutwilliger Pro-

224 SR **241**
225 SR **272**
226 Vgl. S. 90 f. und 219 des Schlussberichts zur Evaluation des Bundesgesetzes über den Datenschutz vom 10. März 2011.
227 SR **822.14**

zessführung auch in unentgeltlichen Verfahren Gerichtskosten auferlegt werden können (Art. 115 ZPO).

Art. 99 Abs. 3 Bst. d

Für Verfahren nach dem DSG soll die Pflicht der klagenden Partei gemäss Artikel 99 Absatz 1 ZPO, auf Antrag der beklagten Partei eine Sicherheit für deren Parteientschädigung leisten zu müssen, abgeschafft werden. Damit soll die finanzielle Belastung für klagende Parteien weiter gesenkt werden.

Dies betrifft Verfahren über zivilrechtliche Klagen nach Artikel 28 des VE, die im ordentlichen Verfahren behandelt werden. Insbesondere diese Klagen wurden bisher praktisch nie erhoben und deren Einleitung wird mit der vorgeschlagenen Änderung erleichtert. Soweit für Verfahren nach Artikel 243 Absatz 2 Buchstabe d ZPO das vereinfachte Verfahren gilt, sind diese bereits nach geltendem und unverändertem Recht von der Pflicht zur Sicherstellung der Parteientschädigung ausgenommen (siehe Art. 99 Abs. 3 ZPO).

Art. 113 Abs. 2 Bst. g

Die Zivilprozessordnung soll dahingehend ergänzt werden, dass neu in Verfahren nach dem DSG auch im Schlichtungsverfahren, das im ordentlichen wie im vereinfachten Verfahren grundsätzlich obligatorisch ist (Art. 197 ZPO), keine Gerichtskosten ausgesprochen werden, wie dies nach geltendem Recht für bestimmte Streitigkeiten vorgesehen ist, zum Beispiel für miet- und pachtrechtliche Streitigkeiten über Wohn- und Geschäftsräume oder Streitigkeiten nach dem Mitwirkungsgesetz (siehe Art. 113 Abs. 22 ZPO).

Durch die Befreiung von den Gerichtskosten reduziert sich das Kostenrisiko bei der Einleitung einer Klage der betroffenen Person bei allen zivilrechtlichen Klagen nach dem DSG. Dies fällt umso mehr ins Gewicht, als im Schlichtungsverfahren grundsätzlich keine Parteientschädigungen gesprochen werden (Art. 113 Abs. 1 Satz 1 ZPO). Grundsätzlich selbst zu tragen sind die Kosten für einen eigenen Rechtsvertreter, es sei denn, es werde eine unentgeltliche Rechtsbeiständin oder ein unentgeltlicher Rechtsbeistand bestellt.

Art. 114 Bst. f

Die Zivilprozessordnung soll dahingehend ergänzt werden, dass in Verfahren nach dem DSG im Entscheidverfahren keine Gerichtskosten gesprochen werden, wie dies zum Beispiel auch für Streitigkeiten nach dem Gleichstellungs- oder Mitwirkungsgesetz oder für arbeitsrechtliche Streitigkeiten bis zu einem Streitwert bis 30 000 Franken gilt.

Durch diese wichtige Neuregelung werden Entscheidverfahren nach dem DSG von den Gerichtskosten ausgenommen, wodurch das Kostenrisiko der betroffenen Person gesenkt wird. Die Parteikosten werden hingegen nach den üblichen Grundsätzen (Art. 104 ff. ZPO) verlegt.

Art. 243 Abs. 2 Bst. d Verfahrensart

Ansprüche nach Artikel 16 E-DSG können wie das Auskunftsrecht im vereinfachten Verfahren geltend gemacht werden. Die Anpassung der Bestimmung ist nötig, weil Artikel 16 ins Gesetz eingefügt wurde.

Art. 407d Übergangsbestimmung

Übergangsrechtlich sollen die neuen Verfahrensbestimmungen mit dem Inkrafttreten auf sämtliche Verfahren anwendbar werden, und zwar auch auf solche, die bereits rechtshängig sind. Insbesondere sollen auch für diese keine Sicherheit mehr geleistet werden müssen und keine Gerichtskosten mehr gesprochen werden (Art. 113 Abs. 2 Bst. g und Art. 114 Bst. f E-ZPO).

9.2.16 Bundesgesetz vom 18. Dezember 1987[228] über das Internationale Privatrecht

Art. 130 Abs. 3

Wie bereits ausgeführt (vgl. Ziff. 9.2.2), ist das Konzept der Datensammlung durch die technische Entwicklung überholt. Zudem wird es in Rechtsordnungen anderer Staaten kaum verwendet. Auch der E-DSG stellt nun ausschliesslich auf die Datenbearbeitung ab. Damit erscheint es angezeigt, Artikel 130 Absatz 3 des Bundesgesetzes über das Internationale Privatrecht (IPRG), wo vom «Ort, wo die Datensammlung geführt oder verwendet wird» die Rede ist, ebenfalls anzupassen.

Artikel 130 E-IPRG sieht weiterhin vor, dass Klagen zur Durchsetzung eines Auskunfts- oder Einsichtsrechts im Zusammenhang mit der Bearbeitung von Personendaten bei den Gerichten nach Artikel 129 IPRG eingereicht werden können. Demgemäss kann die berechtigte Person in der Schweiz nach ihrer Wahl an folgenden Orten klagen: Am Ort des Wohnsitzes oder, bei Fehlen eines solchen, des gewöhnlichen Aufenthalts der pflichtigen Person, am Ort der betroffenen Geschäftsniederlassung derselben sowie am Handlungs- oder Erfolgsort. Die unerlaubte Handlung im Sinne von Artikel 129 IPRG besteht vorliegend in der Nichtgewährung eines bestehenden Auskunfts- oder Einsichtsrechts. Handlungsort ist daher der Ort, von dem aus die Auskunftserteilung oder Einsichtsgewährung hätte erfolgen müssen.[229] Dies ist in der Regel der Ort, wo die pflichtige Person die Tätigkeit ausübt, in deren Rahmen die fragliche Datenbearbeitung stattfindet. Erfolgsort ist der Ort, an dem die

228 SR **291**

229 Vgl. BGE **113** II 476 E. 3 und **125** III 346 E. 4c/bb zum Handlungsort bei Unterlassungen.

berechtigte Person ihre Auskunft hätte erhalten bzw. Einsicht hätte nehmen sollen. Dies ist in der Regel der Ort ihres gewöhnlichen Aufenthalts.[230]

Anders als in der Vernehmlassungsvorlage ist nicht mehr von einer alternativen Klagemöglichkeit «am Ort, wo der betreffende Vorgang stattfindet» (der betreffende Passus sollte die bisherige alternative Anknüpfung an den Ort, «wo die Datensammlung geführt oder verwendet wird», ersetzen) die Rede. Es darf davon ausgegangen werden, dass sich auch ein auf ausländischem Recht basierendes Auskunfts- oder Einsichtsrecht gegen die Person richtet, die für die Datenbearbeitung verantwortlich ist (vgl. z. B. Artikel 15 der Verordnung [EU] 2016/679). Als Ort der Datenbearbeitung muss hier sinnvollerweise der Ort gelten, an dem die betreffende Person die Tätigkeit ausübt, in deren Rahmen die fragliche Datenbearbeitung stattfindet.[231] Dieser entspricht dem bereits in Artikel 129 Absatz 1 IPRG erwähnten Handlungsort (vgl. den vorangehenden Absatz). In aller Regel dürfte der besagte Ort auch mit demjenigen der involvierten Geschäftsniederlassung gleichzusetzen sein[232], welcher in Artikel 129 Absatz 1 IPRG ebenfalls aufgeführt wird. Für gewisse Autoren ergibt sich der Gerichtsstand am Ort der Datenbearbeitung gar aus dem Erfolgsortgerichtsstand des Artikel 129 Absatz 1 IPRG.[233] Vor diesem Hintergrund hätte der nunmehr gestrichene Passus keinen Mehrwert gebracht, sondern im Gegenteil lediglich Verwirrung gestiftet.

In einigen Eingaben zum Vernehmlassungsverfahren wurde ein ergänzender Satz in Artikel 139 Absatz 3 IPRG beantragt. Die bestehende Bestimmung sieht vor, dass Artikel 139 Absatz 1 IPRG, der das auf Persönlichkeitsverletzungen anwendbare Recht regelt, auch für «Ansprüche aus Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten sowie aus Beeinträchtigung des Rechts auf Auskunft über Personendaten» gilt. Der beantragte ergänzende Satz würde wie folgt oder sinngemäss lauten: «Dabei kann ein ausländischer Erfolgsort im Sinne von Absatz 1 Buchstabe c nicht allein damit begründet werden, dass die Daten im betreffenden Land gespeichert sind.» Der Bundesrat sieht von einer entsprechenden Änderung ab, da er sie als unnötig erachtet. Der Erfolgsort im Sinne des erwähnten Absatz 1 Buchstabe c ist nämlich nach Massgabe der geltend gemachten Verletzungshandlung zu bestimmen. Der blosse Ort der Datenspeicherung kommt daher nur in bestimmten Fällen als Erfolgsort in Betracht, etwa wenn geltend gemacht wird, dass die Art und Weise der Speicherung datenschutzrechtliche Bestimmungen verletzt.[234] So gesehen kann ein Erfolgsort im Sinne von Absatz 1 Buchstabe c nie allein damit begründet

230 Vgl. Rosenthal David, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 139 IPRG N 24; gleiches Ergebnis bei Vischer Frank, in: ZK-IPRG, 2. A., Zürich 2004, Art. 139 IPRG N 28; Umbricht Robert/Rodriguez Rodrigo/Krüsi Melanie, in: Honsell Heinrich/ Vogt Nedim Peter, Schnyder Anton K./Berti Stephen V. (Hrsg.), BSK-IPRG, 3. A., Basel 2013, Art. 130 IPRG N 11, und Bonomi Andrea, in: Bucher Andreas (Hrsg.), CR-LDIP/CL, Art. 139 IPRG N 16; vorliegend an den gewöhnlichen Aufenthalt der berechtigten Person anzuknüpfen wäre wohl auch nach Dasser Felix, in: BSK-IPRG, a.a.O., Art. 139 IPRG N 43.

231 Vgl. Dasser, in: BSK-IPRG, a.a.O., Art. 139 IPRG N 45.

232 Vgl. Die zivilrechtliche Verantwortlichkeit von Providern, Bericht des Bundesrates vom 11. Dezember 2015, S. 90 ff.

233 So etwa Bucher Andreas, Le premier amendement de la LDIP, in: Etudes de droit international en l'honneur de Pierre Lalive, Basel 1993, S. 8.

234 Vgl. Rosenthal, Handkommentar zum Datenschutzgesetz, a.a.O., Art. 139 IPRG N 22.

werden, dass die Daten im betreffenden Staat gespeichert sind. Bei Klagen zur Durchsetzung eines Auskunfts- oder Einsichtsrechts würde nach dem oben Ausgeführten kaum je das Recht eines blossen Speicherorts zur Anwendung gelangen.

9.2.17 Strafgesetzbuch[235]

Art. 179novies Unbefugtes Beschaffen von Personendaten

Die Bestimmung ist nicht mehr auf die Daten juristischer Personen anwendbar, da diese nicht mehr dem DSG unterstehen. Die Übergangsbestimmung gemäss Artikel 66 E-DSG gelangt nicht zur Anwendung. Zur Berücksichtigung der Aufhebung der Begriffe «Persönlichkeitsprofil» und «Datensammlung» im E-DSG werden diese in der Bestimmung ausserdem gestrichen. Schliesslich wird die Wendung «nicht frei zugänglich» durch «nicht für jedermann zugänglich» ersetzt.

Art. 179decies Identitätsmissbrauch

Der Bundesrat wird mit der durch das Parlament angenommenen Motion 14.3288 Comte beauftragt, einen Entwurf zur Änderung des Strafrechts auszuarbeiten, damit der Missbrauch einer Identität, der eine schwerwiegende Verletzung der Persönlichkeit darstelle, eine strafbare Handlung für sich wird.

Die Identität eines Menschen ist durch verschiedene konstituierende Merkmale bestimmbar, etwa durch seinen Namen, seine Herkunft, sein Bild, die soziale, familiäre oder berufliche Positionierung, sowie durch andere persönliche Daten wie Geburtsdatum, Internetadresse, Kontonummer oder *Nickname*.

Die vorgeschlagene Strafbestimmung gegen den Identitätsmissbrauch schützt die Persönlichkeit des Individuums. Das Recht auf Respektierung und Achtung seiner Identität soll unter strafrechtlichen Schutz gestellt werden, indem der Missbrauch der Identität als Teil seiner Persönlichkeit bestraft wird. Die systematische Einordnung erfolgt unter den Titel der strafbaren Handlungen gegen die Ehre und den Geheim- oder Privatbereich[236]. Es soll jedoch davon abgesehen werden, die Verwendung einer fremden Identität zum Selbstzweck, um ihrer selbst willen, unter Strafe zu stellen, da dadurch die Grenzen des Strafrechts zu stark ausgeweitet würden. Der Täter muss vielmehr in der Absicht handeln, einen Schaden zu verursachen oder einen Vorteil zu erwirken. Die Verwendung einer Identität aus reinem Übermut oder als Scherz fällt damit nicht unter die Bestimmung. Die Verwendung einer neuen, fiktiven Identität fällt ebenso wenig in den Anwendungsbereich.

Das Phänomen und die Problematik des Missbrauchs einer fremden Identität haben sich durch den verbreiteten Gebrauch elektronischer Medien und entsprechender Kommunikationsmittel akzentuiert und verschärft. Die praktische Schwelle, in fremdem Namen auf sozialen Medien Äusserungen abzugeben oder via elektronischer Kommunikationsmittel entsprechende Handlungen auszuführen, hat sich im

235 SR **311.0**
236 Art. 173 ff. StGB.

Vergleich zur herkömmlichen Kommunikation deutlich gesenkt. Die vorgeschlagene Strafbestimmung soll jedoch unabhängig vom Tatmittel und Medium, mit dem die Tat begangen wird, Anwendung finden. Auch der herkömmliche Missbrauch einer Identität, beispielsweise eine schriftlich erfolgte Warenbestellung oder eine persönliche, mündliche Kontaktaufnahme im Vorfeld eines sogenannten Enkeltrick-Betruges, wird durch die Strafbestimmung erfasst. Es wird somit davon abgesehen, lediglich den mittels eines Computers oder eines Telefons begangenen Identitätsmissbrauch unter Strafe zu stellen.

Der in der Strafbestimmung statuierte Nachteil für den durch den Identitätsmissbrauch Betroffenen muss eine gewisse Schwere erreichen und kann materieller oder immaterieller Natur sein. Die Absicht, beim Betroffenen einen massiven Ärger auszulösen, kann als Nachteilsabsicht bereits ausreichen[237].

Bei der Verwendung einer fremden Identität in Schädigungsabsicht oder zwecks Erlangung eines unrechtmässigen Vorteils stellt sich in der Regel die Frage nach der Anwendung weiterer Strafbestimmungen wie Betrug, Urkundenfälschung oder Delikte gegen die Ehre. In Fällen, in welchen der Unrechtsgehalt der Tat durch den gleichzeitig anwendbaren Tatbestand nicht gänzlich abgedeckt wird, der Aspekt der Persönlichkeitsverletzung durch den Identitätsmissbrauch also noch nicht berücksichtigt wird, ist von echter Konkurrenz auszugehen. Beide Strafbestimmungen finden Anwendung. Nimmt der Täter beispielsweise auf einem sozialen Netzwerk die Identität von B an und verleumdet C, wird neben dem Straftatbestand der Verleumdung auch der neu zu schaffende Tatbestand des Identitätsmissbrauchs angewendet. Nur so wird das gegen B begangene Unrecht geahndet und die bei diesem entstandenen negativen Folgen wie Reputationsverlust, Einleitung eines Verfahrens oder eine aufwändige und nur bedingt erfolgreiche Richtigstellung berücksichtigt. Im Falle des unbefugten Beschaffens von Personendaten[238] und dem anschliessenden Missbrauch der entsprechenden Identität kommen ebenfalls beide Strafbestimmungen zur Anwendung. Erfolgt der Identitätsmissbrauch als Teil einer betrügerischen Handlung mit dem Ziel, einen unrechtmässigen Vorteil zu erlangen, kann der Betrugstatbestand auch den (in der Regel vorgelagerten) Tatbestand des Identitätsmissbrauchs umfassen, womit dieser mitbestraft ist.

Die gesetzliche Strafandrohung soll verhältnismässig sein zum Wert des geschützten Rechtsguts sowie zum Unrechtsgehalt der Straftat. Andernfalls verliert das Strafrecht an Glaubwürdigkeit und an präventiver Wirkungskraft. Die vom Phänomen des Missbrauchs einer fremden Identität ausgehende Gefahr soll, gerade im digitalen Zeitalter, nicht unterschätzt oder verharmlost werden, auch wenn der konkrete Unrechtsgehalt der Tat und die Folgen für die geschädigte Person nicht in jedem Fall schwer sein müssen. Entsprechend wird der neue Straftatbestand als Vergehen ausgestaltet und mit einer Strafandrohung von Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe versehen.

237 Vgl. zum identischen Tatbestandselement beim Amtsmissbrauch Heimgartner Stefan, in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar, Strafrecht II, 3. Aufl., Basel 2013, Art. 312 StGB N 23.

238 Art. 179novies StGB

Gesetzlich erlaubte und damit rechtmässige Handlungen, zum Beispiel im Rahmen polizeilicher Ermittlungen und Strafuntersuchungen, bleiben nach Artikel 14 des Schweizerischen Strafgesetzbuches vorbehalten und damit straffrei.

Art. 352 Abs. 2

Der E-DSG muss nicht mehr integral zitiert werden, weil die Abkürzung in Artikel 349*a* eingeführt wird (vgl. Änderung des StGB unter Ziff. II).

Art. 355a Abs. 1

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 365 Abs. 1 erster Satz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.18 Bundesgesetz vom 22. März 1974[239] über das Verwaltungsstrafrecht

Das Verwaltungsstrafrecht (VStrR) findet Anwendung, wenn die Verfolgung und Beurteilung von Widerhandlungen, die in der Verwaltungsgesetzgebung des Bundes mit Strafe bedroht sind, einer Verwaltungsbehörde des Bundes übertragen ist (Art. 1 und 2). Aufgrund des neuen Wortlauts von Artikel 2 Absatz 3 E-DSG, müssen die besonderen datenschutzrechtlichen Bestimmungen des VStrR geändert werden. Dazu wird die Regelung der StPO übernommen und an die Neuerungen dieser Vorlage angepasst.

Art. 18a Beschaffung von Personendaten

In dieser Bestimmung wird die Transparenz bei der Beschaffung von Personendaten geregelt. Sie entspricht der Regelung nach Artikel 95 StPO.

Art. 18b Bearbeitung von Personendaten

Siehe sinngemäss die Erläuterungen zu Artikel 95*a* E-StPO (Ziff. 9.3.2).

Art. 18c Bekanntgabe und Verwendung von Personendaten bei hängigem Strafverfahren

Diese Bestimmung regelt die Bekanntgabe und Verwendung von Daten in einem hängigen Verfahren. Sie entspricht der Regelung nach Artikel 96 StPO.

239 SR **313.0**

Art. 18d Auskunftsrecht bei hängigem Verfahren

Diese Bestimmung regelt die Auskunftsrechte in einem hängigen Verfahren. Sie entspricht der Regelung nach Artikel 97 StPO.

Art. 18e Richtigkeit der Personendaten

In dieser Bestimmung wird die Richtigkeit der Daten geregelt. Sie entspricht der Regelung nach Artikel 98 StPO. In Bezug auf Absatz 2 wird auf die Erläuterungen zu Artikel 98 Absatz 2 E-StPO verwiesen (vgl. Ziff. 9.3.2).

9.2.19 Militärstrafprozess vom 23. März 1979[240]

Die Militärjustiz ist eine unabhängige Gerichtsbehörde (Art. 1). Sie kann mit dem Begriff «Gericht» nach Artikel 2 Absatz 3 E-DSG gleichgesetzt werden. Der Militärstrafprozess sieht, anders als die StPO, jedoch keine eigenständigen Datenschutzbestimmungen vor. Der Bundesrat erachtet es daher als sinnvoll, das Gesetz entsprechend anzupassen, indem zum grossen Teil die Regelung der StPO übernommen und an die Neuerungen dieser Vorlage angepasst wird.

Art. 25a Beschaffung von Personendaten

In dieser Bestimmung wird die Transparenz bei der Beschaffung von Personendaten geregelt. Sie entspricht der Regelung nach Artikel 95 StPO.

Art. 25b Bearbeitung von Personendaten

Siehe sinngemäss die Erläuterungen zu Artikel 95*a* E-StPO (Ziff. 9.3.2).

Art. 25c Bekanntgabe und Verwendung von Personendaten bei hängigem Verfahren

Diese Bestimmung regelt die Bekanntgabe und Verwendung von Personendaten in einem hängigen Verfahren. Sie entspricht der Regelung nach Artikel 96 StPO.

Art. 25d Auskunftsrecht bei hängigem Verfahren

Diese Bestimmung regelt die Auskunftsrechte in einem hängigen Verfahren. Sie entspricht der Regelung nach Artikel 97 StPO.

Art. 25e Richtigkeit der Personendaten

In dieser Bestimmung wird die Richtigkeit der Daten geregelt. Sie entspricht der Regelung nach Artikel 98 StPO. In Bezug auf Absatz 2 wird auf die Erläuterungen zu Artikel 98 Absatz 2 E-StPO verwiesen.

240 SR **322.1**

9.2.20 Bundesgesetz vom 13. Juni 2008[241] über die polizeilichen Informationssysteme des Bundes

Art. 3 Abs. 2 erster Satz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 5 Sachüberschrift und Abs. 2

Nach Ansicht des Bundesrates kann Artikel 5 Absatz 2 BPI aufgehoben werden. Die Auftragsdatenbearbeitung, auch zu Kontroll- und Wartungszwecken, wird ausschliesslich durch Artikel 8 E-DSG geregelt. Dementsprechend muss auch die Sachüberschrift angepasst werden.

Art. 7 Abs. 1

Der Verweis auf den E-DSG wird angepasst.

9.2.21 ETH-Gesetz vom 4. Oktober 1991[242]

Art. 36a Abs. 1 erster Satz, Art. 36b Abs. 1 und 5 zweiter Satz und Art. 36c

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

In Artikel 36*c* Absatz 2 wird zudem der Verweis auf den E-DSG angepasst.

9.2.22 Sportförderungsgesetz vom 17. Juni 2011[243]

Art. 21 Abs. 3 Einleitungssatz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 25 Abs. 1 Einleitungssatz und Abs. 4

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2. Absatz 4 regelt die Bekanntgabe von Personendaten an die zuständigen Behörden eines Drittstaats durch den Verweis auf die Artikel 13 und 14 E-DSG.

241 SR **361**
242 SR **414.110**
243 SR **415.0**

9.2.23 Bundesgesetz vom 19. Juni 2015[244] über die Informationssysteme des Bundes im Bereich Sport

Art. 1 Abs. 1 Einleitungssatz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 4

Diese Bestimmung regelt die Datenbearbeitung für Arbeiten an den Informationssystemen. Sie kann aufgehoben werden. Die Auftragsdatenbearbeitung, auch zu Kontroll- und Wartungszwecken, wird ausschliesslich durch Artikel 8 E-DSG geregelt.

Art. 9 Einleitungssatz, Art. 14 Einleitungssatz, Art. 18 Einleitungssatz, Art. 22 Einleitungssatz, Art. 26 Einleitungssatz, Art. 32 Einleitungssatz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.24 Bundesstatistikgesetz vom 9. Oktober 1992[245]

Aufgrund der Aufhebung des Schutzes der Personendaten juristischer Personen müssen aus Gründen der Rechtssicherheit einige Bestimmungen des Bundesstatistikgesetzes geändert werden (vgl. auch die Erläuterungen in Ziff. 9.1.11). Der Bundesrat ist der Ansicht, dass im Bereich der Statistik für die natürlichen und die juristischen Personen dasselbe Datenschutzniveau gewährleistet sein muss. Des Weiteren werden einige Begriffe an die neue Terminologie des E-DSG angepasst.

Art. 5 Abs. 2 Bst. a und 4 Bst. a

Der Begriff «Personendaten» wird durch «Personendaten oder Daten juristischer Personen» ersetzt.

Art. 7 Abs. 2

Der Begriff «Datensammlung» wird durch «Datenbank» ersetzt (siehe die Erläuterungen unter Ziff. 9.2.2). Der Verweis auf Artikel 22 DSG muss an die neue Nummerierung des E-DSG (Art. 35) angepasst werden.

244 SR **415.1**
245 SR **431.01**

Art. 10 Abs. 4 und 5 zweiter Satz

In Absatz 4 wird der Begriff «Daten aus ihren Datensammlungen» durch «Daten aus ihren Datenbanken» ersetzt.

In Absatz 5 zweiter Satz wird der Verweis auf den E-DSG angepasst.

Art. 12 Abs. 2

Der Begriff «Datensammlung» wird durch «Datenbank» ersetzt.

Art. 14 Abs. 1

Der Begriff «der Betroffene» wird durch «die betroffene natürliche oder juristische Person» ersetzt.

Art. 14a Abs. 1 zweiter Satz

Nach dem Begriff «besonders schützenswerte [Personen-]Daten» wird der Ausdruck «besonders schützenswerte Daten juristischer Personen» eingefügt. Der Begriff «Persönlichkeitsprofile» wird durch «wesentliche Merkmale einer natürlichen oder juristischen Person» ersetzt.

Art. 15 Abs. 1

Der Begriff «Personendaten» wird durch «Personendaten oder Daten juristischer Personen» ersetzt. Der Grundsatz der Datensicherheit muss für beide Kategorien von Personen gelten.

Art. 16 Abs. 1

Aufgrund der Aufhebung des Schutzes der Daten juristischer Personen muss präzisiert werden, dass das künftige DSG ausschliesslich für die Bearbeitung von Personendaten über natürliche Personen gilt.

Art. 19 Abs. 2 Einleitungssatz

Der Begriff «Personendaten» wird durch «Personendaten und Daten juristischer Personen» ersetzt.

9.2.25 Bundesgesetz vom 18. Juni 2010[246] über die Unternehmens-Identifikationsnummer

Art. 3 Abs. 1 Bst. d und Art. 5 Abs. 1 Bst. b

Der Begriff «Datensammlung» wird ersetzt durch «Datenbank». Siehe die Erläuterungen unter Ziffer 9.2.2.

246 SR **431.03**

9.2.26 Nationalbibliotheksgesetz vom 18. Dezember 1992[247]

Art. 2 Abs. 2 und Art. 7

Betrifft nur den deutschen Text. Der Begriff «Datensammlung» wird in den Artikeln 2 Absatz 2 und Artikel 7 durch «Datenbank» ersetzt.

9.2.27 Bundesgesetz vom 16. März 2012[248] über den Verkehr mit Tieren und Pflanzen geschützter Arten

Art. 23 Abs. 2 erster Satz

Nach geltendem Recht dürfen Daten im Abrufverfahren bekannt gegeben werden, wenn die entsprechende ausländische Gesetzgebung einen angemessenen Schutz der Persönlichkeit der betroffenen Personen gewährleistet, und bestimmt der Bundesrat die Staaten sowie die supranationalen und internationalen Organisationen, die diesen Schutz gewähren. Zur Gewährleistung einer einheitlichen Regelung im Bundesrecht ist ein Verweis auf Artikel 13 E-DSG einzufügen.

9.2.28 Tierschutzgesetz vom 16. Dezember 2005[249]

Art. 20c Abs. 1 Einleitungssatz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.29 Militärgesetz vom 3. Februar 1995[250]

Art. 31 Abs. 2 zweiter Satz

Nach Artikel 31 Absatz 1 stehen den Angehörigen der Armee Dienste für die medizinische, seelsorgerische, psychologische und soziale Beratung und Betreuung im Zusammenhang mit dem Militärdienst zur Verfügung. Aufgrund der Art dieser Aufgaben muss der Begriff «Persönlichkeitsprofile» gestrichen werden.

247 SR **432.21**
248 SR **453**
249 SR **455**
250 SR **510.10**

Art. 99 Abs. 2 erster Satz und 3 Bst. d

Aufgrund der Art der Aufgaben des Nachrichtendienstes der Armee muss der Begriff «Persönlichkeitsprofil» in Absatz 1 erster Satz ersetzt werden durch «Personendaten, welche die Beurteilung des Grades der Gefährlichkeit einer Person erlauben». Diese Änderung entspricht dem Erfordernis einer gesetzlichen Grundlage nach Artikel 30 Absatz 2 Buchstabe c E-DSG.

In Absatz 3 Buchstabe d muss der Begriff «Datensammlung» durch «Datenbearbeitungstätigkeit» ersetzt werden. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 100 Abs. 2 erster Satz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 146

Der Begriff «Persönlichkeitsprofil» muss durch «Personendaten, welche die Beurteilung des Grades der Gefährlichkeit einer Person erlauben» ersetzt werden.

9.2.30 Geoinformationsgesetz vom 5. Oktober 2007[251]

Art. 11 Datenschutz

Der Absatz 1 entspricht dem heutigen Art. 11 des Geoinformationsgesetzes (GeoIG). Er hält fest, dass das künftige DSG auf alle Geobasisdaten des Bundesrechts Anwendung findet, bei denen es sich um Personendaten handelt. Gemäss der Botschaft vom 6. September 2006[252] zum Geoinformationsgesetz wird damit erreicht, «dass für alle Geobasisdaten des Bundesrechts eine einheitliche Regelung des Datenschutzes gilt, nämlich die des Bundes, und zwar unabhängig davon, ob eine Behörde des Bundes, des Kantons oder der Gemeinde oder eine im (hoheitlichen) öffentlichen Auftrag handelnde Privatperson die personenrelevanten Geobasisdaten bearbeitet. Bei Geobasisdaten des Bundesrechts, die der Datenherrschaft der Kantone oder Gemeinden unterstehen und Personendaten darstellen, bleibt die Datenschutzaufsicht trotz der Anwendbarkeit des DSG bei den kantonalen bzw. kommunalen Datenschutzaufsichtsbehörden.»

Soweit Geobasisdaten des Bundesrechts Personendaten sind, müssen diese grundsätzlich in Anwendung von Art. 11 DSG im Verzeichnis der Bearbeitungstätigkeiten verzeichnet sein. Da bei den meisten Geobasisdaten des Bundesrechts über die Geometrie des Grundstückes, die Grundstücksnummer und die öffentlichen Grundbuchdaten indirekt ein Bezug zur Grundeigentümerin bzw. zum Grundeigentümer hergestellt werden kann, müssten der Bund und alle Kantone je rund 50 der insgesamt rund 190 Geobasisdatensätze in die Verzeichnisse der Bearbeitungstätigkeiten aufnehmen. Dies macht aus Sicht des Datenschutzes wenig Sinn, zumal sämtliche

251 SR **510.62**
252 BBl **2006** 7817, 7852

Geobasisdaten des Bundesrechts bereits im Anhang zur Geoinformationsverordnung vom 21. Mai 2008[253] verzeichnet und die meisten Geobasisdaten Kraft spezialgesetzlicher Regelung öffentlich zugänglich sind. Deshalb soll der Bundesrat gemäss Absatz 2 die Geobasisdaten von der Aufnahme ins Verzeichnis der Bearbeitungstätigkeiten ausschliessen können, soweit diese nicht grundrechtlich heikle Positionen berühren.

Im neuen Absatz 3 wird festgehalten, dass der Bundesrat für Geobasisdaten des Bundesrechts verbindliche Zugangsberechtigungsstufen festlegen kann, die sämtliche Aspekte des Datenschutzes, besonderer Geheimhaltungspflichten und des Öffentlichkeitsprinzips berücksichtigen. Diese seit dem Inkrafttreten des Geoinformationsrechts im Jahre 2008 auf Verordnungsebene geltende Regelung hat sich bewährt und soll im Gesetz verankert werden. Diese Zugangsberechtigungsstufen betreffen den Zugang von Dritten und Behörden zu Geodaten. Ausnahmen zum Auskunftsrecht der betroffenen Person bezüglich ihrer eigenen Daten sind nur nach den Voraussetzungen von Artikel 24 E-DSG zulässig.

9.2.31 Bundesgesetz vom 3. Oktober 2008[254] über die militärischen Informationssysteme

Art. 1 Abs. 1 Einleitungssatz und 3

In Absatz 1 Einleitungssatz kann der Begriff «Persönlichkeitsprofile» durch «Personendaten» ersetzt werden. Denn der Katalog der Personendaten, die bearbeitet werden dürfen, wird in den Gesetzesbestimmungen definiert, die auf das betreffende Informationsystem anwendbar sind.

In Absatz 3 wird der Verweis auf den E-DSG angepasst.

Art. 10 Bst. c

Die Terminologie ist an jene von Artikel 4 Buchstabe c Ziffer 2 E-DSG anzupassen.

Art. 11 Abs. 2

Artikel 11 sieht für die Verknüpfungen bestimmter Daten eine eingeschränkte Datenbearbeitung vor. Der Begriff der «Persönlichkeitsprofile» wird auf andere Weise umschrieben als Personendaten, deren Verknüpfung die Beurteilung von wesentlichen Merkmalen einer Person erlaubt. Für solche verknüpfte Daten legt der Absatz 2 eine maximale Aufbewahrungsfrist fest.

253 SR **510.620**
254 SR **510.91**

9.2.32 Kriegsmaterialgesetz vom 13. Dezember 1996[255]

Art. 30 Abs. 2 zweiter Satz

Bei der Umsetzung des Kriegsmaterialgesetzes wirkt die Zentralstelle zur Bekämpfung der illegalen Herstellung von Kriegsmaterial bei der Deliktsverhütung mit und meldet Verstösse gegen Bestimmungen dieses Gesetzes den zuständigen Strafverfolgungsbehörden. Nach Artikel 30 Absatz 2 zweiter Satz des Kriegsmaterialgesetzes ist die Zentralstelle zu diesem Zweck befugt, Personendaten, mit Einschluss von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen, zu bearbeiten, soweit und solange es der Vollzug ihrer Aufgaben erfordert. Aufgrund der Art der Aufgaben der Zentralstelle muss der Begriff «Persönlichkeitsprofil» durch «Personendaten, welche die Beurteilung der Gefahr erlauben, dass eine Person Widerhandlungen gegen dieses Gesetz begeht» ersetzt werden.

9.2.33 Waffengesetz vom 20. Juni 1997[256]

Art. 32e Abs. 1 und 2

Siehe die Erläuterungen zu Artikel 111*d* Abs. 1 und 2 E-AuG (Ziff. 9.2.3).

Art. 32g zweiter Satz

Siehe die Erläuterungen zu Artikel 111*f* zweiter Satz E-AuG (Ziff. 9.2.3).

9.2.34 Bundesgesetz vom 4. Oktober 2002[257] über den Bevölkerungsschutz und den Zivilschutz

Art. 72 Abs. 1 zweiter Einleitungssatz und Bst. a und b sowie Abs. 1bis

Nach geltendem Recht ist die zuständige Bundesbehörde befugt, namentlich zur Abklärung des Kaderpotenzials von Schutzdienstpflichtigen und Kursteilnehmenden Persönlichkeitsprofile zu erstellen. In Absatz 1 muss der Begriff «Persönlichkeitsprofile» durch «Personendaten, die es erlauben, die Zuteilung der Grundfunktion oder die Abklärung des Kaderpotenzials zu beurteilen» ersetzt werden. In Absatz 1bis muss der Begriff «Persönlichkeitsprofil» ersetzt werden durch «Personendaten, die es erlauben, die Eignung für eine Kader- oder Spezialistenfunktion zu beurteilen».

255 SR **514.51**
256 SR **514.54**
257 SR **520.1**

9.2.35 Finanzhaushaltsgesetz vom 7. Oktober 2005[258]

Art. 60c Abs. 1 Einleitungssatz und Absatz 3

Der Begriff «Persönlichkeitsprofil» muss gestrichen werden. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.36 Finanzkontrollgesetz vom 28. Juni 1967[259]

Art. 10 Abs. 3

Diese Änderung betrifft nur den deutschen Text. Der Begriff «Datensammlung» muss im ersten Satz gestrichen und im letzten Satz durch «System» ersetzt werden.

9.2.37 Zollgesetz vom 18. März 2005[260]

Art. 38 Abs. 2

Die Veranlagungsverfügung nach Absatz 1 kann als automatisierte Einzelentscheidung nach Artikel 19 E-DSG erfolgen. Gemäss Artikel 19 Absatz 4 muss die Behörde diese Verfügung entsprechend kennzeichnen, sodass die betroffene Person erkennen kann, dass sie automatisiert erging.

Art. 103 Abs. 1 Einleitungssatz und Abs. 2

Das Festhalten der Identität kann auch durch die Abnahme genetischer Daten erfolgen. Dies war bislang in Artikel 226 Absatz 3 Buchstabe b Ziffer 1 der Zollverordnung vom 1. November 2006[261] festgehalten und wird nun in das Gesetz überführt.

Art. 110 Abs. 1 und 2

In Absatz 1 wird der Begriff «Persönlichkeitsprofil» gestrichen. Die Bearbeitungszwecke nach Absatz 2 des geltenden Rechts sind nun in Absatz 1 aufgeführt.

Im ersten Satz des neuen Absatz 2 ist nun lediglich festgehalten, dass die EZV zu diesem Zweck Informationssysteme führen darf.

Der zweite Satz in Absatz 2 ist neu. Darin wird die EZV für die Erfüllung der Aufgaben in Absatz 1 mit Ausnahme von Buchstabe d zum Profiling befugt. Die EZV bearbeitet und analysiert auf automatisierte Weise Personendaten, um Risikoprofile zu erstellen, die es erlauben, Kontrollen gezielter durchzuführen. Für diese Tätigkeit benötigt die EZV eine formell-gesetzliche Grundlage.

258 SR **611.0**
259 SR **614.0**
260 SR **631.0**
261 SR **631.01**

Art. 110a Abs. 3 Bst. b

Der Begriff «Persönlichkeitsprofil» muss gestrichen werden. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 112 Abs. 2 Einleitungssatz und 4 Bst. b sowie 6 zweiter Satz

Der Begriff «Persönlichkeitsprofil» muss im Einleitungssatz von Absatz 2 gestrichen werden. Siehe die Erläuterungen unter Ziffer 9.2.2.

In Absatz 2 ist zudem eine gesetzliche Grundlage für die Bekanntgabe von Personendaten vorzusehen, die auf einem Profiling beruhen (vgl. die Erläuterungen zu Art. 32 E-DSG in Ziff. 9.1.7).

Absatz 4 Buchstabe b kann aufgehoben werden, da er nicht mehr anwendbar ist.

In Absatz 6 zweiter Satz wird der Verweis auf den E-DSG angepasst.

Art. 113 und Art. 114 Abs. 2

Der Begriff «Persönlichkeitsprofil» muss gestrichen werden. Siehe die Erläuterungen unter Ziffer 9.2.2.

In beiden Bestimmungen ist zudem eine gesetzliche Grundlage für die Bekanntgabe von Personendaten vorzusehen, die auf einem Profiling beruhen (vgl. die Erläuterungen zu Art. 32 E-DSG in Ziff. 9.1.7).

9.2.38 Bundesgesetz vom 12. Juni 2009[262] über die Mehrwertsteuer

Art. 76 Abs. 1 zweiter Satz

Nach geltendem Recht unterhält die Eidgenössische Steuerverwaltung die Datensammlungen und die Mittel zur Bearbeitung und Aufbewahrung der erforderlichen Daten. Die Bestimmung ist überflüssig, sie kann aufgehoben werden.

9.2.39 Tabaksteuergesetz vom 21. März 1969[263]

Art. 18 Abs. 4

Die Festsetzung des Steuerbetrags kann als automatisierte Einzelentscheidung nach Artikel 19 E-DSG erfolgen. Gemäss Artikel 19 Absatz 4 muss die Behörde diese Verfügung entsprechend kennzeichnen, sodass die betroffene Person erkennen kann, dass sie automatisiert erging.

262 SR **641.20**
263 SR **641.31**

9.2.40 Biersteuergesetz vom 6. Oktober 2006[264]

Art. 17 Abs. 3 zweiter Satz

Vgl. die Erläuterungen zu Artikel 18 Absatz 4 E-Tabakgesetz (Ziff. 9.2.39).

9.2.41 Mineralölsteuergesetz vom 21. Juni 1996[265]

Art. 21 Abs. 2bis

Vgl. die Erläuterungen zu Artikel 18 Absatz 4 E-Tabakgesetz (Ziff. 9.2.39).

9.2.42 Schwerverkehrsabgabegesetz vom 19. Dezember 1997[266]

Art. 11 Abs. 4

Vgl. die Erläuterungen zu Artikel 18 Absatz 4 E-Tabakgesetz (Ziff. 9.2.39).

9.2.43 Kernenergiegesetz vom 21. März 2003[267]

Art. 24 Abs. 2

Nach geltendem Recht können im Rahmen der Prüfung der Zuverlässigkeit der Personen, die in Sicherheitsfunktionen eingesetzt werden, besonders schützenswerte Personendaten über die Gesundheit und die psychische Eignung sowie sicherheitsrelevante Daten über die Lebensführung der betroffenen Person bearbeitet werden. Der zweite Satz ist überflüssig und kann gestrichen werden.

9.2.44 Elektrizitätsgesetz vom 24. Juni 1902[268]

Art. 25a Abs. 2

Der Satzteil «Sie können die Daten elektronisch aufbewahren» kann gestrichen werden, denn er ist überflüssig.

264 SR **641.411**
265 SR **641.61**
266 SR **641.81**
267 SR **732.1**
268 SR **734.0**

9.2.45 Strassenverkehrsgesetz vom 19. Dezember 1958[269]

Art. 76b Abs. 3 zweiter Satz

Der Begriff «Persönlichkeitsprofil» muss gestrichen werden. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.46 Eisenbahngesetz vom 20. Dezember 1957[270]

Art. 16a Datenbearbeitung durch Konzessionsinhaberinnen

In Absatz 1 müssen die Verweise auf das künftige DSG angepasst werden. Die deutsche Fassung wird redaktionell an die französische und italienische Fassung angepasst.

Der Begriff «Persönlichkeitsprofil» muss in Absatz 2 gestrichen werden. Siehe die Erläuterungen unter Ziffer 9.2.2.

Gemäss Absatz 3 richtet sich die Aufsicht über die Bearbeitung von Personendaten durch die konzessionierten Eisenbahnunternehmen nach Artikel 27 DSG. Absatz 3 kann aufgehoben werden, da im E-DSG nicht mehr zwischen der Aufsicht des Beauftragten über Private und über Bundesorgane unterschieden wird.

9.2.47 Personenbeförderungsgesetz vom 20. März 2009[271]

Art. 54 Datenbearbeitung durch Konzessionsinhaberinnen

Siehe die Erläuterungen zu Artikel 16*a* des Eisenbahngesetzes (Ziff. 9.2.46).

9.2.48 Rohrleitungsgesetz vom 4. Oktober 1963[272]

Art. 47a Abs. 2

Siehe die Erläuterungen zu Artikel 25*a* Absatz 2 des Elektrizitätsgesetzes (Ziff. 9.2.44).

269 SR **741.01**
270 SR **742.101**
271 SR **745.1**
272 SR **746.1**

9.2.49 Luftfahrtgesetz vom 21. Dezember 1948[273]

Art. 107a Abs. 2 Einleitungssatz, 4 und 5

Im Einleitungssatz von Absatz 2 wird der Begriff «Persönlichkeitsprofil» gestrichen. Dies hat keinen Einfluss auf die Gesetzesgrundlage in Buchstabe a Ziffern 1–3.

Die Änderung in Absatz 4 betrifft lediglich den deutschen Text. Der Begriff der Datensammlung wird durch Datenbeschaffung ersetzt.

In Absatz 5 wird der Begriff «Persönlichkeitsprofile» gestrichen. Die Bekanntgabe von Personendaten an ausländische Behörden ist möglich, wenn die Voraussetzungen nach Artikel 13 E-DSG erfüllt sind.

Es wird auf die Änderung des Luftfahrtgesetzes vom 16. Juni 2017 hingewiesen.[274] Die Koordinationsbestimmungen (vgl. Ziff. 13.7) sehen gegebenenfalls die Aufhebung des Begriffs «Persönlichkeitsprofile» in Artikel 21*c* Absatz 1 Buchstabe b vor.

9.2.50 Postgesetz vom 17. Dezember 2010[275]

Art. 26 Abs. 1, Abs. 2 Einleitungssatz und 3 zweiter Satz und Art. 28

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.51 Fernmeldegesetz vom 30. April 1997[276]

Art. 13a Abs. 1 erster Satz und Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.52 Bundesgesetz vom 24. März 2006[277] über Radio und Fernsehen

Art. 69f Abs. 1 zweiter Satz und Art. 88 Abs. 2

Gemäss diesen Bestimmungen richtet sich die Aufsicht über die Bearbeitung von Personendaten durch die Erhebungsstelle und die Aufsichtsbehörde nach den für Bundesorgane geltenden Bestimmungen des DSG. Die Bestimmungen müssen

273 SR **748.0**
274 BBl **2017** 4257
275 SR **783.0**
276 SR **784.10**
277 SR **784.40**

geändert werden, da im E-DSG nicht mehr zwischen der Aufsicht des Beauftragten über Private und über Bundesorgane unterschieden wird.

9.2.53 Humanforschungsgesetz vom 30. September 2011[278]

Art. 42 Abs. 2

Anstatt auf Artikel 6 DSG muss auf die Artikel 13 und 14 E-DSG verwiesen werden.

9.2.54 Bundesgesetz vom 3. Oktober 1951[279] über die Betäubungsmittel und die psychotropen Stoffe

Art. 3f Abs. 1

Der Begriff «Persönlichkeitsprofile» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 18c zweiter Satz

Siehe die Erläuterungen zu Artikel 111*f* zweiter Satz E-AuG (Ziff. 9.2.3).

9.2.55 Epidemiengesetz vom 28. September 2012[280]

Art. 60 Abs. 9 erster Satz

In dieser Bestimmung sind die Verweise auf das E-DSG anzupassen.

Art. 62 Abs. 1 sowie 3 Einleitungssatz und Bst. a und d

Artikel 62 regelt die Bekanntgabe von Personendaten an ausländische Behörden. Die Änderungen entsprechen der neuen Regelung nach den Artikeln 13 und 14 E-DSG.

278 SR **810.30**
279 SR **812.121**
280 SR **818.101**

9.2.56 Bundesgesetz vom 17. Juni 2005[281] gegen die Schwarzarbeit

Art. 17 Sachüberschrift und Abs. 1 Einleitungssatz sowie Abs. 2 und 4

Aufgrund der Aufhebung des Schutzes der Daten von juristischen Personen müssen zwei verschiedene Gesetzesgrundlagen geschaffen werden (vgl. auch die Erläuterungen in Ziff. 9.1.11). Artikel 17 regelt fortan nur noch die Bearbeitung von Personendaten durch die zuständigen Kantonsbehörden. In Absatz 4 dieser Bestimmung wird der Verweis auf den E-DSG angepasst.

Art. 17a Bearbeitung von Daten juristischer Personen

Artikel 17*a* ermächtigt die zuständigen Kantonsbehörden zur Bearbeitung von Daten über juristische Personen.

9.2.57 Arbeitsvermittlungsgesetz vom 6. Oktober 1989[282]

Art. 33a Abs. 1 Einleitungssatz und Abs. 3 und Art. 35 Abs. 2, 3bis und 5 Bst. d

Wie aus der Botschaft des Bundesrates vom 24. November 1999 über die Anpassung und Harmonisierung der gesetzlichen Grundlagen für die Bearbeitung von Personendaten in den Sozialversicherungen[283] hervorgeht, müssen die Organe, die an der Umsetzung der verschiedenen Sozialversicherungsgesetze, zu denen im weiteren Sinn auch das Arbeitsvermittlungsgesetz (AVG) gehört, mitwirken, zwangsläufig ständig eine grosse Menge von Personendaten bearbeiten. Personendaten müssen bereits beim Eintritt in die Versicherungspflicht bearbeitet werden, dann wieder bei der Berechnung und bei der Erhebung der Beiträge oder Prämien und schliesslich auch für die Festlegung und die Auszahlung der Versicherungsleistungen. Die bearbeiteten Personendaten sind von unterschiedlichster Art. Es kann sich um Daten über die Identität einer Person, um besonders schützenswerte Daten zur Gesundheit oder um Angaben, die zur Privatsphäre gerechnet werden können wie beispielsweise das Alter, das Einkommen, die Berufslaufbahn, die Familiengeschichte, handeln. Je nachdem wie diese Daten zusammengetragen werden, können sie ein Bild von der Persönlichkeit eines Menschen vermitteln und somit ein Persönlichkeitsprofil im Sinn von Artikel 3 Buchstabe d DSG bilden.

Im Gesetzesentwurf wird der Begriff «Persönlichkeitsprofil» aufgehoben und somit die entsprechende gesetzliche Grundlage in Artikel 33*a* AVG. Der Bundesrat erachtet es indes als notwendig, eine formellgesetzliche Grundlage für Bearbeitungen zu schaffen, die – wie vorangehend beschrieben – ein Bild von der Persönlichkeit eines Menschen vermitteln können (Artikel 30 Absatz 2 Buchstabe c E-DSG). Im Bereich der Sozialversicherungen können solche Datenbearbeitungen einen schwerwiegenden Eingriff in die Grundrechte der betroffenen Person mit sich bringen. Der Bun-

281 SR **822.41**
282 SR **823.11**
283 BBl **2000** 255

desrat schlägt deshalb vor, Artikel 33*a* mit einem neuen Absatz 3 zu ergänzen, mit dem die zuständigen Organe ermächtigt werden, Personendaten, welche die Beurteilung der persönlichen und wirtschaftlichen Situation der Empfänger von Beratungsleistungen erlauben, im Sinn von Absatz 1 zu bearbeiten.

Art. 35b

Im französischen Text wird der Begriff «fichier» durch «registre» ersetzt. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.58 Bundesgesetz vom 20. Dezember 1946[284] über die Alters- und Hinterlassenenversicherung

Art. 49a Abs. 1 Einleitungssatz und 2

Im Gesetzesentwurf wird der Begriff «Persönlichkeitsprofil» aufgehoben und somit die entsprechende gesetzliche Grundlage in Artikel 49*a*. Wie beim Arbeitsvermittlungsgesetz (vgl. Ziff. 9.2.57) erachtet es der Bundesrat indes als notwendig, eine formell-gesetzliche Grundlage für Bearbeitungen zu schaffen, die ein Bild von der Persönlichkeit eines Menschen vermitteln können (Art. 30 Abs. 2 Bst. c E-DSG). Solche Datenbearbeitungen können einen schwerwiegenden Eingriff in die Grundrechte der betroffenen Person mit sich bringen, vor allem wenn es sich um besonders schützenswerte Gesundheitsdaten handelt. Der Bundesrat schlägt deshalb vor, Artikel 49*a* mit einem neuen Absatz 2 zu ergänzen, mit dem die zuständigen Organe ermächtigt werden, Personendaten, die namentlich die Beurteilung der Gesundheit, der Schwere des physischen oder psychischen Leidens, der Bedürfnisse und der wirtschaftlichen Situation der versicherten Person erlauben, zu bearbeiten, um die Aufgaben nach Absatz 1 zu erfüllen.

9.2.59 Bundesgesetz vom 25. Juni 1982[285] über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge

Art. 85a Abs. 1 Einleitungssatz und 2

Siehe die Erläuterungen zu Artikel 49*a* E-AHVG (Ziff. 9.2.58).

284 SR **837.0**
285 SR **831.40**

9.2.60 Bundesgesetz vom 18. März 1994[286] über die Krankenversicherung

Art. 84 Abs. 1 Einleitungssatz und 2

Siehe die Erläuterungen zu Artikel 49*a* E-AHVG (Ziff. 9.2.58).

Auch bezüglich des neuen Artikels 84 Absatz 2 des Bundesgesetzes über die Krankenversicherung kann im Wesentlichen auf die Ausführungen zu Artikel 49*a* Absatz 2 E-AHVG (vgl. Ziff. 9.2.58) verwiesen werden. Im Vergleich zu den anderen Sozialversicherungen wird diese Bestimmung innerhalb der sozialen Krankenversicherung hauptsächlich bei der Krankentaggeldversicherung Anwendung finden. Im Bereich der obligatorischen Krankenpflegeversicherung (OKP) und der damit verbundenen Aufgaben der Versicherer ist von einer eingeschränkten Anwendung im Rahmen der gesetzlichen Aufgaben auszugehen, etwa wenn zusätzliche Abklärungen in Einzelfällen, wie z. B. bei der Vergütung gewisser Medikamente (v.a. mit Limitatio), erforderlich sind. Festzuhalten ist, dass Bearbeitungen der in Absatz 2 genannten Datenkategorien für über die Durchführung der OKP und der Krankentaggeldversicherung hinausgehende Zwecke keinesfalls zulässig sind.

9.2.61 Bundesgesetz vom 20. März 1981[287] über die Unfallversicherung

Art. 96 Abs. 1 Einleitungssatz und 2

Im Einleitungssatz zu Absatz 1 wird lediglich der Begriff der Persönlichkeitsprofile gestrichen.

Neu eingefügt wird Absatz 2. Dieser sieht vor, dass die Organe nach Absatz 1 zur Erfüllung ihrer Aufgaben nach jenem Absatz zum Profiling befugt sind und automatisierte Einzelentscheidungen erlassen können.

Die obligatorische Unfallversicherung basiert – im Unterschied zur Krankenversicherung – auf dem Naturalleistungsprinzip. Der Versicherer hat die Pflegeleistungen in natura, auf seine Kosten, zu erbringen. Der Versicherer wird damit zum Schuldner gegenüber dem Leistungserbringer.[288] Gemäss dem Naturalleistungsprinzip gewährt der Versicherer dem Patienten eine umfassende, zweckmässige Behandlung und kommt nicht wie in der Krankenversicherung lediglich für die im Einzelfall eingereichten Kosten auf (Kostenvergütungsprinzip).

Das Naturalleistungsprinzip erlaubt dem Versicherer unter anderem, den Umfang, die Art und die Dauer der Leistungen mitzubestimmen. Dem Versicherer wird somit die Befugnis eingeräumt, die nötigen Anordnungen zur zweckmässigen Behandlung der Versicherten zu treffen (Art. 48 Abs. 1 UVG). Durch eine zweckmässige Behandlung des Versicherten können unter Umständen künftige Rentenleistungen

286 SR **832.10**
287 SR **832.20**
288 Maurer Alfred, Schweizerisches Unfallversicherungsrecht, 2. Aufl., Bern 1989, S. 523 ff.

verhindert werden. Damit die Versicherer die nötigen Anordnungen zur Bestimmung der umfassenden und zweckmässigen Behandlung treffen können, müssen sie jedoch die notwendigen medizinischen Daten bearbeiten können. So kann das Profiling dem Unfallversicherer beispielsweise erlauben, komplexe Fälle frühzeitig zu erkennen und gezielt einer spezialisierten Sachbearbeiterin oder einem spezialisierten Sachbearbeiter zuzuweisen.

Insgesamt gewährt die Anpassung in Absatz 2 den Unfallversicherern keine neuen Kompetenzen, sondern stellt lediglich sicher, dass sie ihre bisherigen weiterhin wahrnehmen können.

9.2.62 Bundesgesetz vom 19. Juni 1992[289] über die Militärversicherung

Art. 94a Abs. 1 Einleitungssatz und 2

Siehe die Erläuterungen zu Artikel 96 E-UVG (Ziff. 9.2.61).

9.2.63 Arbeitslosenversicherungsgesetz vom 25. Juni 1982[290]

Art. 96b Abs. 1 Einleitungssatz und 2 sowie Art. 96c Abs. 2 Einleitungssatz und 2bis

Siehe die Erläuterungen zu Artikel 49*a* E-AHVG (Ziff. 9.2.58).

9.2.64 Tierseuchengesetz vom 1. Juli 1966[291]

Art. 54a Abs. 3

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

9.2.65 Jagdgesetz vom 20. Juni 1986[292]

Art. 22 Abs. 3 erster und zweiter Satz

Der Begriff «elektronische Datensammlung» wird gestrichen, während der Begriff «elektronische Einträge» durch «Personendaten» ersetzt wird.

289 SR **833.1**
290 SR **837.0**
291 SR **916.40**
292 SR **922.0**

9.2.66 Nationalbankgesetz vom 3. Oktober 2003[293]

Art. 14 Abs. 3

Die Nationalbank erhebt zur Wahrnehmung ihrer gesetzlichen Aufgaben und zur Beobachtung auf den Finanzmärkten die erforderlichen statistischen Daten (Art. 14 Abs. 1 des Nationalbankgesetzes [NBG]). Um den Aufwand für die Meldepflichtigen zu begrenzen und Überschneidungen mit Datenerhebungen anderer Statistikstellen und Verwaltungseinheiten des Bundes nach Möglichkeit zu vermeiden, arbeitet sie bei der Erhebung statistischer Daten mit den zuständigen Stellen des Bundes, insbesondere dem Bundesamt für Statistik (BFS) und der FINMA, den zuständigen Behörden anderer Länder und mit internationalen Organisationen zusammen (Art. 14 Abs. 2 NBG).

In der Praxis hat sich nun gezeigt, dass die bestehende Regelung nicht in allen Fällen ausreichend ist. So verbieten in einigen Fällen gesetzliche Geheimhaltungspflichten und Sperrungen eine Weiterleitung von nicht aggregierten Daten an die Nationalbank. So verbietet Artikel 74 des Mehrwertsteuergesetzes vom 12. Juni 2009[294] eine Weiterleitung von Mehrwertsteuerdaten von der Eidgenössischen Steuerverwaltung (ESTV) an die Nationalbank. Zwar kann die ESTV diese Daten dem BFS in nicht anonymisierter Form zur Verfügung stellen (Art. 10 Abs. 4 und 5 des Bundesstatistikgesetzes vom 27. November 2009[295] [BStatG] i.V.m. Art. 136 Abs. 2 der Mehrwertsteuerverordnung vom 27. November 2009[296]). Eine Weiterleitung von der ESTV an die Nationalbank ist hingegen ausgeschlossen, weil das NBG keine analoge Bestimmung zu Artikel 10 Absatz 4 und 5 BStatG enthält. Im Ergebnis muss die Nationalbank Daten, welche bei der ESTV bereits vorhanden sind, bei den Unternehmen nochmals erheben. Dies führt zu einer Doppelbelastung der Unternehmen.

Artikel 14 soll deshalb um einen neuen Absatz 3 ergänzt werden. Analog der Regelung im BStatG wird festgelegt, dass die Eidgenössische Steuerverwaltung der Nationalbank zur Erfüllung ihrer statistischen Aufgaben die Grundlagen und Ergebnisse ihrer Statistiktätigkeit im Bereich der Mehrwertsteuer liefert und, falls erforderlich, Daten aus ihren Datenbeständen und Erhebungen zur Verfügung stellt. Mit dieser Regelung wird sichergestellt, dass die Nationalbank statistische Daten im Bereich der Mehrwertsteuer, die bei der Eidgenössischen Steuerverwaltung vorhanden sind, nicht noch einmal selber erheben muss. Dadurch werden die Unternehmen entlastet.

Um sicherzustellen, dass Dritte nicht über die Nationalbank an Daten gelangen, zu denen sie anderweitig keinen Zugang hätten, wird ausdrücklich festgehalten, dass die Nationalbank Daten, welche sie gestützt auf Absatz 3 von der Eidgenössischen Steuerverwaltung erhält, nicht an Dritte weitergeben darf. Diese Einschränkung gilt ungeachtet von Artikel 35 E-DSG auch für die Bekanntgabe der Daten an Dritte für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik. Ebenso wenig darf die Nationalbank diese Daten mit der FINMA im Rahmen von

293 SR **951.11**
294 SR **641.20**
295 SR **431.01**
296 SR **641.201**

Artikel 16 Absatz 4 NBG, mit dem BFS im Rahmen von Artikel 16 Absatz 4bis oder mit ausländischen Zentralbanken oder internationalen Organisationen und Gremien im Rahmen von Artikel 50*a* und 50*b* NBG austauschen. Eine Bekanntgabe der Daten in aggregierter Form ist hingegen gemäss Artikel 16 Absatz 3 NBG zulässig.

Art. 16 Abs. 4bis und Abs. 5

Artikel 16 regelt die Vertraulichkeit der Daten, die von der Nationalbank zu statistischen Zwecken bearbeitet werden.

Die Nationalbank hat über die von ihr erhobenen statistischen Daten das Geheimnis zu bewahren (Art. 16 Abs. 1 NBG), und zwar auch gegenüber denjenigen Behörden und internationalen Organisationen, mit denen sie eine Statistikzusammenarbeit pflegt. Entsprechend kann die Nationalbank nach geltendem Recht nur mit den zuständigen schweizerischen Finanzmarktaufsichtsbehörden vertrauliche Daten austauschen (Art. 16 Abs. 4 NBG). Allen anderen in- und ausländischen Behörden, insbesondere dem BFS, kann die Nationalbank die von ihr erhobenen Daten grundsätzlich nur in aggregierter Form weiterleiten (Art. 16 Abs. 3 i.V.m. Art. 14 Abs. 2 NBG). Einzige Ausnahme bilden neben der FINMA die Bank für Internationalen Zahlungsausgleich und gewisse internationale Organisationen und Gremien, welchen die Nationalbank seit Kurzem unter restriktiven Voraussetzungen nicht öffentlich zugängliche Informationen (einschliesslich der von ihr erhobenen Statistikdaten) übermitteln kann (Art. 50*a* und 50*b* NBG).

Für die Analyse der Entwicklungen auf den Finanzmärkten, den Überblick über den Zahlungsverkehr, die Erstellung der Zahlungsbilanz oder für die Statistik über das Auslandvermögen erhebt die Nationalbank bei juristischen und natürlichen Personen statistische Daten über deren Geschäftstätigkeit (Art. 15 Abs. 2 NBG). Gerade im Bereich der Zahlungsbilanz ergeben sich bei den Datenbedürfnissen der Nationalbank zahlreiche Überschneidungen mit den Datenbedürfnissen des BFS. Das Fehlen einer klaren gesetzlichen Grundlage für die Datenbekanntgabe von der Nationalbank ans BFS führt deshalb dazu, dass die Nationalbank und das BFS bei ihren Erhebungen einen wesentlich grösseren Aufwand betreiben müssen, um die Qualität ihrer Erhebungen zu gewährleisten. Synergien zwischen den einzelnen Datenerhebungen können nicht genutzt werden. Dies führt nicht nur bei der Nationalbank und dem BFS, sondern insbesondere auch bei den Auskunftspflichtigen, zu einer unnötigen Zusatzbelastung, welche sich durch den gegenseitigen Datenaustausch vermeiden liesse. Hinzu kommt, dass die Nationalbank genau wie das BFS und andere Statistikstellen verpflichtet ist, die Zahl und Art ihrer Erhebungen auf das notwendige Mass zu beschränken und die Belastung der Auskunftspflichtigen möglichst gering zu halten (Art. 4 Abs. 1 der Nationalbankverordnung vom 18. März 2004 [NBV][297]). Insbesondere hat die Nationalbank auf die Erhebung statistischer Daten zu verzichten, «wenn sie Daten vergleichbarer Qualität zeitgerecht auf anderem Weg beschaffen kann» (Art. 4 Abs. 3 NBV).

297 SR **951.131**

Aus diesem Grund soll die Nationalbank im neuen Absatz 4bis die Befugnis erhalten, dem BFS nicht aggregierte Daten bekannt zu geben. Da es sich um eine Ausnahme vom Grundsatz in Absatz 3 handelt, wonach die Nationalbank mit anderen in- und ausländischen Behörden und internationalen Organisationen nur aggregierte Daten austauschen darf, kommt die Regelung nur zur Anwendung, wenn die Datenbekanntgabe zu statistischen Zwecken erfolgt und das BFS zur Erfüllung seiner Aufgaben auf die betreffenden Daten angewiesen ist. Im neuen Absatz wird zudem klargestellt, dass das BFS die von der Nationalbank empfangenen Daten nicht an Dritte weitergeben darf. Dieses Verbot gilt ungeachtet der allgemeinen Regelung in Artikel 35 E-DSG auch für die Weitergabe für nicht personenbezogene Zwecke. Namentlich ist damit auch eine Weitergabe dieser Daten an andere in- oder ausländische Statistikstellen und Behörden ausgeschlossen. Mit dem Verbot der Weitergabe soll verhindert werden, dass Dritte über das BFS an Daten gelangen, zu denen sie sonst keinen Zugang hätten.

Anders als die Nationalbank ist das BFS gestützt auf Artikel 19 Absatz 2 BStatG bereits heute ermächtigt, der Nationalbank unter gewissen Voraussetzungen nicht aggregierte Personendaten zu statistischen Zwecken zur Verfügung zu stellen. Dieser Grundsatz gilt für die Daten des Betriebs- und Unternehmensregisters (BUR) aber nur beschränkt. So darf das BFS aufgrund von Artikel 10 Absatz 5 BStatG die im BUR enthaltenen Mehrwertsteuerdaten nicht an die Nationalbank weiterleiten. Mit dem neuen Artikel 14 Absatz 3 NBG wird daher die rechtliche Basis geschaffen, dass die ESTV der Nationalbank für statistische Zwecke Mehrwertsteuerdaten direkt zur Verfügung stellen kann.

Bei der Änderung von Artikel 16 Absatz 5 handelt es sich um eine Anpassung, welche sich aufgrund des geänderten Geltungsbereichs des E-DSG ergibt. Da der E-DSG inskünftig nur noch für die Daten von natürlichen Personen gilt, drängt sich aus Gründen der Rechtssicherheit eine entsprechende Präzisierung des Verweises auf den E-DSG auf.

Art. 49a Bearbeitung von Personendaten und von Daten juristischer Personen

Die Nationalbank bearbeitet in Erfüllung ihrer öffentlichen Aufgaben eine Vielzahl von Daten juristischer und teilweise natürlicher Personen. Diese Informationen über Finanzmarktteilnehmer und Unternehmen sind eine Grundvoraussetzung für die Ausübung ihrer gesetzlichen Aufgaben. In den Bereichen Statistik (Art. 14–16 NBG) und Finanzstabilität (Art. 16*a* NBG) verfügt die Nationalbank über eine explizite gesetzliche Grundlage für die Datenbearbeitung. Aus Gründen der Rechtssicherheit wird in Artikel 49*a* klargestellt, dass die Nationalbank zur Erfüllung all ihrer gesetzlichen Aufgaben Personendaten, einschliesslich besonders schützenswerter Personendaten, sowie Daten juristischer Personen bearbeiten kann.

9.2.67 Geldwäschereigesetz vom 10. Oktober 1997[298]

Art. 29 Abs. 2 zweiter Satz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Art. 33 Grundsatz

Der Verweis auf den E-DSG wird angepasst.

Art. 34 Sachüberschrift und Abs. 1–3

In der Sachüberschrift sowie in den Absätzen 1 und 2 wird der Begriff «Datensammlungen» durch «Datenbanken» bzw. «Datenbanken und Akten» ersetzt.

In Absatz 3 wird der Verweis auf den E-DSG angepasst.

9.2.68 Finanzmarktaufsichtsgesetz vom 22. Juni 2007[299]

Art. 23 Datenbearbeitung

Im Gesetzesentwurf wird der Begriff «Persönlichkeitsprofil» aufgehoben und somit die entsprechende Gesetzesgrundlage in Artikel 23. Die FINMA bearbeitet im Rahmen ihrer Aufsichtstätigkeit eine Vielzahl von Daten. Für die Ausübung der Finanzmarktaufsicht sind umfassende Informationen über die Beaufsichtigten und über Finanzmarktteilnehmer eine Grundvoraussetzung. Zu den bearbeitenden Daten gehören auch besonders schützenswerte Daten. Zudem kann der Bearbeitungszweck in Grundrechte, vorab die Wirtschaftsfreiheit, eingreifen. Aus diesem Grund schlägt der Bundesrat die Anpassung der formalgesetzlichen Grundlage für die Datenbearbeitung durch die FINMA vor, um der Anforderung nach Artikel 30 Absatz 2 E-DSG Rechnung zu tragen. Die Datenbearbeitung kann durch Auftragsdatenbearbeiter (d.h. FINMA-Beauftragte gemäss Artikel 14 Absatz 4 FINMAG sowie privatrechtlich eingesetzte Dienstleister) erfolgen (Abs. 1 und 2).

Die FINMA erhält von beaufsichtigten Instituten wie von weiteren Dritten naturgemäss eine sehr grosse Menge von Daten. Damit sie ein allfälliges aufsichtsrechtlich relevantes Fehlverhalten aus dieser Datenfülle eruieren kann, kommt sie nicht umhin, Personendaten im Rahmen eines Profilings zu bearbeiten. Insbesondere im Rahmen der sog. Marktaufsicht (z. B. zur Abklärung eines möglichen Insiderhandels oder einer Marktmanipulation) ist die FINMA mit einer sehr grossen Zahl von Handels-/Transaktionsdaten konfrontiert, die personenbezogen automatisiert ausgewertet und bewertet werden müssen. Um eine effiziente Aufsicht sicherzustellen, muss die FINMA entsprechende Daten daher im Rahmen eines Profilings bearbeiten können (Abs. 3).

Wie bisher regelt die FINMA die Einzelheiten in einer Verordnung (Abs. 4).

298 SR **955.0**
299 SR **956.1**

Art. 23a Öffentliches Verzeichnis

Die Bestimmung entspricht dem geltenden Artikel 23 Absatz 2.

9.2.69 Bundesgesetz vom 19. März 1976[300] über die internationale Entwicklungszusammenarbeit und humanitäre Hilfe

Art. 13a Abs. 1 Einleitungssatz und Bst. g

Der Einleitungssatz von Absatz 1 erfasst die Bearbeitung von Personendaten natürlicher und juristischer Personen. Da der Schutz von Personendaten juristischer Personen mit dem E-DSG aufgehoben wird, muss der Einleitungssatz angepasst werden (vgl. auch die Erläuterungen in Ziff. 9.1.11).

Der Begriff «Persönlichkeitsprofil» unter Buchstabe g wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Es wird darauf hingewiesen, dass diese Bestimmung im Vorentwurf des Bundesrates vom 28. Juni 2017 zum Bundesgesetz vom 24. März 2000 über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten aufgehoben wird (vgl. Ziff. 9.2.13).

9.2.70 Bundesgesetz vom 30. September 2016[301] über die Zusammenarbeit mit den Staaten Osteuropas

Art. 15 Abs. 2 Einleitungssatz

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Siehe die Erläuterungen unter Ziffer 9.2.2.

Es wird darauf hingewiesen, dass diese Bestimmung im Vorentwurf des Bundesrates vom 28. Juni 2017 zum Bundesgesetz vom 24. März 2000 über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten aufgehoben wird (vgl. Ziff. 9.2.13).

9.3 Erläuterungen zu den Änderungen der Bundesgesetze, die die Anforderungen der Richtlinie (EU) 2016/680 umsetzen

Wenn dieselbe Änderung in mehreren Erlassen erfolgt, ist sie nur einmal kommentiert und der Text enthält einen entsprechenden Verweis.

300 SR **974.0**
301 SR **974.1**

9.3.1 Strafgesetzbuch[302]

Zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680 umfasst die Vorlage einige Datenschutzbestimmungen zum Datenaustausch im Bereich der polizeilichen Zusammenarbeit. Die Bestimmungen gelten mit einigen Ausnahmen nicht nur für die Bundesbehörden, sondern auch für die Kantonsbehörden. Der Bund macht hierbei Gebrauch von seiner Gesetzgebungskompetenz, weil der Bereich der internationalen Zusammenarbeit in Strafsachen durch Bundesrecht geregelt wird. Wenn die Bundesverfassung dem Bund in einem bestimmten Bereich die Gesetzgebungskompetenz zuspricht, kann der Bundesgesetzgeber auch Datenschutzbestimmungen erlassen, die für kantonale Behörden gelten, die Bundesrecht anwenden müssen.

Art. 349a Rechtsgrundlagen

Mit dieser Bestimmung werden die Artikel 8 und 10 der Richtlinie (EU) 2016/680 umgesetzt. Gemäss diesen ist eine Datenbearbeitung im Anwendungsbereich dieses Rechtsakts im Wesentlichen nur dann rechtmässig, wenn dafür eine Rechtsgrundlage besteht. Fehlt eine Rechtsgrundlage, ist sie nur in bestimmten, in diesen beiden Bestimmungen genannten Fällen erlaubt. Fehlt eine Rechtsgrundlage, so dürfen die zuständigen Bundesbehörden Daten ausschliesslich in den Fällen nach Artikel 349*a* Buchstaben a und b bekannt geben. Die zuständigen Bundesbehörden dürfen sich für eine Bekanntgabe hingegen nicht auf Artikel 32 Absatz 2 Buchstaben a, b und e E-DSG stützen, da diese Bestimmungen nicht mit den Anforderungen der Artikel 8 und 10 der Richtlinie (EU) 2016/680 vereinbar sind.

Art. 349b Gleichbehandlung

Diese Bestimmung setzt Artikel 9 Absätze 3 und 4 der Richtlinie (EU) 2016/680 um, welche die Gleichbehandlung der Behörden der Schengen-Staaten und der nationalen Strafbehörden einführen. Artikel 349*b* entspricht der Lösung des Bundesgesetzgebers in Artikel 6 SIaG. Für die Bekanntgabe von Daten an Behörden eines Schengen-Staates gelten dieselben Datenschutzvorschriften wie für die Bekanntgabe an eine nationale Behörde. Die Verabschiedung neuer gesetzlicher Einschränkungen ist weiterhin möglich, sofern der Gleichbehandlungsgrundsatz eingehalten wird.

Art. 349c Bekanntgabe von Personendaten an einen Drittstaat oder an ein internationales Organ

Diese Bestimmung setzt die Artikel 35–38 der Richtlinie (EU) 2016/680 um, wonach die Schengen-Staaten dafür sorgen müssen, dass Personendaten einem Drittstaat oder einem internationalen Organ nur unter bestimmten kumulativ zu erfüllenden Voraussetzungen weitergeleitet werden dürfen.

Artikel 349*c* ist unter Vorbehalt bestimmter Anpassungen aufgrund der Anforderungen der Artikel 35–38 der Richtlinie (EU) 2016/680 an die Systematik und den Inhalt der Artikel 13 und 14 E-DSG angelehnt.

302 SR **311.0**

Abs. 1

Nach Absatz 1 dürfen der zuständigen Behörde eines Staates, der nicht über eines der Schengen-Assoziierungsabkommen mit der Schweiz verbunden ist (Drittstaat), oder einem internationalen Organ grundsätzlich Daten nicht bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein angemessenes Datenschutzniveau fehlt. Diese Bestimmung erfasst nur die Länder, die durch keines der Schengen-Assoziierungsabkommen gebunden sind.

Abs. 2

In Absatz 2 wird festgelegt, in welchen Fällen ein Drittstaat oder ein internationales Organ ein angemessenes Datenschutzniveau gewährleistet. Es handelt sich um eine abschliessende Liste alternativ zu erfüllender Voraussetzungen. Ist eine der Voraussetzungen erfüllt, steht der Bekanntgabe von Daten an einen Drittstaat oder ein internationales Organ datenschutzrechtlich nichts mehr entgegen.

Nach Absatz 2 Buchstabe a gewährleistet die Gesetzgebung eines Drittstaates ein angemessenes Datenschutzniveau, wenn die Europäische Union dies in einem Beschluss festgehalten hat. Das dafür zuständige Organ ist die Europäische Kommission. Der Angemessenheitsbeschluss wird nach Artikel 36 der Richtlinie (EU) 2016/680 gefasst. Absatz 2 Buchstabe a unterscheidet sich von Artikel 13 Absatz 1 E-DSG, wonach der Bundesrat prüfen soll, ob die Gesetzgebung im betreffenden Staat einen angemessenen Schutz gewährleistet. Beabsichtigt eine Behörde, einem Drittstaat für die polizeiliche und justizielle Schengen-Zusammenarbeit Daten bekannt zu geben, so muss sie sich an die Angemessenheitsbeschlüsse der Europäischen Kommission halten. In den übrigen Bereichen muss sich der Verantwortliche auf die Feststellungen des Bundesrates stützen. Diese unterschiedliche Regelung sorgt grundsätzlich nicht für Rechtsunsicherheit. Denn der Beauftragte veröffentlicht bereits heute eine Liste der Staaten mit einem angemessenen Datenschutzniveau. Diese entspricht im Wesentlichen den Angemessenheitsbeschlüssen der Europäischen Kommission.

Absatz 2 Buchstaben b und c umfasst zwei weitere Fälle, in denen die zuständige Behörde davon ausgehen kann, dass die Persönlichkeit der betroffenen Personen durch die Datenbekanntgabe nicht schwerwiegend gefährdet wird. So ist die Datenbekanntgabe rechtmässig, wenn das angemessene Datenschutzniveau durch einen völkerrechtlichen Vertrag (Bst. b) oder durch spezifische Garantien (Bst. c) gewährleistet ist. Absatz 2 Buchstabe b entspricht der Voraussetzung nach Artikel 13 Absatz 2 Buchstabe a E-DSG. Unter völkerrechtlichen Verträgen sind nicht nur völkerrechtliche Verträge mit einem Drittstaat oder einem internationalen Organ auf dem Gebiet der polizeilichen Zusammenarbeit zu verstehen, die den Anforderungen der Richtlinie (EU) 2016/680 genügen, sondern auch die völkerrechtlichen Datenschutzübereinkommen, die der empfangende Staat ratifiziert hat. Absatz 2 Buchstabe c entspricht der Voraussetzung nach Artikel 13 Absatz 2 Buchstabe c E-DSG. Die zuständige Behörde kann gestützt auf diese Bestimmung einem Drittstaat oder einem internationalen Organ Daten bekannt geben, wenn dieser spezifische Garantien bietet, die einen angemessenen Schutz der betroffenen Person gewährleisten.

Abs. 3

Handelt es sich bei der zuständigen Behörde um eine Bundesbehörde, so informiert sie nach Absatz 3 den Beauftragten über die Kategorien von Bekanntgaben von Personendaten, die nach Absatz 2 Buchstabe c erfolgen. Der Beauftragte muss nicht über jede Bekanntgabe informiert werden. Vielmehr soll ihm gemeldet werden, welche Kategorien von Bekanntgaben auf Grundlage dieser Bestimmung erfolgen. Nach Absatz 3 zweiter Satz wird jede Bekanntgabe dokumentiert. Anhand dieser Dokumentation ist der Beauftragte in der Lage, die erforderlichen Abklärungen vorzunehmen und allenfalls ein Verbot nach Artikel 45 Absatz 2 E-DSG zu erlassen.

Abs. 4 und 5

Falls ein angemessenes Datenschutzniveau im Sinne von Absatz 2 fehlt, enthält Absatz 4 eine abschliessende Liste von Ausnahmen. Trifft eine dieser Ausnahmen zu, ist es der zuständigen Behörde nicht mehr verboten, Drittstaaten oder internationalen Organen, die kein angemessenes Schutzniveau gewährleisten, Personendaten bekannt zu geben. Die Besitmmung erfüllt die Anforderungen nach Artikel 38 der Richtlinie (EU) 2016/680. Gemäss dem Erwägungsgrund 72 des europäischen Rechtsakts sollten diese Ausnahmen restriktiv ausgelegt werden, häufige, umfassende und strukturelle Übermittlungen personenbezogener Daten sowie Datenübermittlungen in grossem Umfang ausschliessen und auf unbedingt notwendige Daten beschränkt sein.

Nach Absatz 4 Buchstabe a dürfen Personendaten bekannt gegeben werden, wenn dies im Einzelfall zum Schutz des Lebens oder der körperlichen Unversehrtheit der betroffenen Person oder eines Dritten notwendig ist. Nach Buchstabe b ist die Bekanntgabe des Weiteren möglich, wenn sie im Einzelfall zur Abwehr einer unmittelbar drohenden ernsthaften Gefahr für die öffentliche Sicherheit eines Schengen-Staates oder eines Drittstaates notwendig ist.

Absatz 4 Buchstaben c und d umfasst zwei weitere Ausnahmen. Diese kommen jedoch nur zu Anwendung, sofern keine überwiegenden schutzwürdigen Interessen der betroffenen Person der Bekanntgabe entgegenstehen. Die Ausdrücke «Verhütung, Feststellung oder Verfolgung einer Straftat» entsprechen dem Anwendungsbereich der Richtlinie (EU) 2016/680, die den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten «zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung» regelt. Im Rahmen der Buchstaben c und d muss die Behörde durch eine Interessenabwägung feststellen, ob das gefährdete öffentliche Interesse oder das Interesse der betroffenen Person überwiegt. Kommt die Behörde zum Schluss, dass das schutzwürdige Interesse der betroffenen Person den Interessen der Strafverfolgung überwiegt, beispielsweise wenn die Bekanntgabe das Leben der betroffenen Person gefährden könnte, muss sie darauf verzichten, sich auf die Ausnahmen nach den Buchstaben c und d zu berufen. Handelt es sich bei der zuständigen Behörde um eine Bundesbehörde, muss sie den Beauftragten über die Bekanntgabe von Daten nach Absatz 4 informieren (Abs. 5).

Art. 349d Bekanntgabe von Personendaten aus einem Schengen-Staat an einen Drittstaat oder an ein internationales Organ

Mit dieser Bestimmung werden die Anforderungen von Artikel 35 Absatz 1 Buchstaben c und e sowie Absatz 2 der Richtlinie (EU) 2016/680 umgesetzt, wonach die Schengen-Staaten dafür sorgen müssen, dass die von einem Schengen-Staat erhaltenen Daten nur unter bestimmten, kumulativ zu erfüllenden Voraussetzungen an einen Drittstaat oder ein internationales Organ bekannt gegeben werden können. Diese Bestimmung gilt für die Schweizer Behörden, die von einem Schengen-Staat im Rahmen eines Verfahrens der polizeilichen Zusammenarbeit Daten erhalten haben und beabsichtigen, diese zur Unterstützung einem Drittstaat oder einem internationalen Organ bekannt zu geben. Unter Vorbehalt einiger Anpassungen entspricht Artikel 349*d* Artikel 6*b* SIaG, der aus systematischen Gründen aufgehoben wird.

Die entsprechende Bekanntgabe von Daten ist nur möglich, wenn die drei Voraussetzungen nach Absatz 1 kumulativ erfüllt sind. In Übereinstimmung mit den Grundsätzen der Zweckbindung und der Verhältnismässigkeit muss die Bekanntgabe für die Verhütung, Feststellung oder Verfolgung einer Straftat erforderlich sein und muss die empfangende Behörde dafür zuständig sein (Abs. 1 Einleitungssatz und Bst. a). Der Schengen-Staat, bei dem die Daten beschafft wurden, muss der Bekanntgabe zudem vorgängig zugestimmt haben (Bst. b). Schliesslich muss der Drittstaat oder das internationale Organ ein angemessenes Datenschutzniveau im Sinne von Artikel 349*c* gewährleisten (Bst. c).

Absatz 2 enthält eine Ausnahme von der Pflicht, vorgängig die Zustimmung des Schengen-Staates einzuholen, der die Daten beschafft hat. Nach den Buchstaben a und b dürfen Daten im Einzelfall bekannt gegeben werden, wenn die vorgängige Zustimmung des Schengen-Staates nicht rechtzeitig eingeholt werden kann und die Bekanntgabe zur Abwehr einer unmittelbar drohenden ernsthaften Gefahr für die öffentliche Sicherheit eines Schengen-Staates oder eines Drittstaates oder zur Wahrung der wesentlichen Interessen eines Schengen-Staates unerlässlich ist. Dabei handelt es sich um kumulativ zu erfüllende Voraussetzungen. Bei einer Bekanntgabe gestützt auf Absatz 2 informiert die zuständige Behörde den betroffenen Schengen-Staat unverzüglich (Abs. 3).

Art. 349e Bekanntgabe von Personendaten an in einem Drittstaat niedergelassene Empfänger

Mit dieser Bestimmung wird Artikel 39 der Richtlinie (EU) 2016/680 umgesetzt, wonach die Schengen-Staaten vorsehen können, dass die zuständigen Behörden Personendaten in besonderen Fällen direkt an in Drittstaaten niedergelassene Empfänger bekannt geben dürfen. Diese Norm bezieht sich auf Einzelfälle, in denen es dringend geboten ist, Daten ins Ausland zu übermitteln, um zum Beispiel das Leben einer Person, die Opfer einer Straftat zu werden droht, zu schützen oder um eine unmittelbar bevorstehende Begehung einer Straftat, einschliesslich einer terroristischen Straftat, zu verhindern.[303]

[303] Erwägungsgrund 73 der Richtlinie (EU) 2016/680.

Gemäss der Begriffsbestimmung nach Artikel 3 Absatz 10 der Richtlinie (EU) 2016/680 bezeichnet der Ausdruck «Empfänger» eine natürliche oder juristische Person, eine Behörde, eine Einrichtung oder eine andere Stelle, der personenbezogene Daten offengelegt werden.

Abs. 1

Nach Absatz 1 ist die Bekanntgabe von Personendaten an in einem Drittstaat niedergelassene Empfänger nur dann möglich, wenn drei Voraussetzungen kumulativ erfüllt sind. Die auf Artikel 349*e* gestützte Bekanntgabe von Daten muss eine Ausnahme bleiben.

Die erste Voraussetzung wird im Einleitungssatz von Absatz 1 genannt. Die zuständige Behörde muss zunächst feststellen, dass die Daten namentlich aufgrund eines Notfalls nicht auf dem üblichen Weg der polizeilichen Zusammenarbeit mit der zuständigen Behörde des betroffenen Drittstaates bekannt gegeben werden können.

Gemäss der zweiten Voraussetzung (Abs. 1 Bst. a) muss die Bekanntgabe für die Erfüllung einer gesetzlichen Aufgabe der zuständigen Behörde erforderlich sein, d. h. Aufgaben auf dem Gebiet der Verhütung, Feststellung oder Verfolgung einer Straftat. Die Bekanntgabe muss ausserdem unentbehrlich sein. Die zuständige Behörde darf somit nicht der Einfachheit halber auf Artikel 349*e* zurückgreifen. Die Bekanntgabe ist nur dann unentbehrlich, wenn sie eine unerlässliche Voraussetzung für die Erfüllung der gesetzlichen Aufgabe der Behörde darstellt.

Schliesslich dürfen der beabsichtigten Bekanntgabe keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen (Abs. 1 Bst. b). Die Behörde muss folglich eine Interessenabwägung vornehmen, um festzustellen, ob das gefährdete öffentliche Interesse oder das Interesse der betroffenen Person überwiegt.

Abs. 2

Nach Absatz 2 gibt die zuständige Behörde dem Empfänger die Personendaten mit dem ausdrücklichen Verbot bekannt, sie für andere Zwecke zu verwenden als für die von der Behörde festgelegten. Damit wird das Gebot der Zweckbindung konkretisiert.

Abs. 3

Gemäss Absatz 3 muss die zuständige Behörde die zuständige Behörde des Drittstaates unverzüglich über jede Bekanntgabe von Personendaten benachrichtigen, sofern diese Information als zweckmässig erachtet wird. Die Behörde kann von einer Benachrichtigung beispielsweise absehen, wenn sie Kenntnis davon hat, dass die zuständige Behörde des betroffenen Drittstaates für Menschenrechtsverletzungen verantwortlich ist (Erwägung 73 der Richtlinie [EU] 2016/680).

Abs. 4 und 5

Handelt es sich bei der zuständigen Behörde um eine Bundesbehörde, so informiert sie nach Absatz 4 auch den Beauftragten unverzüglich über jede Bekanntgabe von Daten nach Artikel 349*e*. Anders als im Fall von Artikel 349*c* Absatz 4 muss der

Beauftragte über jede Bekanntgabe informiert werden und nicht nur über die Kategorien der Bekanntgaben, die erfolgt sind. Die Bekanntgaben sind im Übrigen zu dokumentieren (Abs. 5). Anhand dieser Dokumentation ist der Beauftragte in der Lage, die erforderlichen Abklärungen vorzunehmen und allenfalls ein Verbot nach Artikel 45 Absatz 2 E-DSG zu erlassen.

Art. 349f Richtigkeit der Personendaten

Mit den Absätzen 1, 2 und 5 wird Artikel 7 Absätze 2 und 3 der Richtlinie (EU) 2016/680 umgesetzt. Dieser sieht im Wesentlichen vor, dass die zuständigen Behörden vor der Übermittlung der Daten deren Richtigkeit überprüfen und nach Möglichkeit die erforderlichen Informationen beifügen müssen, die es der empfangenden Behörde gestatten, die Richtigkeit der Daten zu beurteilen.

Absatz 1 ist an Artikel 98 Absatz 1 StPO angelehnt, wonach die zuständigen Strafbehörden unrichtige Personendaten berichtigen müssen.

Absatz 2 übernimmt Artikel 98 Absatz 2 StPO und präzisiert, dass im Fall der Berichtigung unvollständiger Personendaten die zuständige Behörde nicht nur die empfangende Behörde, der sie die unvollständigen Personendaten übermittelt hat, benachrichtigen muss, sondern auch die Behörde, von der sie die Daten erhalten hat.

Absatz 3 entspricht Artikel 12 VDSG.

Absatz 4 Buchstabe a dient der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680, wonach der Verantwortliche so weit wie möglich klar zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen unterscheiden muss. Mit dieser Bestimmung wird auf die Problematik eingegangen, dass betroffene Personen mit Fortschreiten des Verfahrens die Kategorie wechseln können. Gemäss der Erwägung 31 der Richtlinie geht es bei der Bearbeitung von Daten im Rahmen der justiziellen und polizeilichen Zusammenarbeit naturgemäss um betroffene Personen verschiedener Kategorien, die so weit wie möglich unterschieden werden sollten. Der Einleitungssatz von Absatz 4 lässt der zuständigen Behörde einen gewissen Handlungsspielraum. Möglicherweise kann diese Unterscheidung in bestimmten Fällen nicht getroffen werden, etwa wenn gestützt auf den Sachverhalt noch nicht bestimmt werden kann, ob eine Person Zeugin der Straftat ist oder ob sie als Täterin oder Gehilfin in die Tat involviert war.

Mit Absatz 4 Buchstabe b wird Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt, wonach so weit wie möglich zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten zu unterscheiden ist.[304]

Absatz 5 entbindet die Behörde von ihrer Pflicht zur Information des Datenempfängers, wenn die Informationen nach den Absätzen 2 und 3 aus den Personendaten selbst oder aus den Umständen ersichtlich sind. Diese Bestimmung ist an die Lösung in Artikel 12 VDSG angelehnt.

304 Erwägungsgrund 30 der Richtlinie (EU) 2016/680.

Art. 349g Prüfung der Rechtmässigkeit der Datenbearbeitung

Mit dieser Bestimmung wird Artikel 17 der Richtlinie (EU) 2016/680 umgesetzt, wonach die Schengen-Staaten der betroffenen Person das Recht gewähren müssen, die Aufsichtsbehörde im Bereich des Datenschutzes darum zu ersuchen, die Rechtmässigkeit der Bearbeitung der Daten über sie zu überprüfen, wenn die Informationspflicht eingeschränkt wird oder wenn ihr Recht auf Auskunft über ihre Daten, auf Einschränkung der Bearbeitung oder auf Berichtigung oder Löschung der Daten über sie beschränkt wird. Für die Regelung von Artikel 349*g* wurde die Lösung in Artikel 8 BPI übernommen und an die Neuerungen dieser Vorlage angepasst (siehe Ziff. 9.3.7).

Nach Absatz 1 kann die betroffene Person in den Fällen nach den Buchstaben a–c vom Beauftragten verlangen zu prüfen, ob allfällige Daten über sie rechtmässig bearbeitet werden. Aufgrund der Systematik des 4. Titels des 3. Buchs des StGB kann sich die betroffene Person nur für Datenbearbeitungen im Geltungsbereich des 4. Titels, d. h. die Amtshilfe im Bereich der Polizei oder in anderen Worten den Bereich der internationalen polizeilichen Zusammenarbeit, auf Artikel 349*g* berufen. Darüber hinaus kann eine Prüfung nur dann verlangt werden, wenn die verantwortliche Bundesbehörde der Aufsicht des Beauftragten untersteht (Abs. 2). Dies trifft zum Beispiel auf das fedpol oder die Bundeskriminalpolizei zu.

Der Beauftragte teilt der betroffenen Person entsprechend dem Wortlaut nach Absatz 3 die Ergebnisse in immer gleich lautender Form mit. Die Mitteilung kann nicht angefochten werden (Abs. 5).

Beschliesst der Beauftragte, eine Untersuchung gegen die Bundesbehörde zu eröffnen, so ist die betroffene Person nicht Verfahrenspartei (Art. 46 Abs. 2 E-DSG). Sie kann somit kein Rechtsmittel gegen allfällige Verwaltungsmassnahmen des Beauftragten (Art. 45 E-DSG) ergreifen.

Art. 349h Untersuchung

Mit dieser Bestimmung werden die Artikel 52 und 53 der Richtlinie (EU) 2016/680 umgesetzt, wonach die Schengen-Staaten für die betroffene Person das Recht auf Beschwerde bei einer Aufsichtsbehörde im Bereich des Datenschutzes sowie das Recht auf einen Rechtsbehelf gegen den allfälligen Entscheid dieser Behörde vorsehen müssen.

Nach Artikel 43 Absatz 1 E-DSG kann der Beauftragte von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Die betroffene Person kann Anzeige erstatten, sie hat im Verfahren jedoch keine Parteistellung (Art. 43 Abs. 4 e contrario sowie Art. 46 Abs. 2 E-DSG). Da die Schweiz die Anforderungen der Richtlinie (EU) 2016/680 übernehmen und umsetzen muss, ist eine Ausnahme von diesem Grundsatz einzuführen, die jedoch ausschliesslich die Datenbearbeitung durch eine Bundesbehörde im Rahmen eines Verfahrens der polizeilichen Zusammenarbeit betrifft. Demnach kann die betroffene Person gestützt auf Artikel 349*h* Absatz 1 vom Beauftragten die Eröffnung einer Untersuchung verlangen. Damit das entsprechende Gesuch zulässig ist, muss die betroffene Person glaubhaft machen, dass ein Austausch von Daten über sie gegen

die Datenschutzvorschriften verstösst, zum Beispiel in Bezug auf die Anforderungen an die Bekanntgabe von Daten an einen Drittstaat oder ein internationales Organ (Art. 349*c* E-StGB). Kann die betroffene Person keinen Verstoss glaubhaft machen, so ist der Beauftragte berechtigt, das Gesuch für unzulässig zu erklären. In Absatz 2 wird festgehalten, dass eine Untersuchung ausschliesslich gegen eine Bundesbehörde, die der Aufsicht des Beauftragten untersteht, eröffnet werden kann (siehe die Erläuterungen zu Art. 349*g* Abs. 2 E-StGB). Gegebenenfalls kann der Beauftragte gegenüber der Bundesbehörde vorsorgliche Massnahmen oder Verwaltungsmassnahmen anordnen (Art. 44 und 45 E-DSG). Der Entscheid und die Rechtsmittelbelehrung dazu müssen der Bundesbehörde sowie der betroffenen Person eröffnet werden.

Art. 355a Abs. 4

Absatz 4 ist neu. Darin wird präzisiert, dass der Austausch von Personendaten mit Europol dem Austausch mit einer zuständigen Behörde eines Schengen-Staates (Art. 349*b*) gleichgesetzt wird. Gemäss dem Erwägungsgrund 71 der Richtlinie (EU) 2016/680 stellen Kooperationsvereinbarungen zwischen Europol und Drittstaaten ein entscheidendes Kriterium zur Beurteilung des Datenschutzniveaus des betreffenden Staates dar. Es kann somit davon ausgegangen werden, dass die datenschutzrechtlichen Vorschriften von Europol aus Sicht des EU-Gesetzgebers ein angemessenes Datenschutzniveau gewährleisten.

Art. 355f und Art. 355g

Diese Bestimmungen wurden anlässlich der Übernahme des Rahmenbeschlusses 2008/977 /JI durch die Schweiz eingeführt.

Artikel 355*f* StGB regelt die Bekanntgabe von Daten aus einem Schengen-Staat an einen Drittstaat oder ein internationales Organ im Bereich der justiziellen Zusammenarbeit im Rahmen der Schengen-Assoziierungsabkommen. Er kann aufgehoben werden. Aus systematischen Gründen wird diese Kategorie von Bekanntgaben nun im E-IRSG geregelt.

Anders als der Rahmenbeschluss 2008/977/JAI regelt die Richtlinie (EU) 2016/680 die Bekanntgabe von Personendaten aus einem Schengen-Staat an eine Privatperson nicht mehr. Artikel 355*g* kann somit aufgehoben werden.

9.3.2 Strafprozessordnung[305]

Art. 95a Bearbeitung von Personendaten

Buchstabe a dient der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680, wonach der Verantwortliche so weit wie möglich klar zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen unterscheiden muss.

[305] SR **312.0**

Mit dieser Bestimmung wird auf die Problematik eingegangen, dass betroffene Personen mit Fortschreiten des Verfahrens die Kategorie wechseln können. Nach Artikel 6 der Richtlinie (EU) 2016/680 sind beispielsweise Verdächtigte und verurteilte Straftäter zu unterscheiden, Opfer einer Straftat und Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, oder Dritte wie Zeugen oder Personen, die Hinweise zur Straftat geben können. Für den Gesetzgeber der EU ist diese Vorschrift für das Bearbeiten von Personendaten im Rahmen der polizeilichen Zusammenarbeit und justiziellen Zusammenarbeit in Strafsachen besonders wichtig. Denn dabei werden naturgemäss Daten über verschiedene Kategorien betroffener Personen bearbeitet. Gemäss der Erwägung 31 der Richtlinie (EU) 2016/680 dient die Bestimmung der Anwendung des Rechts auf die Unschuldsvermutung (Art. 10 Abs. 1 StPO).

Nach Buchstabe a sorgen die zuständigen Strafbehörden bei der Bearbeitung von Personendaten dafür, dass sie die verschiedenen Kategorien betroffener Personen so weit wie möglich unterscheiden. Sie verfügen dabei über einen gewissen Handlungsspielraum. Denn möglicherweise kann diese Unterscheidung in bestimmten Fällen nicht getroffen werden, etwa wenn gestützt auf den Sachverhalt noch nicht bestimmt werden kann, ob eine Person Zeugin der Straftat ist oder ob sie als Täterin oder Gehilfin in die Tat involviert war.

Buchstabe b setzt die Anforderungen von Artikel 7 der Richtlinie (EU) 2016/680 betreffend die Unterscheidung zwischen personenbezogenen Daten und die Überprüfung der Qualität der Daten um. Nach Absatz 1 sehen die Schengen-Staaten vor, dass bei Personendaten so weit wie möglich zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten unterschieden wird. Aus der Systematik von Artikel 7 geht hervor, dass die Bestimmung den Grundsatz der Richtigkeit der Daten umsetzt und nicht zu eng ausgelegt werden darf. Im Erwägungsgrund 30 der Richtlinie (EU) 2016/680 wird dazu Folgendes festgehalten: «Aussagen, die personenbezogene Daten enthalten, basieren gerade in Gerichtsverfahren auf der subjektiven Wahrnehmung von natürlichen Personen und sind nicht immer nachprüfbar. Infolgedessen sollte sich der Grundsatz der sachlichen Richtigkeit nicht auf die Richtigkeit einer Aussage beziehen, sondern lediglich auf die Tatsache, dass eine bestimmte Aussage gemacht worden ist.» Es ist das Ziel aller Strafbehörden, die materielle Wahrheit zu ermitteln, damit die Strafgerichte Recht sprechen können. Artikel 95*a* E-StPO dient dem gleichen Zweck. Der Grundsatz der Richtigkeit gilt für alle Bearbeitungsarten, da die Verantwortlichen wie die betroffenen Personen ein erhebliches Interesse daran haben, dass nur aktuelle und zutreffende Daten bearbeitet werden. Ein Fall, in dem Artikel 95*a* Buchstabe b E-StPO zur Anwendung kommt, ist Artikel 143 StPO. Die Norm regelt die Durchführung der Einvernahme und schreibt in Absatz 5 vor, dass die Strafbehörde durch klar formulierte Fragen und Vorhalte die Vollständigkeit der Aussagen und die Klärung von Widersprüchen anstreben muss. Schliesslich geht der Bundesrat davon aus, dass Artikel 95*a* Buchstabe b keine Auswirkungen auf das Urteil eines Gerichts oder den Strafbefehl einer Staatsanwaltschaft hat. Denn wenn das Gericht oder die Staatsanwaltschaft beim Urteil oder beim Strafbefehl die Beweggründe des Täters, seine persönlichen Umstände, seine Persönlichkeit oder mildernde Umstände berücksichtigen, handelt es sich nicht um persönliche Einschätzungen, sondern um feste Bestandteile der Begründung ihres Entscheids, die nicht gesondert aufgeführt werden müssen.

Art. 98 Abs. 2

Artikel 98 regelt den Grundsatz der Richtigkeit der Daten.

In Bezug auf die Änderung von Absatz 2 siehe die Erläuterungen zu Artikel 349*f* Absatz 2 E-StGB (Ziff. 9.3.1).

9.3.3 Rechtshilfegesetz vom 20. März 1981[306]

Auf Rechtshilfeverfahren ist der E-DSG nicht anwendbar (Art. 2 Abs. 3 E-DSG). Mit dieser Vorlage wird im IRSG ein neues 1*b*. Kapitel zum Datenschutz eingefügt. Dadurch werden die Anforderungen der Richtlinie (EU) 2016/680 umgesetzt. Denn die Bearbeitung von Personendaten in Rechtshilfeverfahren fällt in den Anwendungsbereich des europäischen Rechtsakts.

Das 1*b*. Kapitel gilt nicht nur für die Bundesbehörden (z. B. das Bundesamt für Justiz oder die Bundesanwaltschaft), sondern auch für kantonale Behörden, die ein Rechtshilfeverfahren unterstützen oder über das ausländische Rechtshilfeersuchen entscheiden müssen (Art. 1 Abs. 1 IRSG). Der Bund nutzt hier seine Gesetzgebungskompetenz, da der Bereich der zwischenstaatlichen Zusammenarbeit in Strafsachen im Bundesrecht geregelt ist.

Die datenschutzrechtlichen Ansprüche werden im hängigen Rechtshilfeverfahren beurteilt und unterliegen denselben Rechtsmitteln.

Art. 11b Auskunftsrecht beim hängigen Verfahren

Mit dieser Bestimmung erhalten Personen, gegen die sich ein Ersuchen um zwischenstaatliche Zusammenarbeit in Strafsachen richtet, ein Recht auf Einsicht in die Personendaten. Damit werden die Anforderungen der Richtlinie (EU) 2016/680 umgesetzt (Art. 14 und 18).

Nach Absatz 1 müssen die betroffenen Personen nebst den sie betreffenden Personendaten sämtliche Informationen nach den Buchstaben a–e erhalten. Die betroffene Person muss über den Zweck und die Rechtsgrundlage der Bearbeitung (Bst. a) sowie die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (Bst. b) informiert werden. Sie muss ausserdem über die Empfänger oder die Kategorien von Empfängern informiert werden (Bst. c) sowie über die verfügbaren Angaben über die Herkunft der Personendaten (Bst. d). Ferner muss sie die Informationen erhalten, die erforderlich sind, damit sie ihre Rechte geltend machen kann (Bst. e). Die zuständige Behörde muss ihr beispielsweise mitteilen, dass ihre datenschutzrechtlichen Ansprüche im hängigen Rechtshilfeverfahren beurteilt werden und denselben Rechtsmitteln unterliegen.

Das Auskunftsrecht der betroffenen Person gilt nicht absolut. Nach Absatz 2 kann die zuständige Behörde die Auskunft verweigern, einschränken oder aufschieben, wenn Gründe nach Artikel 80*b* Absatz 2 IRSG vorliegen oder wenn eine der Voraussetzungen nach den Buchstaben a–c erfüllt ist. Die Verfügung der Behörde muss

306 SR **351.1**

so begründet werden, dass nicht Informationen offengelegt werden, aufgrund deren die Auskunft verweigert wird

Art. 11c Einschränkung des Auskunftsrechts bei Ersuchen um Festnahme zum Zweck der Auslieferung

Mit dieser Bestimmung wird eine Einschränkung des Auskunftsrechts eingeführt, das für Personendaten gilt, die bei Ersuchen um Festnahme zum Zwecke der Auslieferung bearbeitet werden. Bei dieser Regelung handelt es sich um ein sogenanntes «indirektes Auskunftsrecht». Sie ist an die Lösung nach Artikel 8 BPI angelehnt und wurde an die Neuerungen dieser Vorlage angepasst (vgl. Ziff. 9.3.7). Artikel 11*c* trägt zudem Artikel 17 der Richtlinie (EU) 2016/680 Rechnung, wonach die Schengen-Staaten für die betroffene Person das Recht vorsehen müssen, bei einer Einschränkung ihres Auskunftsrechts die Aufsichtsbehörde im Bereich Datenschutz darum zu ersuchen, die Rechtmässigkeit der Bearbeitung der Daten über sie zu überprüfen.

Abs. 1

In Absatz 1 wird die Behörde – das BJ – bestimmt, die dafür zuständig ist, einer Person zu antworten, die erfahren möchte, ob ein ausländischer Staat ein Ersuchen um Festnahme für ihre Auslieferung an die Schweiz gerichtet hat. Jede andere Bundes- oder Kantonsbehörde, an die ein solches Auskunftsbegehren gerichtet wird, ist für dessen Bearbeitung nicht zuständig und muss es umgehend dem BJ weiterleiten.

Abs. 2–6

Nach Absatz 2 erhält jede Person, die das BJ um Auskunft bittet, ob es ein Ersuchen eines ausländischen Staates um Festnahme für ihre Auslieferung erhalten hat, eine gleich lautende Antwort, wonach keine Daten über sie unrechtmässig bearbeitet werden und sie vom Beauftragten verlangen kann, zu prüfen, ob allfällige Daten über sie rechtmässig bearbeitet werden. Die betreffende Person kann so nicht erfahren, ob ein Ersuchen um Festnahme für ihre Auslieferung vorliegt. Die gegenwärtige Situation mit dem direkten Auskunftsrecht der betroffenen Person ist nämlich nicht befriedigend. Denn gestützt auf dieses Recht kann grundsätzlich jede Person in Erfahrung bringen, ob sie gesucht wird. Das Auskunftsrecht kann zwar verweigert werden, aber der Entscheid muss begründet werden. Doch schon allein die Tatsache, dass die Auskunft verweigert wird, kann der gesuchstellenden Person einen Hinweis darauf bieten, dass ein Ersuchen um Festnahme für ihre Auslieferung vorliegt. Mit der Einführung eines indirekten Auskunftsrechts im E-DSG soll verhindert werden, dass gesuchte Personen erfahren können, in welche Länder sie sich begeben können, ohne Gefahr zu laufen, für ihre Auslieferung festgenommen zu werden. Darüber hinaus ist die Regelung nach Artikel 11*c* von beschränkter Dauer. Denn, wenn die betroffene Person in der Schweiz festgenommen wird, kann sie sich im Auslieferungsverfahren auf sämtliche ihr nach dem IRSG zustehenden Rechte berufen.

Wie eben erläutert, kann die betroffene Person vom Beauftragten verlangen, dass er die Rechtmässigkeit der Datenbearbeitung prüft (Abs. 2). Diese Lösung ist ein guter Kompromiss zwischen dem Interesse der betroffenen Person am Schutz der Pri-

vatsphäre und dem öffentlichen Interesse daran, die Strafverfolgung eines ausländischen Staates nicht zu gefährden. Der Bescheid des Beauftragten muss immer gleich lauten. Er teilt der betroffenen Person mit, dass entweder keine Daten über sie unrechtmässig bearbeitet werden oder dass er im Falle von Fehlern bei der Bearbeitung der Personendaten eine Untersuchung nach Artikel 43 E-DSG eröffnet hat. Diese Bestimmung ist gleich auszulegen und anzuwenden wie andere indirekte Auskunftsrechte im Bundesrecht, namentlich in den Artikeln 8 BPI und 18 Absatz 4 BWIS.

Nach Absatz 3 führt der Beauftragte die verlangte Prüfung durch. Er beschränkt sich darauf, zu prüfen, ob die Bearbeitung in Bezug auf die datenschutzrechtlichen Anforderungen rechtmässig ist. Er prüft nicht, ob die Bearbeitung in Bezug auf die Voraussetzungen für die zwischenstaatliche Zusammenarbeit rechtmässig ist. Im Falle eines Fehlers bei der Datenbearbeitung kann der Beauftragte anordnen, dass das BJ diesen behebt. Dies könnte beispielsweise der Fall sein, wenn die Sicherheit der Bearbeitung nicht gewährleistet ist oder wenn unberechtigte Behörden oder Dritte Zugriff auf die Daten haben.

Die Absätze 3–6 stimmen mit den entsprechenden Vorschriften in Artikel 349*g* E-StGB überein (vgl. Ziff. 9.3.1).

Abs. 7

Absatz 7 schliesslich sieht vor, dass das BJ in Abweichung von Absatz 2 der betroffenen Person mit Einverständnis des ersuchenden Staates die Auskünfte geben kann, um die sie ersucht hat.

Art. 11d Anspruch auf Berichtigung und Löschung von Personendaten

Diese Bestimmung regelt die Ansprüche auf Berichtigung und Löschung von Personen, gegen die sich ein Ersuchen um zwischenstaatliche Zusammenarbeit in Strafsachen richtet. Damit werden die Anforderungen der Richtlinie (EU) 2016/680 umgesetzt (Art. 16 und 18).

Nach Absatz 1 kann die Person, gegen die sich ein Ersuchen um zwischenstaatliche Zusammenarbeit in Strafsachen richtet, von der zuständigen Behörde verlangen, dass ihre Personendaten, die unter Verstoss gegen das IRSG bearbeitet werden, berichtigt oder gelöscht werden, namentlich wenn die Personendaten unrichtig sind. Sie kann z. B. verlangen, dass die Personendaten zu ihrer Identität (Name, Vorname, Geschlecht, Geburtsdatum, Staatsangehörigkeit, Geburtsort) berichtigt und ergänzt werden. Der Grundsatz der Richtigkeit gilt für alle Arten von Bearbeitung, da die Behörden wie die betroffenen Personen ein erhebliches Interesse daran haben, dass nur aktuelle und zutreffende Daten bearbeitet werden. Den Nachweis der Unrichtigkeit der Personendaten muss die betroffene Person erbringen. Der Anspruch auf Berichtigung und Löschung gilt jedoch nicht für alle Personendaten. Es ist insbesondere nicht möglich, die Berichtigung oder Löschung des materiellen Inhalts von Personendaten zu verlangen, die zu Beweiszwecken beschafft worden sind, oder die Straftaten betreffen, die dem Ersuchen um zwischenstaatliche Zusammenarbeit in Strafsachen zugrunde liegen. Denn nach Absatz 4 ist für die Prüfung der Richtigkeit solcher Personendaten die entsprechende ausländische Behörde zuständig. Die Person, gegen die sich ein Ersuchen um zwischenstaatliche Zusammenarbeit in

Strafsachen richtet, kann die Richtigkeit folglich nicht bei der zuständigen Behörde des ersuchten Staates bestreiten, sondern muss dies gegebenenfalls bei der zuständigen Behörde des ersuchenden Staates bestreben.

Absatz 2 enthält eine Massnahme, die weniger radikal ist als die Löschung der Personendaten. Statt die Daten zu löschen, schränkt die zuständige Behörde deren Bearbeitung unter bestimmten Voraussetzungen ein. Das bedeutet, dass die Daten weiter bearbeitet werden dürfen, jedoch nur zu bestimmten Zwecken. Gemäss dem Erwägungsgrund 47 der Richtlinie (EU) 2016/680 ist die Einschränkung der Bearbeitung so zu verstehen, dass die Behörde die betreffenden Daten nur zu dem Zweck bearbeiten darf, der ihrer Löschung entgegenstand. Absatz 2 sieht dafür drei Konstellationen vor.

Nach Absatz 2 Buchstabe a muss die zuständige Behörde die Bearbeitung von Personendaten einschränken, wenn die betroffene Person die Richtigkeit der Personendaten bestreitet und weder deren Richtigkeit noch Unrichtigkeit festgestellt werden kann. In diesem Fall bedeutet die Einschränkung der Bearbeitung, dass die zuständige Behörde die bestrittenen Personendaten ausschliesslich zum Zweck bearbeiten darf, deren Richtigkeit oder Unrichtigkeit festzustellen. Die Behörde kann die Daten zum Beispiel zur Überprüfung der ausländischen Behörde bekannt geben, die sie ihr übermittelt hat. Sobald die Richtigkeit der Daten feststeht, darf die zuständige Behörde die Bearbeitung ohne Einschränkungen fortsetzen. Erweisen sich die Personendaten jedoch als unrichtig, so muss sie die zuständige Behörde löschen, sofern im betreffenden Fall nicht Buchstabe b oder c anwendbar ist.

Nach Absatz 2 Buchstabe b muss die zuständige Behörde die Bearbeitung einschränken, wenn überwiegende Interessen, namentlich die Interessen nach Artikel 80*b* Absatz 2 IRSG es erfordern. In diesem Fall muss die zuständige Behörde die Bearbeitung in dem Sinne einschränken, dass sie weiterhin Personendaten bearbeiten darf, jedoch ausschliesslich zu dem Zweck, der ihrer Löschung entgegenstand. Sie darf die Personendaten der ausländischen Behörde folglich bekannt geben, um überwiegende Interessen zu wahren.

Nach Absatz 2 Buchstabe c muss die zuständige Behörde die Personendaten nicht löschen, wenn deren Löschung ein Verfahren der zwischenstaatlichen Zusammenarbeit in Strafsachen oder das Verfahren im Ausland, auf das sich das Ersuchen um Zusammenarbeit in Strafsachen stützt, gefährden kann. In diesem Fall dürfen Personendaten einer ausländischen Behörde bekannt gegeben werden, da deren Löschung die korrekte Durchführung der Verfahren behindern würde.

Gemäss Absatz 3 benachrichtigt die zuständige Behörde die Behörde, die ihr die Personendaten übermittelt oder zur Verfügung gestellt hat oder der sie diese bekannt gegeben hat, unverzüglich über die nach Absatz 1 oder 2 getroffenen Massnahmen.

Absatz 4 schreibt vor, dass für die Prüfung der Richtigkeit von Personendaten, die zu Beweiszwecken beschafft worden sind, oder von Personendaten betreffend Straftaten, die dem Ersuchen um zwischenstaatliche Zusammenarbeit in Strafsachen zugrunde liegen, die entsprechende ausländische Behörde zuständig ist. Ziel der internationalen Rechtshilfe in Strafsachen ist es, dass ein Staat Massnahmen vollzieht, die die Verfolgung und Ahndung von Straftaten in einem anderen Staat erleichtern. Dabei laufen zwei Verfahren: das ausländische Strafverfahren und das

Rechtshilfeverfahren bei der zuständigen Behörde. Letzteres Verfahren dient ersterem. Die Richtigkeit von Personendaten, die zu Beweiszwecken beschafft worden sind (z. B. Bankauszüge, Aufnahmen oder Protokolle der Zeugeneinvernahmen), oder von Personendaten betreffend Straftaten, die dem Ersuchen um zwischenstaatliche Zusammenarbeit in Strafsachen zugrunde liegen (z. B. die Fakten, die Qualifizierung der Straftaten, die Stellung der betroffenen Person im Strafverfahren) könnte von der zuständigen Behörde des im Rahmen eines Rechtshilfeverfahrens ersuchten Staates nicht geprüft werden. Denn das ausländische Strafverfahren dient gerade dem Zweck, die Richtigkeit oder Unrichtigkeit der Personendaten festzustellen. Gemäss dem Untersuchungsgrundsatz muss die zuständige Behörde von Amtes wegen alle Tatsachen abklären, die für die Beurteilung der Tat und der beschuldigten Person bedeutsam sind und dabei die belastenden und entlastenden Umstände untersuchen. In diesem Zusammenhang muss die Richtigkeit der Personendaten, die zu Beweiszwecken beschafft worden sind, oder von Personendaten betreffend Straftaten, die Gegenstand des Strafverfahrens sind, geprüft werden.

Art. 11e Gleichbehandlung

Diese Bestimmung regelt die Gleichbehandlung der Behörden der Schengen-Staaten und der nationalen Behörden in Bezug auf die Datenschutzregelung. Sie setzt Artikel 9 Absätze 3 und 4 der Richtlinie (EU) 2016/680 um.

Artikel 9 Absätze 3 und 4 der Richtlinie (EU) 2016/680 ist in Verbindung mit Artikel 60 der Richtlinie (EU) 2016/680 auszulegen, nach welchem die besonderen Bestimmungen in Rechtsakten der Europäischen Union, die vor dem Erlass der Richtlinie (EU) 2016/680 erlassen worden sind und die Behandlung der Mitgliedstaaten untereinander regeln, unberührt bleiben (siehe ebenfalls die Erwägung 94). Nach dieser Auslegung bleibt folglich die Gemeinsame Erklärung der Schweiz und der Europäischen Union zu Artikel 23 Absatz 7 des Übereinkommens vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union[307] vorbehalten.

Der Grundsatz der Spezialität nach Artikel 67 IRSG bleibt durch Artikel 11*e* gewahrt. Nach Artikel 67 Absatz 1 IRSG dürfen die durch Rechtshilfe erhaltenen Auskünfte und Schriftstücke im ersuchenden Staat in Verfahren wegen Taten, bei denen Rechtshilfe nicht zulässig ist, weder für Ermittlungen benützt noch als Beweismittel verwendet werden.

Siehe des Weiteren die Erläuterungen zu Artikel 349*b* E-StGB (Ziff. 9.3.1).

307 Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands vom 26. Oktober 2004 (SR **0.362.31**).

Art. 11f Bekanntgabe von Personendaten an einen Drittstaat oder an ein internationales Organ

Diese Bestimmung regelt die Bekanntgabe von Daten an einen Drittstaat oder ein internationales Organ. Der Wortlaut dieses Artikels entspricht im Wesentlichen Artikel 349*c* E-StGB. Abweichend von Artikel 349*c* Absatz 3 E-StGB ist in Artikel 11*f* jedoch nicht vorgesehen, dass die Bundesbehörden den Beauftragten über die Kategorien von Bekanntgaben von Personendaten informieren müssen, die nach Artikel 11*f* Absatz 2 Buchstabe c erfolgt sind, oder dass sie ihn über die auf Absatz 3 gestützte Bekanntgabe von Personendaten informieren müssen. Dieser Unterschied ist dadurch gerechtfertigt, dass der Beauftragte nicht für die Aufsicht über die Datenbearbeitung im Rahmen eines zwischenstaatlichen Rechtshilfeverfahrens in Strafsachen zuständig ist (siehe die Erläuterungen zu Art. 3 Abs. 2 Bst. e E-DSG). Des Weiteren wird sinngemäss auf die Erläuterungen zu Artikel 349*c* E-StGB verwiesen (vgl. Ziff. 9.3.1).

Art. 11g Bekanntgabe von Personendaten aus einem Schengen-Staat an einen Drittstaat oder ein internationales Organ

Diese Bestimmung regelt die Bekanntgabe von Daten aus einem Schengen-Staat an einen Drittstaat oder ein internationales Organ. Der Wortlaut dieses Artikels entspricht im Wesentlichen jenem von Artikel 349*d* E-StGB. Abweichend von Artikel 349*d* Absatz 1 Buchstabe a E-StGB erfasst Artikel 11*g* Absatz 1 Buchstabe a auch den Fall, dass die von einem Schengen-Staat erhaltenen Daten einem Drittstaat zur Vollstreckung eines Strafentscheids bekannt gegeben werden. Diese Konstellation ist in der Rechtshilfe gegeben. Siehe des Weiteren sinngemäss die Erläuterungen zu Artikel 349*d* E-StGB (unter Ziff. 9.3.1).

Art. 11h Vorgehen bei der Bekanntgabe von Personendaten

In dieser Bestimmung wird das Vorgehen bei der Bekanntgabe von Personendaten geregelt. Die Bestimmung entspricht Artikel 349*f* Absätze 3–5 E-StGB (siehe die Erläuterungen unter Ziff. 9.3.1).

9.3.4 Bundesgesetz vom 22. Juni 2001[308] über die Zusammenarbeit mit dem Internationalen Strafgerichtshof

Art. 2a Schutz von Personendaten

Zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680 muss im Bundesgesetz vom 22. Juni 2001 über die Zusammenarbeit mit dem Internationalen Strafgerichtshof ein Verweis auf die Artikel 11*b*–11*d* und 11*f*–11*h* E-IRSG eingefügt werden. Artikel 11*e* wird von diesem Verweis ausgenommen, da er die Gleichbe-

308 SR **351.6**

handlung zwischen den Behörden der Schengen-Staaten regelt. Auf den Internationalen Strafgerichtshof ist er folglich nicht anwendbar.

9.3.5 Bundesgesetz vom 3. Oktober 1975[309] zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen

Art. 9a Schutz von Personendaten

Zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680 muss im Bundesgesetz vom 3. Oktober 1975 zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen ein Verweis auf die Artikel 11*b*, 11*d* und 11*f*–11*h* E-IRSG eingefügt werden.

9.3.6 Bundesgesetz vom 7. Oktober 1994[310] über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten

Art. 13 Abs. 2

Zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680 ist es nötig, Artikel 13 Absatz 2 durch eine Verweisung auf Artikel 349*a* bis 349*h* E-StPO anzupassen.

9.3.7 Bundesgesetz vom 13. Juni 2008[311] über die polizeilichen Informationssysteme des Bundes

Art. 7 Abs. 2

In Absatz 2 wird zusätzlich der neue Artikel 8*a* E-BPI vorbehalten.

Art. 8 Einschränkung des Auskunftsrechts beim System Bundesdelikte

Dieser Artikel muss angepasst werden, da der Beauftragte gemäss dem neuen DSG keine Empfehlungen mehr erlässt, sondern eine Untersuchung im Sinne von Artikel 43 E-DSG eröffnen und gegebenenfalls Massnahmen nach den Artikeln 44 und 45 E-DSG anordnen kann.

Absatz 1 bleibt im Vergleich zum geltenden Recht unverändert.

Absatz 2 wird redaktionell angepasst.

309 SR **351.93**
310 SR **360**
311 SR **361**

Absatz 3 wird in dem Sinne geändert, dass der Beauftragte der betroffenen Person nicht mehr mitteilen muss, «dass er […] eine Empfehlung im Sinne von Artikel 27 DSG […] zu deren Behebung an fedpol gerichtet hat», sondern «dass er […] eine Untersuchung nach Artikel 43 DSG eröffnet hat». Da dem Beauftragten in den Artikeln 44 und 45 E-DSG Verfügungskompetenzen verliehen werden, ist es ausserdem nicht mehr erforderlich, dass das Bundesverwaltungsgericht wie gemäss Absatz 3 zweiter Satz des geltenden Gesetzes eingreift; die entsprechende Stelle kann gestrichen werden.

Der geltende Absatz 4 kann aufgehoben werden. Der Verweis auf Artikel 43 E-DSG genügt. Gemäss dem neuen Absatz 4 kann der Beauftragte auf Grundlage der Untersuchung eine Verfügung erlassen (Art. 45 E-DSG), die das fedpol anfechten kann.

Absatz 5 sieht vor, dass die Mitteilungen nach den Absätzen 2 und 3 stets gleich lauten und nicht begründet werden sowie dass die Mitteilung nach Absatz 3 nicht angefochten werden kann.

Absatz 6 entspricht dem geltenden Absatz 7 und bleibt unverändert.

Absatz 7 entspricht Absatz 8, wird aber dahingehend angepasst, dass der Beauftragte nicht mehr nur empfehlen, sondern auch anordnen kann, dass das fedpol der betroffenen Person die verlangten Auskünfte erteilt, wenn die Voraussetzungen dafür erfüllt sind.

Art. 8a Einschränkung des Auskunftsrechts bei Ausschreibungen zur Festnahme zum Zweck der Auslieferung

Mit dieser Bestimmung wird eine Einschränkung des Auskunftsrechts bei Ausschreibungen zur Festnahme zum Zweck der Auslieferung in einem der Systeme nach Artikel 2 BPI eingeführt. Betrifft das Gesuch der betroffenen Person keines dieser Systeme, ist das fedpol gemäss der Bestimmung in Artikel 11*c* Absatz 1 E-IRSG gehalten, es an das BJ weiterzuleiten.

Siehe im Übrigen die Erläuterungen zu Artikel 11*c* E-IRSG (Ziff. 9.3.3).

9.3.8 Schengen-Informationsaustausch-Gesetz vom 12. Juni 2009[312]

Art. 2 Abs. 3

Der Verweis auf die Artikel 6*a*–6*c* SIaG wird durch einen Verweis auf die Artikel 349*a*–349*h* E-StGB ersetzt.

312 SR **362.2**

Art. 6a–6c

Die Artikel 6*a*–6*c* SIaG wurden zur Umsetzung des Rahmenbeschlusses 2008/977/JAI in das Gesetz eingefügt. Um die Normdichte der eidgenössischen Gesetzgebung zu reduzieren, schlägt der Bundesrat vor, diese Bestimmungen aufzuheben und eine Verweisung auf die Artikel 349*a*–349*h* E-StGB einzufügen.

10 Inkrafttreten

Es ist vorgesehen, dass der Bundesrat über das Inkrafttreten des künftigen Gesetzes bestimmt.

Wie unter Ziffer 2.2 erwähnt muss die Schweiz die Richtlinie (EU) 2016/680 innert zwei Jahren ab dem Zeitpunkt der Notifikation durch die Europäische Union in ihre Rechtsordnung umsetzen. Die Richtlinie (EU) 2016/680 wurde der Schweiz am 1. August 2016 notifiziert. Die Frist für die Übernahme des Rechtsaktes und dessen Umsetzung dauert daher bis zum 1. August 2018. Es wäre zwar möglich, dass der Gesetzesentwurf für den öffentlichen und den privaten Sektor zu einem unterschiedlichen Zeitpunkt in Kraft tritt, d. h. zunächst für die Bundesorgane und zu einem späteren Zeitpunkt für die Privatpersonen. Dem Bundesrat erscheint diese Lösung jedoch nicht angemessen. Denn die Verordnung (EU) 2016/679 gilt ab dem 25. Mai 2018 für die Mitgliedstaaten der Europäischen Union (Art. 99). Es liegt im Interesse der Schweiz, dass der Gesetzesentwurf unter Vorbehalt bestimmter Übergangsbestimmungen so rasch als möglich in Kraft tritt. Auf diese Weise kann auch die Frist von zwei Jahren, die gemäss den Schengen-Verpflichtungen für die Umsetzung der Richtlinie (EU) 2016/680 besteht, grundsätzlich weitgehend eingehalten werden.

11 Auswirkungen

Die Auswirkungen der Vorlage und jene der Übernahme der Richtlinie sind untrennbar miteinander verbunden und werden daher nicht getrennt dargestellt.

11.1 Finanzielle und personelle Auswirkungen auf den Bund

11.1.1 Finanzielle und personelle Auswirkungen auf den Beauftragen

Durch den Gesetzesentwurf wird eine Reihe von Massnahmen eingeführt, die zu neuen Aufgaben für den Beauftragten führen. Die Massnahmen entsprechen zum Teil den Anforderungen des europäischen Rechts (d. h. des E-SEV 108, der Richtlinie [EU] 2016/680 und der Verordnung [EU] 2016/679) und sind erforderlich, damit die Schweiz weiterhin ein angemessenes Datenschutzniveau nach Massgabe der Standards der Europäischen Union gewährleisten und ihren Pflichten aufgrund der Schengen-Abkommen nachkommen kann. Einige Massnahmen entsprechen einem

Bedürfnis der Wirtschaft und sollen den Unternehmen die Umsetzung des Gesetzes erleichtern. Da aufgrund des weit gefassten Anwendungsbereichs der Verordnung (EU) 2016/679 (Art. 3) voraussichtlich zahlreiche Schweizer Unternehmen diesem Erlass unterliegen werden, ist es wichtig, dass die Vorlage nicht zu stark davon abweicht. Denn abgesehen von der Frage des Angemessenheitsbeschlusses müssen die Unternehmen aus Gründen der Wirtschaftlichkeit und Rechtssicherheit ein Geschäftsgebaren und interne Vorschriften entwickeln, die unabhängig von der Unterstellung unter europäisches oder schweizerisches Recht ziemlich identisch sind.

Aufgrund der neuen Aufgaben des Beauftragten benötigt dieser zusätzliche Personal- und Informatikressourcen. Diesbezüglich ist zu betonen, dass die Ausstattung des Beauftragten mit ausreichenden Ressourcen für die Europäische Union sowohl in Bezug auf den Angemessenheitsbeschluss als auch auf die Umsetzung des Schengen-Besitzstands ein wichtiges Element ist. So ist denn die Pflicht, die Aufsichtsbehörden mit ausreichenden Mitteln auszustatten – für deren Unabhängigkeit zentral –, in allen europäischen Erlassen verankert (Art. 12bis Abs. 5 E-SEV 108, 42 Abs. 4 der Richtlinie [EU] 2016/680 und 52 Abs. 4 der Verordnung [EU] 2016/679). Bei der Beurteilung des angemessenen Datenschutzniveaus wird auch die effektive Umsetzung der Massnahmen evaluiert. Die nächste Schengen-Evaluation, die 2018 stattfindet, wird diesen Aspekt ebenfalls beinhalten. Die Gruppe der Aufsichtsbehörden für SIS II hat sich jüngst an die Europäische Kommission, das Europäische Parlament und den Rat der Europäischen Union gewandt mit der Aufforderung, sicherzustellen, dass die Aufsichtsbehörden tatsächlich die für ihre gesetzlichen Aufgaben angemessenen personellen und finanziellen Mittel erhalten.

11.1.1.1 Personalbedarf

Der zusätzliche Personalbedarf des Beauftragten ist weder statisch noch linear und wird sich mit der Zeit entwickeln. So werden ihm zu Beginn voraussichtlich wenige Verhaltenskodizes vorgelegt werden, da die Branchen für deren Erarbeitung Zeit benötigen werden. Zudem hängen viele Massnahmen miteinander zusammen, sodass der Beauftragte aufgrund der Aufgaben in Verbindung mit einer Massnahme in einem anderen Bereich weniger oder nicht mehr tätig werden muss. In Bezug auf die Verhaltenskodizes beispielsweise wird die Einholung der Stellungnahme des Beauftragten voraussichtlich dazu beitragen, dass weniger Untersuchungen eröffnet werden müssen, da dadurch ein gesetzeskonformes Verhalten gefördert wird. Schliesslich werden die präventiven Kontrollaufgaben des Beauftragten zu einer erhöhten Beachtung der Gesetzgebung beitragen und dadurch weniger Untersuchungen zur Folge haben. Um den tatsächlichen Bedarf des Beauftragten so genau wie möglich zu bestimmen, schlägt der Bundesrat deshalb einerseits vor, schrittweise Personalressourcen zu gewähren (siehe Tabelle unten) und andererseits den Bedarf nach spätestens fünf Jahren nach Inkrafttreten des Gesetzes wieder zu evaluieren.

Es ist schwierig, präzise Schätzungen zu treffen. Deshalb war der Bundesrat bestrebt, bei jeder neuen Aufgabe mit einem zusätzlichen Personalbedarf aufzuzeigen, welche Hypothesen seiner Einschätzung zugrunde liegen. Dieses Vorgehen ist auch

im Hinblick auf die Evaluation des Bedarfs im Fünfjahresrhythmus von Bedeutung. Denn eventuell sinkt der Bedarf in einigen Bereichen mit der Zeit. Soweit möglich und gemäss dem Kostendeckungsprinzip werden die neuen Stellen durch Gebühren finanziert (Art. 53 E-DSG).

Der Personalbedarf des Beauftragten beläuft sich auf schätzungsweise zehn zusätzliche Stellen (Juristinnen und Juristen sowie Informatikerinnen und Informatiker in der Lohnklasse 24, d. h. 1 800 000 Franken). Diese verteilen sich wie folgt:

– Nach Artikel 10 E-DSG können die privaten Berufs- und Wirtschaftsverbände sowie die Bundesorgane dem Beauftragten *Verhaltenskodizes* vorlegen. Dieser muss Stellung nehmen und seine Stellungnahmen veröffentlichen. Die Erarbeitung von Verhaltenskodizes durch die Branchen und die entsprechenden Stellungnahmen des Beauftragten sollen die Selbstregulierung im privaten Sektor ermöglichen. In den Verhaltenskodizes kann das Gesetz präzisiert und dadurch je nach Tätigkeitsbereich differenziert umgesetzt werden.[313] Die Kodizes entsprechen einem in der Regulierungsfolgenabschätzung identifizierten Bedarf an Rechtssicherheit (siehe Ziff. 1.8).

  Obwohl die Verhaltenskodizes nicht verbindlich sind, werden sie längerfristig zu einer besseren Umsetzung des Gesetzes führen, wodurch die Anzahl der Untersuchungen des Beauftragten abnehmen wird. Ausserdem werden jene, die dem Beauftragten ihren Verhaltenskodex vorgelegt haben, unter bestimmten Voraussetzungen von der Pflicht entbunden, eine Datenschutz-Folgenabschätzung (Art. 20 Abs. 5 E-DSG) vorzunehmen. Dadurch wird auch der Beauftragte entlastet, da er in der Folge nicht mehr vorgängig konsultiert werden muss (Art. 21 E-DSG).

  Die Förderung der Selbstregulierung ist eine in der Verordnung (EU) 2016/679 enthaltene Massnahme (Art. 40). Anders als im E-DSG ist im europäischen Erlass jedoch vorgesehen, dass die Aufsichtsbehörde den Kodex genehmigt. So erhält er für die Verantwortlichen, die ihm beitreten, einen verbindlichen Charakter. Der Bundesrat hat auf eine solche Lösung verzichtet. Sie hätte höhere Kosten nach sich gezogen, da der Beauftragte mittels beschwerdefähiger Verfügungen hätte entscheiden müssen.

  Die Anzahl der jährlich dem Beauftragten vorgelegten Verhaltenskodizes wird auf rund zehn geschätzt. Der damit verbundene Arbeitsaufwand wird je nach Komplexität und Länge der Kodizes variieren. Es ist jedoch davon auszugehen, dass diese Aufgabe durchschnittlich eine Vollzeit beschäftigte Person in Anspruch nehmen wird. Der Bundesrat schätzt, dass im ersten Jahr wenige Verhaltenskodizes vorgelegt werden, da die Branchen sie zuerst erarbeiten müssen. Nach seiner Auffassung dürften mit der Zeit auch weniger Kodizes vorgelegt werden, da die Anzahl der Organisationen, die dazu ermächtigt sind, beschränkt ist. Aus diesem Grund ist für das erste Jahr und das fünfte Jahr eine halbe Stelle eingeplant und eine ganze Stelle für das zweite bis vierte Jahr. Dies in der Annahme, dass der Beauftragte in diesen drei Jahren stärker beansprucht wird.

313 Siehe zum Beispiel den Verhaltenskodex der Union française du marketing vom 17. März 2005 unter www.cnil.fr/sites/default/files/typo/document/projet-codeUFMD.pdf.

Die Stelle sollte zu rund sechzig Prozent durch Gebühren finanziert werden können. Denn da die Förderung der Selbstregulierung einem öffentlichen Interesse entspricht, kann der Beauftragte in bestimmten Fällen in Anwendung von Artikel 3 Absatz 2 Buchstabe a AllgGebV auf die Gebührenerhebung verzichten.

– Nach Artikel 13 Absatz 2 Buchstaben d und e E-DSG müssen die Verantwortlichen dem Beauftragten für die Bekanntgabe von Personendaten ins Ausland *Standarddatenschutzklauseln* und *verbindliche unternehmensinterne Datenschutzvorschriften* zur Genehmigung unterbreiten, die einen angemessenen Datenschutz gewährleisten sollen. Die Genehmigung durch den Beauftragten entspricht einer Anforderung des europäischen Rechts (Art. 12bis Abs. 2 Bst. b E-SEV 108 und 46 Abs. 2 Bst. b und d sowie 47 der Verordnung [EU] 2016/679). Der Beauftragte muss die ihm unterbreiteten Texte dementsprechend prüfen und gegebenenfalls genehmigen. Im Hinblick auf den Angemessenheitsbeschluss der Europäischen Union und die Anforderungen des E-SEV 108 ist dies ein zentrales Element für die Gewährleistung eines angemessenen Datenschutzniveaus. Der Beauftragte wird per Verfügung entscheiden. Diese präventive Kontrolle durch den Beauftragten wird wie die Verhaltenskodizes zu einer besseren Beachtung der Datenschutznormen beitragen und sollte so längerfristig dazu führen, dass die Anzahl der von ihm eingeleiteten Untersuchungen rückläufig ist.

– Die Anzahl der dem Beauftragten vorgelegten Standarddatenschutzklauseln und verbindlichen unternehmensinternen Vorschriften wird auf rund zwanzig pro Jahr geschätzt. Der Arbeitsaufwand wird hauptsächlich von der Komplexität und Länge der Texte abhängen. Diese neue Aufgabe dürfte durchschnittlich eine Vollzeit beschäftigte Person in Anspruch nehmen. Der Personalbedarf wird mit der Zeit womöglich sinken, da die Anzahl der Standarddatenschutzklauseln und der verbindlichen unternehmensinternen Vorschriften, die erlassen werden müssen, nicht unbeschränkt ist. Die Stelle sollte zu rund sechzig Prozent durch Gebühren finanziert werden können. Auch hier kann in bestimmten Fällen in Anwendung von Artikel 3 Absatz 2 Buchstabe a AllgGebV auf die Gebührenerhebung verzichtet werden.

– Nach Artikel 21 E-DSG muss der Beauftragte vorgängig konsultiert werden, wenn eine *Datenschutz-Folgenabschätzung* (Art. 20 E-DSG) ergibt, dass die geplante Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hätte, wenn der Verantwortliche keine Massnahmen zur Eindämmung des Risikos trifft. Genauer gesagt muss der Beauftragte konsultiert werden, wenn der Verantwortliche der Auffassung ist, dass das Risiko unter Berücksichtigung der verfügbaren Technologien und der Implementierungskosten nicht durch vertretbare Mittel eingedämmt werden kann. Die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung ist eine Anforderung des europäischen Rechts (Art. 8bis Abs. 2 E-SEV 108, 27 der Richtlinie [EU] 2016/680 und 35 der Verordnung [EU] 2016/679). Die vorgängige Konsultation der Aufsichtsbehörde auf dem Gebiet des Datenschutzes ist in der Richtlinie (EU) 680/2016 (Art. 28) und der Verordnung (EU) 679/2016 (Art. 36) ausdrücklich vorgesehen.

– Aufgrund dieser neuen Aufgabe muss der Beauftragte die Folgenabschätzungen, die ihm unterbreitet werden, die geplanten Datenbearbeitungen sowie die von den Verantwortlichen vorgeschlagenen Massnahmen genau prüfen. Der Beauftragte muss darauf innert einer (um einen Monat verlängerbaren) Frist von zwei Monaten Stellung nehmen. Hat er Einwände, muss er geeignete Massnahmen vorschlagen. Dabei handelt es sich um ein zwingendes, oft komplexes Verfahren, in dem eine Juristin oder ein Jurist sowie eine Informatikerin oder ein Informatiker eingesetzt werden müssen. Mit der fortschreitenden Entwicklung der digitalen Wirtschaft werden die Datenbearbeitungen, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen zur Folge hätten, tendenziell zunehmen und komplexer werden, sodass auch das Instrument der Datenschutz-Folgenabschätzung an Bedeutung gewinnen wird.

  Die Anzahl der Überprüfungen wird auf zehn bis fünfzehn pro Jahr geschätzt. Für diese neue Aufgabe sind drei zusätzliche Stellen erforderlich. Angesichts der Tatsache, dass Artikel 21 E-DSG während zwei Jahren nach Inkrafttreten des Gesetzes nur für Datenbearbeitungen gemäss Artikel 1 und 2 der Richtlinie (EU) 2016/680 gilt (Art. 63 Abs. 2 E-DSG), schlägt der Bundesrat vor, dass zwei der drei zusätzlichen Stellen nach Ablauf dieser Frist für die Überprüfung der Datenschutz-Folgenabschätzungen geschaffen werden. Die Schaffung einer Stelle ab Inkrafttreten des Gesetzes ist dadurch begründet, dass der Beauftragte die internen Verfahren für diese neue Aufgabe definieren muss, damit er zum gegebenen Zeitpunkt operativ ist (Informatik, Weisungen). Ausserdem muss angesichts der Komplexität des Instruments der Datenschutz-Folgenabschätzung bei den Verantwortlichen eine grosse Sensibilisierungsarbeit geleistet werden. Die Massnahmen sollten längerfristig ebenfalls zur korrekten Umsetzung des Gesetzes und zu einer Verminderung der Anzahl Untersuchungen des Beauftragten führen. Die erforderlichen Stellen sollten fast ganz durch Gebühren finanziert werden können.

– Der Beauftragte eröffnet neu eine *Untersuchung*, wenn Anzeichen bestehen, dass gegen die Datenschutzvorschriften verstossen wurde, während die Fälle, in denen er nach geltendem Recht eine Untersuchung eröffnet (Art. 29 DSG), beschränkt sind. In Fällen von geringfügiger Bedeutung kann er auf eine Untersuchung verzichten (Art. 43 Abs. 2 E-DSG). Während er heute nur Empfehlungen abgeben kann, kann er in Zukunft verbindliche Verfügungen erlassen und zum Beispiel selbst eine Datenbearbeitung untersagen (Art. 43 ff. E-DSG). Er wird auch die Meldungen von Verletzungen der Datensicherheit nach Artikel 22 E-DSG prüfen. Diese neuen Kompetenzen werden vom europäischen Recht gefordert (Art. 7 Abs. 2 und 12bis Abs. 2 Bst. a und c E-SEV 108, 30 und 47 der Richtlinie [EU] 2016/680 und 33 und 58 Abs. 1 Bst. b und Abs. 2 der Verordnung [EU] 2016/679) und sind somit sehr wichtig im Hinblick auf den Angemessenheitsbeschluss und die Erfüllung der Anforderungen des E-SEV 108 sowie der Richtlinie (EU) 2016/680. Es sei hier auch daran erinnert, dass der Schweiz in der Schengen-Evaluation des Jahres 2014 (siehe Ziff. 1.2.2.3) von den europäischen Ex-

pertinnen und Experten bereits empfohlen worden ist, dem Beauftragten Verfügungskompetenzen zu erteilen.

Der Beauftragte wird noch weitere Aufsichtsaufgaben erfüllen müssen, die im Rahmen der Schengen-Zusammenarbeit in Strafsachen vorgesehen sind. So wird er auf Gesuch der betroffenen Personen, deren Rechte eingeschränkt wurden (Art. 349*g* E-StPO und Art. 11*c* E-IRSG) namentlich überprüfen müssen, ob die Personendaten rechtmässig bearbeitet worden sind.

Die Anzahl der vom Beauftragten durchgeführten Untersuchungen wird auf fünfzehn bis zwanzig pro Jahr geschätzt, die Anzahl der Meldungen von Verletzungen der Datensicherheit auf fünf bis zehn pro Jahr. Zur Erfüllung dieser neuen Aufgaben sind drei neue Stellen für ein interdisziplinäres Team aus zwei Juristinnen und Juristen und einer Informatikerin bzw. einem Informatiker notwendig. Nach Ansicht des Bundesrates dürfte dieser Bedarf nach ein paar Jahren abnehmen. Denn es ist anzunehmen, dass die Verantwortlichen mit der Zeit die geltenden Vorschriften kennen und sie von selbst besser umsetzen werden. Darüber hinaus werden die Verfügungen des Beauftragten sowie allfällige strafrechtliche Sanktionen der Kantonsbehörden voraussichtlich positive Anreize schaffen. Aus diesen Gründen schlägt der Bundesrat vor, den Bestand nach vier Jahren (d. h. 2022–2023) von drei auf zweieinhalb Stellen zu senken.

Was die eigentlichen Aufsichtsaufgaben anbelangt, können diese Stellen nur zu rund dreissig Prozent über Gebühren finanziert werden. Der Bundesrat weist allerdings darauf hin, dass er auf die Einführung von Verwaltungssanktionen verzichtet hat, denn für ein solches Regime wären aufgrund der damit verbundenen zusätzlichen Verfahrensgarantien mehr Mittel nötig gewesen.

– Artikel 49 E-DSG regelt die *Amtshilfe* zwischen dem Beauftragten und den ausländischen Datenschutzbehörden. Angesichts des zunehmend grenzüberschreitenden Charakters der Datenbearbeitungen ist die Zusammenarbeit zwischen den nationalen Datenschutzbehörden unerlässlich. Es handelt sich dabei zudem um eine Anforderung des europäischen Rechts (Art. 12bis Abs. 7 und 13 ff. E-SEV 108, 46 Abs. 1 Bst. h und 50 der Richtlinie [EU] 680/2016 und 57 Abs. 1 Bst. g und 61 der Verordnung [EU] 2016/679). Der zusätzliche Personalbedarf beläuft sich auf schätzungsweise eine Stelle. Für diese Aufgabe ist keine Selbstfinanzierung vorgesehen.

– Schliesslich sind für das neue *Privacy Shield* zwischen der Schweiz und den USA (siehe Ziff. 5) ebenfalls zusätzliche Ressourcen erforderlich. Die finanziellen Auswirkungen auf den Beauftragten in diesem Bereich wurden dem Bundesrat bereits angekündigt, als er am 11. Januar 2017 den neuen rechtlichen Rahmen für die Bekanntgabe von Personendaten aus der Schweiz an Unternehmen mit Sitz in den Vereinigten Staaten zur Kenntnis genommen hat.

  Für den Beauftragten zieht das Privacy Shield bestimmte Kooperationspflichten nach sich. Er leitet die Beschwerden der betroffenen Personen an die Federal Trade Commission, das Department of Commerce oder an die

Ombudsperson des Department of State weiter. Er leitet ausserdem die Auskunftsgesuche an die Ombudsperson des Department of State weiter. Da in den Vereinigten Staaten immer mehr Datenbearbeitungen fremdvergeben werden und in der Schweiz heute verbreitet Dienste amerikanischer Unternehmen wie Facebook, Google oder Apple in Anspruch genommen werden, ist davon auszugehen, dass die Anzahl der vom Beauftragten zu bearbeitenden Beschwerden und Gesuche stark zunehmen wird. In zwei Fällen müssen die unter dem Privacy Shield zertifizierten Unternehmen mit dem Beauftragten zusammenarbeiten: Werden HR-Daten aus Schweizer Unternehmen bearbeitet, müssen die Unternehmen in Datenschutzbelangen auf jeden Fall mit dem Beauftragten kooperieren. Diese Form der Zusammenarbeit kann ausserhalb der Bearbeitung von HR-Daten von den Unternehmen auch freiwillig gewählt werden.

Schliesslich muss der Beauftragte jährlich in Zusammenarbeit mit dem SECO die Qualität der im Privacy Shield vereinbarten Massnahmen zum Schutz der Persönlichkeit der betroffenen Personen überprüfen und einen Bericht verfassen.

Der zusätzliche Personalbedarf beläuft sich auf schätzungsweise eine Stelle, die nicht durch Gebühren finanziert werden kann.

Der zusätzliche Personalaufwand kann nicht intern kompensiert werden. Dies umso mehr, als der Beauftragte mit der exponentiell fortschreitenden Digitalisierung unabhängig von der Revisionsvorlage mit immer mehr Aufgaben betraut worden ist. Demgegenüber fällt kaum ins Gewicht, dass der Beauftragte wegen der Aufhebung der Pflicht zur Meldung von Datensammlungen im privaten Sektor auch von einigen Aufgaben entlastet wird.

Wie einleitend erwähnt wird sich der Personalbedarf des Beauftragten je nach Aufgabe im Verlauf der Zeit verändern. Die dynamische Entwicklung des Personalbedarfs lässt sich aus folgender nach Jahren aufgeschlüsselten Tabelle ablesen. Der Bedarf wird spätestens im Jahr 2023 neu beurteilt werden. Der Vollständigkeit halber umfasst die Tabelle auch den Personalbedarf des BJ (siehe Ziff. 11.1.2 für weitere Erläuterungen dazu).

	2018–19	2019–20	2020–21	2021–22	2022–23	Durch Gebühren finanziert
Prüfung der Verhaltens-kodizes	0,5	1	1	1	0,5	~ 60 %
Genehmigung der Standard-klauseln und der verbindli-chen unternehmensinternen Datenschutzvorschriften	1	1	1	1	1	~ 60 %
Prüfung der Datenschutz-Folgen-abschätzungen	1	1	3	3	3	~ 90 %
Untersuchungen / Prüfung der Meldungen von Verlet-zungen der Datensicherheit	3	3	3	3	2,5	~ 30 %
Amtshilfe	1	1	1	1	1	–
Aufgaben im Rahmen des Swiss-US Privacy Shield	1	1	1	1	1	–
Total Stellen Beauftragter	7,5	8	10	10	9	
Total Stellen OFJ	1	1	1	1	1	
Gesamttotal	**8,5**	**9**	**11**	**11**	**10**	

11.1.1.2 Informatikbedarf

Im Rahmen seiner Unabhängigkeit benötigt der Beauftragte ein minimales, auf seine Auftragserfüllung ausgerichtetes IT-Budget für Investitionen und Betrieb. Um einen effizienten und wirtschaftlich möglichst günstigen Betrieb sicherstellen zu können, bezieht der Beauftragte bereits heute alle Supportfunktionen (Informatik, Finanzen, Personal, Logistik) bei der Bundeskanzlei (BK). Ferner hat er sich entschieden, die IT-Standardleistungen des Bundes zu beziehen. Mit den gewählten Lösungen trägt der Beauftragte zur wirtschaftlich effizienten Aufgabenerfüllung bei, ohne seine Unabhängigkeit in Frage zu stellen. Trotz all dieser Bemühungen reicht das heutige Budget von rund 300 000 Franken für den Informatikbedarf für die Umsetzung des neuen DSG nicht mehr aus.

Nicht nur die Wirtschaft, sondern auch die Bundesverwaltung betreibt und entwickelt eine Vielzahl von Applikationen, die grosse Datenbestände bearbeiten. Der Beauftragte muss sich dabei vergewissern, dass die Personendaten in einer Art und Weise anonymisiert oder pseudonymisiert werden, die nach dem jeweils aktuellen Stand der Technik eine Re-Identifizierung von Personen mit hinreichender Wahrscheinlichkeit ausschliesst. Moderne Applikationen zur Bearbeitung von Personendaten werden heute in der Regel nicht mehr zur lokalen Installation ausgeliefert, sondern über das Internet zugänglich gemacht. Das bedeutet, dass die Sachverhaltsklärungen des Beauftragten im Hinblick auf mögliche Datenschutzverletzungen mit zunehmender Digitalisierung dynamischer und die Kontrollen anspruchsvoller und rascher abgeschlossen werden müssen.

Angesichts der zunehmenden Digitalisierung sind zusätzliche IKT-Mittel erforderlich, damit der Beauftragte seine neuen Aufgaben wahrnehmen kann:

Aufgabe	IT-Investitionen	IT-Betrieb, Wartung, Support, Release-management	Externes Expertenwissen. Spezifische Fragestellungen
	2019	*pro Jahr* ab 2020	ab 2019 jährlich
Testinfrastruktur/ Testsysteme: Diese dienen der Prüfung der datenschutzrechtlichen Relevanz der Datenbearbeitungen von Unternehmen und Verwaltungen	200 000 Franken	105 000 Franken	
Einbezug externer Spezialisten: Gezielter Einbezug externer IT-Spezialisten vor dem Hintergrund zunehmender Erhebung und Bearbeitung sowie des Austausches personenbezogener Daten			60 000 Franken
Ausbau der elektronischen Kommunikations- und Arbeitsmittel (Webservices) für Auskünfte und Beratungen	240 000 Franken	85 000 Franken	
Total einmalige IKT-Investitionsausgaben	440 000 Franken		
Total jährlich wiederkehrende IKT-Aufwendungen		190 000 Franken	60 000 Franken

Für die Prüfung der datenschutzrechtlichen Relevanz der Datenbearbeitung von Unternehmen und Bundesorganen sollen Testsysteme beschafft werden. Die Analyse soll sich dabei auf Dienstleistungen, Produkte und Geschäftsprozesse mit erhöhtem Gefahrenpotenzial für die Privatsphäre fokussieren. Hierfür sind besondere Schutzmassnahmen erforderlich, weshalb diese Untersuchungen in abgesicherten virtuellen Umgebungen über einen normalen Internetzugang gemacht werden. So lässt sich u. a. der Datenaustausch von Applikationen und Produkten über das Internet nachvollziehen (z. B. Webportale, Einbindung sozialer Netzwerke und Webtracking in Webseiten, Datenbearbeitungen von mobilen Geräten).

Aufgrund der steigenden technologischen Anforderungen an den Datenschutz und der wachsenden Zahl von mobilen Geräten, die über Sensoren Daten beschaffen und über das Internet in Rechenzentren weiterleiten, wird die Datenschutzbehörde des Bundes situativ auch externes Expertenwissen beiziehen müssen. Aufgrund der hohen Dynamik der Informations- und Kommunikationstechnologien wäre ein Aufbau und aktiver Unterhalt von spezifischem Wissen nicht sinnvoll. Obschon es für einzelne Abklärungen des Einbezugs von Spezialisten bedarf, ist eine generelle

Auslagerung der Abklärungen an Dritte wegen der Vertraulichkeit der Abklärungen nicht möglich.

Der Ausbau der elektronischen Kommunikations- und Arbeitsmittel (Webservices) soll es der Datenschutzbehörde des Bundes erlauben, gemäss den neuen gesetzlichen Aufgaben präventiv und beratend tätig zu sein. Dazu gehört insbesondere die internetbasierte Unterstützung bei Datenschutz-Folgenabschätzungen, die Erfassung und Bearbeitung von Meldungen von Verletzungen der Datensicherheit und von Garantien beim Austausch von Personendaten mit dem Ausland sowie interaktive Tools zur Förderung von datenschutzkonformen Verhaltensregeln. Ebenso soll ein Trigger- und Meldesystem (z. B. Hinweisgebersysteme, Datenverarbeitungsregister) für die – auch anonyme – Anzeige von Verstössen gegen die Datenschutzvorschriften umgesetzt werden. Soweit vorhanden sollen Lösungen und Services aus der Bundesverwaltung übernommen werden.

Die einmaligen IKT-Investitionen inkl. Projektkosten für die Umsetzung des neuen DSG werden heute auf 440 000 Franken geschätzt. Durch die notwendigen IKT-Infrastrukturen, Anwendungen und Services ist mit zusätzlichen, jährlichen IKT-Kosten von 105 000 Franken zu rechnen. Der jährliche Mehrbedarf an IKT-Mitteln für den Beizug von IKT-Spezialwissen beträgt 60 000 Franken.

Die neuen Lösungen sollen bis spätestens 2020 entwickelt und eingeführt werden. Sie sind nach einer Einsatzperiode von fünf Jahren neu zu beschaffen.

11.1.2 Finanzielle und personelle Auswirkungen auf das Bundesamt für Justiz

Die Prüfung des Datenschutzniveaus eines fremden Staates oder eines internationalen Organs (Art. 13 Abs. 1 E-DSG) wird dem BJ obliegen. Es wird nicht nur prüfen müssen, ob eine Gesetzgebung bzw. eine interne Regelung vorliegt, die einen angemessenen Datenschutz gewährleistet, sondern auch, wie sie umgesetzt wird. Geprüft werden müssen namentlich die Gesetzestexte, die Rechtsprechung und die Lehre zum Thema. Es sind auch einzelne Reisen ins Ausland sowie eine Zusammenarbeit mit anderen Behörden, etwa mit der Europäischen Kommission oder dem Ausschuss für das revidierte Übereinkommen SEV 108, vorzusehen.

Der Bundesrat geht davon aus, dass für diese neue Aufgabe eine neue Stelle geschaffen werden muss (eine Juristin bzw. ein Jurist in der Lohnklasse 25). Das entspricht jährlichen Personalkosten von 192 900 Franken, einschliesslich der Arbeitgeberbeiträge. Diese Kosten können nicht intern finanziert werden. Die Kosten für die Einrichtung eines Arbeitsplatzes hingegen können kompensiert werden. Dazu kommen 50 000 Franken für Berufskosten und Aufträge an Sachverständige.

Bei seinen Abklärungen wird sich der Bundesrat so weit wie möglich auf verfügbare Quellen stützen (insbesondere die Evaluationen im Rahmen des Übereinkommens SEV 108 oder der Europäischen Union). Doch die Anzahl der zu beurteilenden Staaten dürfte in Zukunft steigen. Es handelt sich zudem um einen dynamischen Prozess, der nicht unterschätzt werden darf. Darüber hinaus wird die vom Bundesrat veröffentlichte Liste einen höheren Stellenwert haben und der Bundesrat wird die

Verantwortung für die Evaluation des angemessenen Datenschutzniveaus der geprüften Staaten übernehmen.

11.2 Auswirkungen auf die Kantone und Gemeinden

Die Ratifizierung des Änderungsprotokolls zum Übereinkommen SEV 108 durch die Schweiz ist auch für die Kantone verbindlich. Die Bestimmungen des Übereinkommens müssen unter Einhaltung der verfassungsmässigen Kompetenzverteilung ins Schweizer Recht übertragen werden. Dasselbe gilt für die Bestimmungen der Richtlinie (EU) 2016/680.

Weitere Auswirkungen auf die Kantone und Gemeinden ergeben sich daraus, dass der Beauftragte, gemäss den ihm vom neuen Gesetz verliehenen Kompetenzen, zur Umsetzung seiner Untersuchungsmassnahmen die Hilfe der kantonalen und kommunalen Polizeiorgane anfordern kann. Zudem ist die Amtshilfe zwischen dem Beauftragten und den kantonalen Datenschutzbehörden vorgesehen.

Der Ausbau der Strafbestimmungen, insbesondere die Einführung des Straftatbestands des Missachtens von Verfügungen des Beauftragten, sollte nicht zu einem deutlichen Anstieg der Strafverfahren in den Kantonen führen. Denn die Verfügungen des Beauftragten können angefochten werden. Es dürfte nur in einzelnen Fällen vorkommen, dass die Verfügungen missachtet werden, sobald sie rechtskräftig sind.

11.3 Auswirkungen im Informatikbereich

Der Gesetzesentwurf hat gewisse Folgen für die automatisierte Datenbearbeitung. So muss der Verantwortliche sicherstellen, dass die betroffene Person während der gesamten Datenbearbeitung im Internet oder im Falle einer automatisierten Einzelentscheidung informiert ist. Zudem muss der Verantwortliche, wenn er risikobehaftete Bearbeitungen plant, eine Datenschutz-Folgenabschätzung vornehmen und die Risiken sowie die entsprechenden Massnahmen dem Beauftragten melden. Der Verantwortliche hat ausserdem standardmässig ab dem Zeitpunkt der Planung einer Datenbearbeitung auf die Einhaltung der Datenschutzgrundsätze zu achten sowie ein Verzeichnis der Bearbeitungstätigkeiten zu führen. Schliesslich muss er dem Beauftragten und gegebenenfalls auch der betroffenen Person Verstösse gegen die Sicherheit von Personendaten melden.

Die Auswirkungen auf die Bundesorgane sind in verschiedener Hinsicht geringfügiger. So wird die Pflicht, vorgängig eine Datenschutz-Folgenabschätzung vorzunehmen und ab der Planung die Datenschutzgrundsätze einzuhalten, in der Praxis kaum Auswirkungen haben, da die Bundesorgane bereits heute dem Datenschutzverantwortlichen oder, falls kein solcher vorhanden ist, dem Beauftragten unverzüglich alle Projekte zur automatisierten Bearbeitung von Personendaten melden müssen, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden (Art. 20 Abs. 2 VDSG).

Artikel 25 der Richtlinie (EU) 2016/680 verpflichtet die Schengen-Staaten, bestimmte Bearbeitungsvorgänge in automatisierten Systemen zu protokollieren. Gemäss dieser Bestimmung müssen es die Protokolle ermöglichen, die durchgeführten Bearbeitungsvorgänge zu bestimmen und die Begründung, das Datum und die Uhrzeit einer Abfrage oder Offenlegung von Personendaten und so weit wie möglich die Identifizierung der Person, die die Daten abgefragt oder offengelegt hat, und die Identität des Empfängers festzustellen. Der Bundesrat ist der Auffassung, dass die automatisierten Datenbearbeitungssysteme, die von den Bundesorganen in der Schengen-Zusammenarbeit in Strafsachen betrieben werden, den Anforderungen der Bestimmung der EU entsprechen. Es ist jedoch nicht ausgeschlossen, dass die europäischen Expertinnen und Experten bei einer künftigen Evaluation der Schweiz auf dem Gebiet des Datenschutzes zu einem anderen Schluss kommen und der Schweiz empfehlen, die technischen Massnahmen zu ergreifen, damit die Protokollierung der geprüften automatisierten Bearbeitung sämtliche Angaben nach Artikel 25 der Richtlinie (EU) 2016/680 liefert. Die Umsetzung einer solchen Empfehlung wäre mit finanziellen Auswirkungen verbunden, die zum jetzigen Zeitpunkt nicht beziffert werden können. Schliesslich hat auch die Pflicht der Bundesorgane, ihre Bearbeitungstätigkeiten dem Beauftragten zu melden, keine praktischen Auswirkungen, da sie im Wesentlichen der in Artikel 11*a* Absatz 2 DSG vorgesehenen Pflicht entspricht, dem Beauftragten sämtliche Datensammlungen zur Registrierung anzumelden.

In Bezug auf das vom Beauftragten geführte Register der Datensammlungen ergibt sich mit dem Inkrafttreten des neuen Gesetzes die Änderung, dass darin nur noch die Bearbeitungstätigkeiten der Bundesorgane gespeichert werden und nicht mehr jene von privaten Personen.

11.4 Auswirkungen auf die Volkswirtschaft

Ziel des Gesetzesentwurfs ist es, den Datenschutz zu verbessern, insbesondere indem die Datenbearbeitung transparenter gestaltet wird und die betroffenen Personen mehr Kontrolle über ihre Daten erhalten. Denn angesichts sich ständig weiterentwickelnder Technologien wird es für diese immer schwieriger, zu wissen, wer zu welchem Zweck und für wen Daten über sie bearbeitet. Zudem soll mit dem Gesetzesentwurf für eine bessere Überwachung der Anwendung und Einhaltung der nationalen Datenschutzbestimmungen gesorgt werden: Durch die ihm neu erteilten Verfügungskompetenzen ist der Beauftragte erheblich besser in der Lage, die Privatsphäre der betroffenen Personen zu schützen.

Ferner wird mit dem Gesetzesentwurf bezweckt, den grenzüberschreitenden Datenverkehr zu erleichtern, indem sichergestellt wird, dass die Daten von Land zu Land ausgetauscht werden können. So wird die Schweiz von den EU-Mitgliedstaaten als Drittstaat betrachtet, wenn es um den Datenaustausch im privaten Sektor geht. Derzeit profitiert die Schweiz von einem Angemessenheitsbeschluss der Europäischen Kommission[314], welcher der Schweiz ein ausreichendes Datenschutzniveau

314 ABl. L 215 vom 25.8.2000, S. 1.

bescheinigt. Dadurch wird die Datenübermittlung zwischen einem in der Europäischen Union angesiedelten Privatunternehmen und einer privaten Person in der Schweiz einer Datenübermittlung innerhalb der Europäischen Union gleichgestellt. In Bezug auf die Angemessenheit kann die EU-Kommission jedoch gemäss Artikel 46 Absätze 4 und 5 der Verordnung (EU) 2016/679 jederzeit zu einem anderen Ergebnis kommen. Der Gesetzesentwurf dient also auch dazu, das Schweizer Recht so den europäischen Anforderungen anzupassen, dass die Schweiz weiterhin von einem positiven Angemessenheitsbeschluss der Europäischen Union ausgehen kann. Die Ratifizierung des Änderungsprotokolls zum Übereinkommen SEV 108 sollte es allgemein erlauben den grenzüberschreitenden Datenverkehr zwischen der Schweiz und den Mitgliedsstaaten sowie den Nichtmitgliedsstaaten beizubehalten, welche das Übereinkommen unterzeichnet haben. Es ist davon auszugehen, dass die Ratifizierung dieses Protokolls für die Europäische Union eine wesentliche Voraussetzung dafür ist, der Schweizer Rechtsordnung ein angemessenes Schutzniveau zu bescheinigen (Art. 45 Verordnung [EU] 2016/679).

Mit der Anhebung des Datenschutzniveaus auf den europäischen Standard stärkt der Gesetzesentwurf auch das Vertrauen der Verbraucherinnen und Verbraucher in die Bearbeitung ihrer persönlichen Daten, insbesondere in Bezug auf elektronisch abgewickelte Transaktionen. In dieser Hinsicht ist der Gesetzesentwurf nicht nur positiv für die Verbraucherinnen und Verbraucher, sondern er bringt auch Vorteile für die Unternehmen, da diese attraktiv bleiben und sich ihnen neue Geschäftsmöglichkeiten eröffnen könnten, insbesondere was den elektronischen Handel angeht. Die Kosten für die Umsetzung der neuen Pflichten des Verantwortlichen dürften durch diese Vorteile aufgewogen werden.

Ausserdem ist zu berücksichtigen, dass schweizerische Unternehmen, welche in den Mitgliedstaaten der EU Dienstleistungen anbieten, die Verordnung (EU) 2016/679 bereits aufgrund des darin vorgesehenen weiten räumlichen Anwendungsbereichs berücksichtigen müssen. Für diese Unternhmen führt der vorliegende Gesetzesentwurf nicht zu hohen zusätzlichen Kosten, da er ähnliche Massnahmen wie die europäische Veordnung enthält.

Die staatlichen Eingriffe werden auf ein absolutes Minimum begrenzt. Die Idee besteht vielmehr darin, das Verantwortungsbewusstsein der Verantwortlichen zu stärken und diese zur Einhaltung von Verhaltenskodizes oder zur Nutzung des Zertifizierungsverfahrens zu ermutigen. Grosse Autonomie erhalten auch die wirtschaftlichen Akteure, die zum Beispiel in Bezug auf den grenzüberschreitenden Datenverkehr die Möglichkeit haben, sich durch freiwillige Massnahmen – wie vom Beauftragten vorgängig genehmigte Standarddatenschutzklauseln oder verbindliche unternehmensinterne Datenschutzvorschriften – des Bestehens eines geeigneten Datenschutzniveaus zu versichern. Durch die nach der Vernehmlassung eingeführten Erleichterungen, namentlich im Bereich der Meldepflichten, sollte der Verwaltungsaufwand beschränkt bleiben.

11.5 Auswirkungen auf Gesundheit und Gesellschaft

Um die mit den neuen Technologien verbundenen gesellschaftlichen Herausforderungen zu bewältigen, sieht der Gesetzesentwurf unter anderem die Stärkung der Aufsichtsbefugnisse des Beauftragten vor. Ausserdem erhält der Beauftragte die Aufgabe, die Öffentlichkeit, namentlich besonders schutzbedürftige Personen wie Minderjährige und ältere Menschen, für den Datenschutz zu sensibilisieren.

Die neue Gesetzgebung stärkt zudem die Position der Verbraucherinnen und Verbraucher sowie von schutzbedürftigen Personen.

Abgesehen davon, dass der verbesserte Datenschutz auch für Datenbearbeitungen zu medizinischen Zwecken gilt, sind keine direkten Auswirkungen auf die Gesundheit zu erwarten.

11.6 Auswirkungen auf die Gleichstellung von Mann und Frau

Es sind keine Auswirkungen auf die Gleichstellung von Mann und Frau zu erwarten.

11.7 Auswirkungen auf die Umwelt

Es sind keine direkten ökologischen Auswirkungen zu erwarten.

12 Verhältnis zur Legislaturplanung und zu den nationalen Strategien des Bundesrates

12.1 Verhältnis zur Legislaturplanung

Der Gesetzesentwurf ist in der Botschaft vom 27. Januar 2016 über die Legislaturplanung 2015–2019[315] angekündigt worden.

12.2 Verhältnis zu Strategien des Bundesrates

Der Entwurf ist mit der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) und mit der Strategie «Open Government Data» vereinbar. Ferner ist der Gesetzesentwurf Teil des Massnahmenkatalogs zur Umsetzung der Strategie «Digitale Schweiz» (vgl. Ziff. 1.1.3).

315 BBl **2016** 1105 1219

13 Rechtliche Aspekte

13.1 Verfassungsmässigkeit

13.1.1 Zuständigkeit für die Genehmigung des Notenaustausches betreffend die Übernahme der Richtlinie (EU) 2016/680

Gemäss Artikel 54 Absatz 1 BV sind die auswärtigen Angelegenheiten Sache des Bundes, woraus sich ergibt, dass der Bund auch für den Abschluss von Verträgen mit anderen Staaten zuständig ist. Grundsätzlich müssen solche Verträge gemäss Artikel 166 Absatz 2 BV von der Bundesversammlung genehmigt werden. Der Bundesrat kann völkerrechtliche Verträge nur dann selbständig abschliessen, wenn er durch ein Bundesgesetz oder durch einen von der Bundesversammlung genehmigten völkerrechtlichen Vertrag dazu ermächtigt ist oder wenn es sich um einen Vertrag mit beschränkter Tragweite handelt (Art. 166 Abs. 2 BV, Art. 24 Abs. 2 ParlG, Art. 7*a* RVOG).

Im vorliegenden Fall fehlt es an einer besonderen gesetzlichen oder vertraglichen Ermächtigung des Bundesrates, da Artikel 36 Absatz 5 DSG nicht anwendbar ist. Ebenfalls ist der Notenaustausch betreffend die Übernahme der Richtlinie (EU) 2016/680 nicht lediglich von beschränkter Tragweite. Folglich ist die Bundesversammlung für die Genehmigung des Notenaustausches zuständig.

Artikel 141 Absatz 1 Buchstabe d BV bestimmt, dass internationale Verträge dem Referendum unterstehen, wenn sie unbefristet und unkündbar sind (Ziff. 1), den Beitritt zu einer internationalen Organisation vorsehen (Ziff. 2), wichtige rechtsetzende Bestimmungen enthalten oder deren Umsetzung den Erlass von Bundesgesetzen erfordert (Ziff. 3).

Der Notenaustausch zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 fällt nicht unter Artikel 141 Absatz 1 Buchstabe d Ziffern 1 und 2 BV. Es bleibt also zu prüfen, ob dieses Abkommen wichtige rechtsetzende Bestimmungen enthält oder seine Umsetzung den Erlass von Bundesgesetzen erfordert. Als rechtsetzende Bestimmungen gelten gemäss Artikel 22 Absatz 4 ParlG Bestimmungen, die in unmittelbar verbindlicher und generell-abstrakter Weise Pflichten auferlegen, Rechte verleihen oder Zuständigkeiten festlegen. Im Übrigen sind nach Artikel 164 Absatz 1 BV alle wichtigen rechtsetzenden Bestimmungen in der Form eines Bundesgesetzes im formellen Sinne zu erlassen.

Die Umsetzung des Notenaustauschs betreffend die Übernahme der Richtlinie (EU) 2016/680 erfordert mehrere Gesetzesänderungen. Daraus folgt, dass der Bundesbeschluss zur Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 gemäss Artikel 141 Absatz 1 Buchstabe d Ziffer 3 BV dem Referendum für völkerrechtliche Verträge untersteht.

13.1.2 Zuständigkeit für die Genehmigung des Änderungsprotokolls zum Übereinkommen SEV 108

Artikel 4 des Entwurfs des Protokolls zur Revision des Übereinkommens SEV 108 bestimmt die Pflichten der Vertragsparteien. Gemäss Absatz 1 muss jede Vertragspartei in ihrem innerstaatlichen Recht die erforderlichen Massnahmen treffen, um die Bestimmungen des Übereinkommens SEV 108 zu verwirklichen. Absatz 2 regelt zudem, dass diese Massnahmen spätestens zu dem Zeitpunkt zu treffen sind, an dem das neue Übereinkommen ratifiziert wird oder der Beitritt zu diesem erfolgt. Vorbehalte sind gemäss Artikel 25 des Entwurfs nicht zulässig.

Der Gesetzesentwurf steht im Einklang mit dem E-SEV 108. Sobald das Änderungsprotokoll zum Übereinkommen SEV 108 zur Unterzeichnung aufgelegt wird, könnte der Bundesrat dieses unterzeichnen und dem Parlament zur Genehmigung vorlegen. Aus den in Ziffer 13.1.1 genannten Gründen untersteht auch der Bundesbeschluss über die Genehmigung des Änderungsprotokolls zum Übereinkommen SEV 108 durch die Schweiz gemäss Artikel 141 Absatz 1 Buchstabe d Ziffer 3 BV dem Referendum für völkerrechtliche Verträge.

13.1.3 Rechtsetzungskompetenz des Bundes

Wie der Bundesrat in seiner Botschaft vom 19. Februar 2003 zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll des Datenschutzübereinkommens[316] schreibt, enthält die Bundesverfassung keine Bestimmung, die dem Bund ausdrücklich eine Kompetenz im Datenschutzbereich zuweist. Wohl stipuliert Artikel 13 Absatz 2 BV den Anspruch jeder Person auf Schutz vor Missbrauch ihrer persönlichen Daten. Es handelt sich hier aber um ein Grundrecht, dass dem Bund keine neuen Zuständigkeiten überträgt. Gemäss Artikel 35 Absätze 2 und 3 BV sind Personen, die staatliche Aufgaben wahrnehmen, an die Grundrechte gebunden und verpflichtet, zu ihrer Verwirklichung beizutragen, und die Behörden sorgen dafür, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden. Der Entwurf trägt in diesem Sinne zur Verwirklichung von Artikel 13 Absatz 2 BV bei, und zwar sowohl hinsichtlich der Beziehungen zwischen Staat und Privaten als auch zwischen Individuen. Der E-DSG konkretisiert die Garantien von Artikel 13 Absatz 2 BV für die natürlichen Personen. Für die Bearbeitung von Daten juristischer Personen durch Bundesorgane schlägt der Bundesrat die Einführung einer Minimalregelung im RVOG vor.

Beim Erlass privatrechtlicher Datenschutzbestimmungen kann sich der Bundesgesetzgeber auf die Rechtsetzungskompetenzen in den Bereichen Zivilrecht (Art. 122 BV), privatwirtschaftliche Erwerbstätigkeit (Art. 95 BV) und Verbraucherschutz (Art. 97 Abs. 1 BV) stützen.

316 BBl **2003** 2101, 2151

In Bezug auf den Erlass öffentlich-rechtlicher Datenschutzbestimmungen für Behörden und Verwaltungsstellen kann sich der Bundesgesetzgeber auf die organisatorische Zuständigkeit nach Artikel 173 Absatz 2 BV berufen.

Die Bundesverfassung gesteht den Kantonen volle organisatorische Autonomie zu, sodass es in deren Kompetenz liegt, den Datenschutz in ihrem Bereich zu regeln. Der Bund kann deshalb nur für jene öffentlichen kantonalen oder kommunalen Bereiche Datenschutzbestimmungen erlassen, in denen die Kantone Bundesrecht ausführen, welches selbstverständlich wiederum einer verfassungsrechtlichen Grundlage bedarf. Der Bund muss jedoch selbst in diesem Fall darauf achten, nicht in die organisatorischen Kompetenzen der Kantone einzugreifen. Der vorliegende Entwurf beachtet diese Grenzen. Die Bereiche, in denen der Datenschutz verstärkt wird, betreffen die Bearbeitung von Daten durch Bundesrecht ausführende Kantonsbehörden oder gemeinsame Datenbearbeitungen von Organen des Bundes und der Kantone. Schliesslich wird im Gesetzesentwurf Artikel 37 DSG (Vollzug durch die Kantone) aufgehoben.

13.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Der Gesetzesentwurf ist vereinbar mit den internationalen Verpflichtungen der Schweiz (vgl. insbesondere Ziff. 1.2, 1.3, 2, 3, 4 und 9.3). Er erlaubt ihr, das Änderungsprotokoll zum Übereinkommen SEV 108 zu ratifizieren, sobald dies möglich ist (vgl. Ziff. 3.2 und 3.3). Zudem kann die Schweiz auf diese Weise die Verpflichtungen nach dem Schengen-Assoziierungsabkommen mit der Europäischen Union erfüllen (vgl. Ziff. 1.2.2.3, 2.2–2.4 und 9.3).

Artikel 61 der Richtlinie (EU) 2016/680 bestimmt, dass internationale Übereinkünfte, welche die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, die von den Mitgliedstaaten vor dem Inkrafttreten der Richtlinie (EU) 2016/680 geschlossen wurden und die mit dem vor dem genannten Datum geltenden Unionsrecht vereinbar sind, in Kraft bleiben, bis sie geändert, ersetzt oder gekündigt werden.[317]

Der Gesetzesentwurf hat auch keine Auswirkungen auf die gemeinsame Erklärung der Schweiz und der Europäischen Union betreffend Artikel 23 Absatz 7 des Übereinkommens vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union.[318] Artikel 60 der Richtlinie (EU) 2016/680 sieht vor, dass die Bestimmungen der Rechtsakte, welche die Europäische Union vor der Richtlinie (EU) 2016/680 verabschiedet hat, unverändert bleiben.

317 Erwägung 95.
318 SR **0.362.31**

13.3 Erlassform

Die Vorlage des Bundesrates umfasst zwei Erlassentwürfe:

- den Entwurf eines Bundesbeschlusses zur Genehmigung des Notenaustausches betreffend die Übernahme der Richtlinie (EU) 2016/680,
- den Entwurf eines Mantelerlasses, mit einer Totalrevision des DSG und im Anhang dazu die dadurch notwendigen Anpassungen weitere Bundesgesetze (Ziffer I) sowie den Änderungen von Bundesgesetzen, die sich aus der Umsetzung der Richtlinie (EU) 2016/680 im Rahmen der Schengen-Verpflichtungen ergeben (Ziffer II).

13.4 Unterstellung unter die Ausgabenbremse

Der Gesetzesentwurf bringt keine Ausgaben mit sich, welche der Ausgabenbremse (Art. 159 Abs. 3 Bst. b BV) unterstehen.

13.5 Einhaltung der Grundsätze des Subventionsgesetzes

Der Gesetzesentwurf sieht keine Subventionen vor.

13.6 Delegation von Rechtssetzungsbefugnissen

Der E-DSG enthält namentlich in den folgenden Bestimmungen eine Delegation von Rechtsetzungskompetenzen an den Bundesrat:

- *Art. 11 Abs. 5, Art. 23 Abs. 6:* Der Bundesrat kann Ausnahmen von den Pflichten betreffend die Führung eines Verzeichnisses der Bearbeitungstätigkeiten sowie vom Auskunftsrecht der betroffenen Personen und von der Kostenlosigkeit vorsehen.
- *Art. 13 Abs. 3:* Der Bundesrat kann andere geeignete Garantien für die Bekanntgabe von Personendaten ins Ausland vorsehen.
- *Art. 29:* Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.
- *Art. 31:* Der Bundesrat behält die Kompetenz, unter bestimmten Voraussetzungen im Rahmen von Pilotversuchen die automatisierte Bearbeitung besonders schützenswerter Daten zu bewilligen.
- *Art. 53:* Der Bundesrat kann festlegen, in welchen Fällen es möglich ist, auf die Erhebung einer Gebühr zu verzichten oder sie zu reduzieren.

13.7 Koordination mit anderen Gesetzesvorlagen

In den parlamentarischen Beratungen müssen folgende Bundesgesetze geändert werden, die nach der Verabschiedung der vorliegenden Botschaft in Kraft treten:

- Das Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit: Die neuen Artikel 23*b* und 23*c* treten gleichzeitig mit dem Bundesgesetz vom 25. September 2015[319] über den Nachrichtendienst in Kraft. In Artikel 23*b* Absatz 2 Buchstabe c muss der Begriff «Persönlichkeitsprofil» durch «Personendaten» ersetzt werden und im Einleitungssatz von Artikel 23*c* Absatz 2 muss er gestrichen werden.
- Mehrwertsteuergesetz vom 12. Juni 2009[320]: Die eidgenössische Steuerverwaltung (ESTV) bearbeitet und analysiert auf automatisierte Weise Daten natürlicher Personen (z. B. Betreibungen, Verlustscheine, Rechnungsfehler, Angaben im Bereich des Zollwesens etc.), um Risikoprofile zu erstellen, die es erlauben, Steuerprüfungen gezielter durchzuführen. Hierfür benötigt die ESTV eine formell-gesetzliche Grundlage. In Artikel 76 Absatz 1 und Artikel 76*a* Absatz 1 muss der Begriff des «Persönlichkeitsprofils» entfernt werden. Stattdessen muss die ESTV die Kompetenz zum Profiling erhalten. Artikel 76*a* Absatz 3 Buchstabe g ist aufzuheben. Artikel 76*b* Absatz 2 ist so anzupassen, dass die ESTV auch im Nachgang eines Profilings Daten bekanntgeben darf. Artikel 76 ist um einen Absatz 1bis zu ergänzen, wonach der Beauftragte für seine Aufsichtstätigkeit Zugang zum Bearbeitungssystem der ESTV erhält.
- Das Bundesgesetz vom 25. September 2015 über den Nachrichtendienst: In Artikel 44 Absatz 1 muss der Begriff «Persönlichkeitsprofil» ersetzt werden durch «andere Personendaten, welche die Beurteilung des Gefährlichkeitsgrades einer Person erlauben». In Artikel 46 Absatz 1 muss der Begriff «Datensammlung» durch «Datenbank» ersetzt werden. In Artikel 61 Absatz 2 muss der Verweis auf Artikel 6 Absatz 2 DSG durch einen Verweis auf Artikel 13 Absatz 1 E-DSG ersetzt werden. Artikel 64 muss ebenfalls in verschiedenen Punkten geändert werden: Absatz 2 muss angepasst werden, da der Beauftragte gemäss dem künftigen DSG keine Empfehlungen mehr abgibt, sondern befugt ist, eine Untersuchung zu eröffnen; Absatz 3 kann aufgehoben werden, da es nicht mehr erforderlich ist, dass das Bundesverwaltungsgericht eingreift; Absatz 4 muss dahingehend angepasst werden, dass der Beauftragte bei Fehlern bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft den Nachrichtendienst des Bundes (NDB) mit Verfügung verpflichten muss, diese zu beheben; Absatz 5 muss dahingehend angepasst werden, dass der Beauftragte verfügen kann, dass der NDB der betroffenen Person sofort Auskunft erteilt, wenn die Voraussetzungen nach dieser Bestimmung erfüllt sind. Artikel 65 kann aus den gleichen Gründen wie Artikel 64 Absatz 3 aufgehoben werden; auch der Verweis auf Artikel 65 Absatz 1 in Artikel 66 Absatz 1 muss gestrichen werden. Schliesslich muss die Terminologie in Artikel 78 angepasst werden: Der Begriff «Inha-

319 BBl **2015** 7211
320 SR **641.20**, Änderungen vom 30. September 2016 AS **2017** 3575

ber der Datensammlung» muss durch «Verantwortlicher» ersetzt werden; der Begriff «Datensammlung» kann durch «Informationssysteme, Datenbanken und Akten» ersetzt werden.

– Bundesgesetz vom 20. Juni 2014[321] über das Schweizer Bürgerrecht: Dieses Gesetz tritt am 1. Januar 2018 in Kraft. In Artikel 44 muss der Begriff «Persönlichkeitsprofil» durch «Personendaten, welche die Beurteilung der Eignungsvoraussetzungen der Bewerberin oder des Bewerbers erlauben» ersetzt werden.

– Militärgesetz vom 3. Februar 1995: Der neue Artikel 100 tritt am 1. Januar 2018 in Kraft.[322] In Absatz 3 Buchstabe a muss der Begriff «Persönlichkeitsprofil» durch «Personendaten, welche die Beurteilung des Grades der Gefährlichkeit einer Person erlauben» ersetzt und in Buchstabe b muss auf die Artikel 13 und 14 E-DSG verwiesen werden. In Absatz 4 Buchstabe c Ziffer 2 wird der Begriff «Datensammlung» durch «Datenbearbeitungstätigkeit» ersetzt.

In den parlamentarischen Beratungen müssen ferner Bestimmungen zur Koordination des Gesetzesentwurfs mit folgenden Bundesgesetzen, bei denen das Datum des Inkrafttretens noch nicht bekannt ist, formuliert werden:

– Bundesgesetz vom 18. März 2016[323] betreffend die Überwachung des Post- und Fernmeldeverkehrs: In Artikel 4 muss der Begriff «Persönlichkeitsprofil» gestrichen werden. In Artikel 13 muss der Begriff «Inhaber der Datensammlung» durch «Verantwortlicher» ersetzt werden.

– Änderung vom 18. März 2016 des Heilmittelgesetzes[324]: In Artikel 62*a* muss der Begriff «Persönlichkeitsprofil» gestrichen werden.

– Strafregistergesetz vom 17. Juni 2016[325]: In Artikel 3 Absatz 1 muss der Begriff «Datenherr» durch «Verantwortlicher» ersetzt werden. In Artikel 12 Absatz 2 ist der Begriff «Datensammlung» durch «Datenbank» zu ersetzen. In Artikel 25 Absatz 1 schliesslich ist in der französischen Fassung der Begriff «fichier journal» zu streichen.

– Energiegesetz vom 30. September 2016[326]: Aufgrund der Aufhebung des Schutzes der Daten juristischer Personen im E-DSG und der Beschränkung des Begriffs der Personendaten in Artikel 4 Buchstabe a E-DSG auf Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, muss die Terminologie in Artikel 56 Absatz 1, in Artikel 58 Sachüberschrift, Absatz 1 und Absatz 3 sowie in Artikel 59 Sachüberschrift, Absatz 1 und Absatz 2 angepasst werden, um klarzustellen, dass diese Bestimmungen auch auf Daten juristischer Personen Anwendung finden. Der Ausdruck «Personendaten» ist jeweils durch «Personendaten sowie Daten juristischer Personen» zu ersetzen bzw. zu ergänzen. In dem durch das Energiegesetz

321 BBl **2014** 5133
322 BBl **2014** 7063
323 BBl **2016** 1991
324 BBl **2016** 1953
325 BBl **2016** 4871
326 BBl **2016** 7683

vom 30. September 2016 zu ändernden Stromversorgungsgesetz vom 23. März 2007[327] sind folgende Anpassungen vorzunehmen: In Artikel 17*c* Absatz 1 soll ergänzt werden, dass das DSG sinngemäss auch auf die Bearbeitung von Daten juristischer Personen Anwendung findet. In Artikel 27 Absatz 1 ist der Ausdruck «Personendaten» durch «Personendaten sowie Daten juristischer Personen» zu ersetzen.

– Änderung vom 16. Juni 2017 des Bundespersonalgesetzes[328]: In Artikel 27 Absatz 2 muss der Begriff «Persönlichkeitsprofile» gestrichen werden.

– Änderung vom 16. Juni 2017 des Luftfahrtgesetzes[329]: In Artikel 21*c* Absatz 1 Buchstabe b muss der Begriff «Persönlichkeitsprofil» gestrichen werden.

– Krebsregistrierungsgesetz vom 18. März 2016[330]: In Artikel 7 Absatz 2 muss der Begriff «Inhaber einer Datensammlung» durch «Verantwortlicher» ersetzt werden.

13.8 Koordination mit anderen Gesetzgebungsgeschäften

Der Gesetzesentwurf kann Auswirkungen auf folgende Erlasse haben, die revidiert werden:

– Entwurf zum Bundesgesetz über Geldspiele (BGS)[331]: Die gesetzlichen Grundlagen zu den Persönlichkeitsprofilen müssen angepasst werden.

– Entwurf zum Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG).

– Entwurf zum Bundesgesetz über die Organisation der Bahninfrastruktur[332].

– Entwurf zur Revision des Fernmeldegesetzes[333]: Die Botschaft sollte Ende Sommer 2017 verabschiedet werden. Gegebenenfalls müssen bestimmte Datenschutzbegriffe an die neue Terminologie des künftigen DSG angepasst werden.

– Entwurf zur Revision des Ausländergesetzes: Die Botschaft des Bundesrates sollte im Herbst 2017 verabschiedet werden. Gegebenenfalls müssen bestimmte Datenschutzbegriffe an die neue Terminologie des künftigen DSG angepasst werden.

– Entwurf zur Änderung des Schweizerischen Zivilgesetzbuchs (Beurkundung des Personenstands und Grundbuch)[334]: Der neue Wortlaut von Artikel 45*a* ZGB ist zu berücksichtigen und allenfalls anzupassen.

327 SR **734.7**; vgl. BBl **2016** 7683
328 SR **172.220.1**; vgl. BBl **2016** 353 362
329 BBl **2017** 4257
330 BBl **2016** 1939
331 BBl **2015** 7769
332 BBl **2016** 8749
333 SR **784.10**
334 BBl **2014** 3587

– Vorentwurf des Bundesgesetz über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten: Die Terminologie muss gegebenenfalls angepasst werden und der Begriff «Persönlichkeitsprofil» aufgehoben werden.

– Entwurf zur Änderung des Finanzmarktaufsichtsgesetzes (Änderung des Erlasses im Rahmen des Entwurfs zum Bundesgesetz über die Finanzinstitute)[335]: In Artikel 13*a* Absatz 2 muss der Begriff «Persönlichkeitsprofile» gestrichen werden. In Artikel 13*a* Absatz 1 ist ausserdem zu ergänzen, dass die FINMA neben Daten ihrer Angestellten auch die Daten von «Stellenbewerberinnen und Stellenbewerbern» bearbeiten kann. Bei der beispielhaften Aufzählung der Aufgaben der FINMA, für welche sie Daten bearbeitet, ist der «Bewerbungsprozess» hinzuzufügen. Schliesslich soll präzisiert werden, dass die FINMA für die Datenbearbeitung die Unterstützung von Auftragsbearbeitern in Anspruch nehmen kann.

335 BBl **2015** 9139