



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz und Polizeidepartement EJPD

Bundesamt für Justiz BJ

Direktionsbereich Öffentliches Recht

Fachbereich Rechtssetzungsprojekte und -methodik

21. Dezember 2016

Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz

Inhalt

Zusammenfassung	5
1 Grundzüge der Vorlage	6
1.1 Ausgangslage auf nationaler Ebene	6
1.1.1 Geltendes Recht	6
1.1.2 Vorarbeiten und Konzept	8
1.1.3 Strategie «Digitale Schweiz»	8
1.1.4 Weitere Arbeiten der Bundesverwaltung im Zusammenhang mit dem Datenschutz	9
1.1.5 Parlamentarische Vorstösse	10
1.2 Ausgangslage auf internationaler Ebene	13
1.2.1 Vorbemerkung	13
1.2.2 Europäische Union	13
1.2.2.1 Einschlägige Regelung	13
1.2.2.2 Angemessenheitsbeschluss	14
1.2.2.3 Empfehlungen im Zusammenhang mit den Schengener Abkommen	15
1.2.3 Europarat	15
1.2.4 Vereinte Nationen	16
1.2.5 OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten	17
1.3 Ziele der Revision	17
1.4 Darstellung des revidierten Datenschutzgesetzes	18
1.4.1 Leitlinien der Revision	18
1.4.2 Hauptsächliche Neuerungen	19
1.4.2.1 Änderung des Geltungsbereichs des künftigen DSGVO	19
1.4.2.2 Erhöhte Transparenz von Datenbearbeitungen und verstärkte Kontrolle durch die betroffenen Personen	20
1.4.2.3 Förderung der Selbstregulierung	20
1.4.2.4 Stärkung der Stellung und Ausbau der Befugnisse und Aufgaben des Beauftragten	20
1.4.2.5 Ausbau der strafrechtlichen Sanktionen	20
1.5 Darstellung der Revision anderer Bundesgesetze	21
1.6 Weitere geprüfte Massnahmen	21
1.6.1 Erlass verbindlicher Datenschutzvorschriften durch den Beauftragten	21
1.6.2 Beweislastumkehr	21
1.6.3 Kollektive Rechtsdurchsetzung	21
1.6.4 Recht auf Datenportabilität	22
1.6.5 Ausserparlamentarische Kommission für die Erarbeitung und Genehmigung von Empfehlungen der guten Praxis	22
1.6.6 Änderung der Organisation der Aufsichtsbehörde	22
1.6.7 Einrichtung spezieller Konfliktlösungsmechanismen	22
1.7 Regulierungsfolgenabschätzung	22
1.7.1 Notwendigkeit und Möglichkeit staatlichen Handelns	23
1.7.2 Auswirkungen auf die einzelnen gesellschaftlichen Gruppen	23
1.7.3 Auswirkungen auf die Gesamtwirtschaft	24
1.7.4 Alternative Regelungen	24
1.7.5 Zweckmässigkeit im Vollzug	24
2 Richtlinie (EU) 2016/680	25
2.1 Erläuterung der Richtlinie (EU) 2016/680	25
2.1.1 Verlauf der Verhandlungen	25
2.1.2 Kurzer Überblick	25
2.2 Übernahme der Richtlinie (EU) 2016/680 als Schengen-Weiterentwicklung	26
2.3 Regelungskonzept	27
2.4 Hauptsächliche notwendige Gesetzesänderungen	28
3 Entwurf zur Revision des Übereinkommens SEV 108 (E-SEV 108)	28
3.1 Kurzer Überblick	28
3.2 Ratifizierung des Änderungsprotokolls zum Übereinkommen SEV 108	29
3.3 Hauptsächliche notwendige Gesetzesänderungen	30
4 Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten	30
4.1 Kurzer Überblick	30
4.2 Angleichung der schweizerischen Gesetzgebung	31
5 Vergleich mit der Gesetzgebung aussereuropäischer Staaten, die das Übereinkommen SEV 108 nicht ratifiziert haben	32
5.1 Argentinien	32
5.2 Neuseeland	33
5.3 Südkorea	34
5.4 Japan	35
5.5 Singapur	35

6	Umsetzung.....	36
7	Abschreibung parlamentarischer Vorstösse.....	37
8	Gesetzesänderungen	38
8.1	Erläuterung des VE-DSG	38
8.1.1	Zweck, Geltungsbereich und Begriffe.....	38
8.1.1.1	Art. 1 Zweck	38
8.1.1.2	Art. 2 Geltungsbereich	39
8.1.1.3	Art. 3 Begriffe	43
8.1.2	Allgemeine Datenschutzbestimmungen	45
8.1.2.1	Art. 4 Grundsätze	45
8.1.2.2	Art. 5 Bekanntgabe ins Ausland	48
8.1.2.3	Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen	51
8.1.2.4	Art. 7 Auftragsdatenbearbeitung.....	52
8.1.2.5	Art. 8 Ausarbeitung von Empfehlungen der guten Praxis.....	52
8.1.2.6	Art. 9 Einhaltung der Empfehlungen der guten Praxis	53
8.1.2.7	Art. 10 Zertifizierung	54
8.1.2.8	Art. 11 Datensicherheit	54
8.1.2.9	Art. 12 Daten einer verstorbenen Person.....	54
8.1.3	Pflichten des Verantwortlichen und des Auftragsbearbeiters.....	56
8.1.3.1	Art. 13 Informationspflicht bei der Beschaffung von Daten.....	56
8.1.3.2	Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen	57
8.1.3.3	Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung	59
8.1.3.4	Art. 16 Datenschutz-Folgenabschätzung	60
8.1.3.5	Art. 17 Meldung von Verletzungen des Datenschutzes.....	62
8.1.3.6	Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen.....	63
8.1.3.7	Art. 19 Weitere Pflichten	65
8.1.4	Rechte der betroffenen Person.....	66
8.1.4.1	Art. 20 Auskunftsrecht.....	66
8.1.4.2	Art. 21 Einschränkung des Auskunftsrechts.....	67
8.1.4.3	Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende	67
8.1.5	Besondere Bestimmungen für die Bearbeitung von Daten durch private Personen	68
8.1.5.1	Art. 23 Persönlichkeitsverletzungen.....	68
8.1.5.2	Art. 24 Rechtfertigungsgründe.....	69
8.1.5.3	Art. 25 Rechtsansprüche.....	70
8.1.6	Besondere Bestimmungen für die Bearbeitung von Daten durch Bundes-organe	71
8.1.6.1	Art. 26 Verantwortliches Organ und Kontrolle	71
8.1.6.2	Art. 27 Rechtsgrundlagen	72
8.1.6.3	Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen	72
8.1.6.4	Art. 29 Bekanntgabe von Personendaten.....	73
8.1.6.5	Art. 30 Widerspruch gegen die Bekanntgabe von Daten.....	73
8.1.6.6	Art. 31 Angebot von Unterlagen an das Bundesarchiv.....	73
8.1.6.7	Art. 32 Bearbeiten für Forschung, Planung und Statistik.....	74
8.1.6.8	Art. 33 Privatrechtliche Tätigkeit von Bundesorganen.....	74
8.1.6.9	Art. 34 Ansprüche und Verfahren	74
8.1.6.10	Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Daten enthalten.....	75
8.1.6.11	Art. 36 Register der Datenbearbeitungstätigkeiten	76
8.1.7	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte bzw. -beauftragter	76
8.1.7.1	Art. 37 Ernennung und Stellung.....	76
8.1.7.2	Art. 38 Wiederwahl und Beendigung der Amtsdauer	76
8.1.7.3	Art. 39 Nebenbeschäftigung.....	77
8.1.7.4	Art. 40 Aufsicht.....	77
8.1.7.5	Art. 41 Untersuchung.....	77
8.1.7.6	Art. 42 Vorsorgliche Massnahmen.....	79
8.1.7.7	Art. 43 Verwaltungsmassnahmen.....	79
8.1.7.8	Art. 44 Verfahren	80
8.1.7.9	Art. 45 Anzeigepflicht.....	80
8.1.7.10	Art. 46 Amtshilfe zwischen schweizerischen Behörden	81
8.1.7.11	Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden	81
8.1.7.12	Art. 48 Information	82
8.1.7.13	Art. 49 Weitere Aufgaben.....	82
8.1.8	Strafbestimmungen	83
8.1.8.1	Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten	83
8.1.8.2	Art. 51 Verletzung der Sorgfaltspflichten	85
8.1.8.3	Art. 52 Verletzung der beruflichen Schweigepflicht.....	85
8.1.8.4	Art. 53 Übertretungen in Geschäftsbetrieben	86
8.1.8.5	Art. 54 Anwendbares Recht und Verfahren	87
8.1.8.6	Art. 55 Verfolgungsverjährung für Übertretungen	87
8.1.9	Abschluss von Staatsverträgen.....	87
8.1.10	Schluss- und Übergangsbestimmungen.....	87

8.1.10.1	Art. 57 Vollzug durch die Kantone	87
8.1.10.2	Art. 58 Aufhebung und Änderung anderer Erlasse	87
8.1.10.3	Art. 59 Übergangsbestimmung	88
8.2	Erläuterungen zu den Änderungen anderer Bundesgesetze	88
8.2.1	Aufhebung des Bundesgesetzes über den 19. Juni 1992 über den Datenschutz	88
8.2.2	Änderung der Terminologie in Bundesgesetzen	88
8.2.3	Ausländergesetz vom 16. Dezember 2015	88
8.2.4	Asylgesetz vom 26. Juni 1998	89
8.2.5	Öffentlichkeitsgesetz vom 17. Dezember 2004	89
8.2.6	Verwaltungsverfahrensgesetz vom 20. Dezember 1968	90
8.2.7	Zivilgesetzbuch	90
8.2.8	Bundesgesetz vom 24. März 2000 über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten	91
8.2.9	Zivilprozessordnung	91
8.2.9.1	Gerichtsstand	91
8.2.9.2	Befreiung von den Gerichtskosten	91
8.2.9.3	Verfahrensart	92
8.2.10	Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht	92
8.2.11	Strafgesetzbuch	93
8.2.12	Bundesgesetz vom 22. März 1974 über das Verwaltungsstrafrecht	94
8.2.13	Militärstrafprozess vom 23. März 1979 (MStP)	95
8.2.14	Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes	96
8.2.15	Bundesstatistikgesetz vom 9. Oktober 1992	96
8.2.16	Militärgesetz vom 3. Februar 1995	96
8.2.17	Bundesgesetz vom 3. Oktober 2008 über die militärischen Informationssysteme	97
8.2.18	Waffengesetz vom 20. Juni 1997	97
8.2.19	Bundesgesetz vom 4. Oktober 2002 über den Bevölkerungsschutz und den Zivilschutz	97
8.2.20	Bundesgesetz vom 21. Dezember 1948 über die Luftfahrt	97
8.2.21	Bundesgesetz vom 3. Oktober 1951 über die Betäubungsmittel und die psychotropen Stoffe	97
8.3	Kommentare zu den Änderungen der Bundesgesetze, welche die Anforderungen der Richtlinie (EU) 2016/680 umsetzen	98
8.3.1	Strafgesetzbuch	98
8.3.1.1	Art. 349a	98
8.3.1.2	Art. 349b	98
8.3.1.3	Art. 349c	98
8.3.1.4	Art. 349d	98
8.3.1.5	Art. 349e	100
8.3.1.6	Art. 349f	101
8.3.1.7	Art. 349g	102
8.3.1.8	Art. 349h	103
8.3.1.9	Art. 349i	103
8.3.1.10	Art. 355a Abs. 1 und 4	104
8.3.1.11	Art. 355f und Art. 355g	104
8.3.2	Strafprozessordnung	104
8.3.3	Rechtshilfegesetz vom 20. März 1981	104
8.3.3.1	Art. 11b	105
8.3.3.2	Art. 11c	105
8.3.3.3	Art. 11d	105
8.3.3.4	Art. 11e	106
8.3.3.5	Art. 11f	106
8.3.3.6	Art. 11g	107
8.3.3.7	Art. 11h	107
8.3.3.8	Art. 11i	107
8.3.4	Bundesgesetz vom 3. Oktober 1975 zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen	107
8.3.5	Bundesgesetz vom 7. Oktober 1994 über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten	107
8.3.6	Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes	108
8.3.7	Schengen-Informationsaustausch-Gesetz vom 12. Juni 2009	108
9	Auswirkungen	108
9.1	Finanzielle und personelle Auswirkungen auf den Bund	108
9.2	Auswirkungen auf die Kantone und Gemeinden	109
9.3	Auswirkungen im Informatikbereich	109
9.4	Auswirkungen auf die Volkswirtschaft	110
9.5	Auswirkungen auf Gesundheit und Gesellschaft	111
9.6	Auswirkungen auf die Gleichstellung von Mann und Frau	111
9.7	Auswirkungen auf die Umwelt	111
10	Verhältnis zur Legislaturplanung und zu den nationalen Strategien des Bundesrates	111
10.1	Verhältnis zur Legislaturplanung	111
10.2	Verhältnis zu Strategien des Bundesrates	111

11	Rechtliche Aspekte.....	112
11.1	Verfassungsmässigkeit	112
11.1.1	Zuständigkeit für die Genehmigung des Notenaustausches betreffend die Übernahme der Richtlinie (EU) 2016/680.....	112
11.1.2	Zuständigkeit für die Genehmigung E-SEV 108.....	112
11.1.3	Rechtsetzungskompetenz des Bundes	113
11.2	Vereinbarkeit mit internationalen Verpflichtungen der Schweiz	113
11.3	Erlassform	113
11.4	Unterstellung unter die Ausgabenbremse	114
11.5	Einhaltung der Grundsätze des Subventionsgesetzes	114
11.6	Delegation von Rechtssetzungsbefugnissen	114

Zusammenfassung

Die vorliegende Revision hat zum Ziel, den Datenschutz zu stärken, indem die Transparenz der Bearbeitung und die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten verbessert werden. Zugleich soll das Verantwortungsbewusstsein der für die Bearbeitung verantwortlichen Personen 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 gewährleistet und verbessert werden, namentlich indem die Bekanntgabe von Daten ins Ausland erleichtert wird. Ein hoher, international anerkannter Schutzstandard soll auch die Entwicklung neuer Wirtschaftszweige im Bereich der Digitalisierung der Gesellschaft fördern.

Ausgangslage und Ziele der Revision

Die Revision beruht auf einem Bundesratsbeschluss, wonach eine Vorlage mit zwei Zielsetzungen ausgearbeitet werden soll: 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 Europarates und der Europäischen Union Rechnung tragen. Das Projekt ist auch in den Zielen des Bundesrates für das Jahr 2016 und dem Legislaturprogramm 2015-2019 enthalten. Der Datenschutz war in den vergangenen Jahren auch Gegenstand zahlreicher parlamentarischer Interventionen. Dies verdeutlicht, dass der politische Wille besteht, die Bundesgesetzgebung in diesem Bereich zu stärken.

Auch auf internationaler Ebene wird dem Datenschutz immer grössere Beachtung geschenkt. So hat die Europäische Union 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 Anfang 2017 verabschiedet werden soll.

Die Revision 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 die Vorlage die Anforderungen der Richtlinie (EU) 2016/680 übernehmen, damit die Schweiz ihren Schengen-Verpflichtungen nachkommen kann. Die Revision setzt auch die Empfehlungen um, welche die Europäische Union ihr im Rahmen der Schengen-Evaluation gemacht hat. Dabei wurde insbesondere empfohlen, die Kompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten auszubauen. Schliesslich soll die Vorlage die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Diese Annäherung bildet zusammen mit der Ratifizierung des revidierten Übereinkommens SEV 108 die zentrale Voraussetzung dafür, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht. Dieser

Angemessenheitsbeschluss ist insbesondere für die Schweizer Wirtschaft von zentraler Bedeutung.

Wesentliche Inhalte der Vorlage

Im Einklang mit den europäischen Normen und der Mehrheit der ausländischen Rechtsordnungen wird der Datenschutz für juristische Personen abgeschafft. Dies erleichtert auch die Bekanntgabe von Daten ins Ausland, die ebenfalls verbessert wird.

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 über Entscheidungen informiert werden, die auf einer rein automatisierten Datenbearbeitung beruhen. Auch muss sie die Gelegenheit erhalten, ihren Standpunkt darzulegen. 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 insbesondere über Empfehlungen der guten Praxis, welche die Tätigkeit der Verantwortlichen erleichtern und die Einhaltung des Gesetzes verbessern sollen. Die Empfehlungen können einerseits durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten erarbeitet werden, der dabei auch die interessierten Kreise miteinbeziehen muss. Andererseits können die interessierten Kreise selbst Empfehlungen entwickeln und sie anschliessend durch den Beauftragten genehmigen lassen.

Die Unabhängigkeit und die Position des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten wird 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 bei deren Abschluss eine Verfügung erlassen kann.

Schliesslich werden auch die Strafbestimmungen des Datenschutzgesetzes in verschiedener Hinsicht verschärft. Dies erfolgt insbesondere, weil der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, anders als seine europäischen Amtskollegen, keine Verwaltungsanktionen verfügen darf.

Neben der Revision des Datenschutzgesetzes müssen verschiedene weitere Bundesgesetze angepasst werden. Namentlich müssen die Anforderungen der Richtlinie (EU) 2016/680 ins Strafgesetzbuch, die Strafprozessordnung und das Rechtshilfegesetz umgesetzt sowie einige Bestimmungen des Schengen-Informationsaustauschgesetzes angepasst werden.

1 Grundzüge der Vorlage

1.1 Ausgangslage auf nationaler Ebene

1.1.1 Geltendes Recht

Auf Bundesebene ist der Datenschutz gegenwärtig im Bundesgesetz vom 19. Juni 1992¹ über den Datenschutz (DSG) geregelt, das am 1. Juli 1993 in Kraft getreten ist.

Das DSG gilt für die Bearbeitung von Daten natürlicher und juristischer Personen durch private Personen und 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).

¹ SR 235.1

Das DSG enthält zunächst 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. Personen oder Bundesorgane, die Personendaten bearbeiten, haben sich zudem über deren Richtigkeit zu vergewissern (Art. 5).

Anschliessend enthält das DSG Vorschriften über die Bekanntgabe von Personendaten ins Ausland (Art. 6) und das Auskunftsrecht (Art. 8 bis 10). In Artikel 10a ist die Bearbeitung von Daten durch Dritte geregelt. Gemäss Artikel 11a ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (im Folgenden « der Beauftragte») 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 gegen den ausdrücklichen Willen der betroffenen Person keine Personendaten 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 das DSG 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 18a sind Bundesorgane verpflichtet, die betroffene Person über die Beschaffung von Personendaten zu informieren; vorbehalten sind einige Ausnahmen (Art. 18b). Grundsätzlich dürfen Bundesorgane Personendaten nur an Dritte bekannt geben, wenn dafür eine Rechtsgrundlage besteht (Art. 19 Abs. 1). Auch dürfen Personendaten nur 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 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 26a 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 DSGVO und Bestimmungen in Spezialgesetzen des Bundes wird die 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 DSGVO 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 DSGVO einer Evaluation² unterzogen. Diese hat ergeben, dass durch die technologischen und gesellschaftlichen Entwicklungen seit dem Inkrafttreten des DSGVO neue Bedrohungen für den Datenschutz entstanden sind. Die Wirksamkeit des DSGVO soll deshalb verbessert werden. Zum Teil reicht das DSGVO nicht mehr aus, um einen genügenden Schutz zu gewährleisten. Ausgehend von den Schlussfolgerungen des Berichts vom 9. Dezember 2011³ 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 DSGVO zu begleiten. Diese Arbeitsgruppe setzte sich aus Vertreterinnen und Vertretern der Bundesverwaltung⁴, der Kantone⁵, der Wirtschaft⁶, der Konsumentenschutzorganisationen⁷ sowie aus Expertinnen und Experten zusammen. Die Begleitgruppe präsentierte ihre Überlegungen im Bericht vom 29. Oktober 2014 mit dem Titel «Normkonzept zur Revision des Datenschutzgesetzes»⁸.

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 Bundesrat hat entschieden, einen Vorentwurf in Form eines referendumspflichtigen Mantelerlasses (Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz; im Folgenden «VE») in die Vernehmlassung zu geben. Der Mantelerlass besteht aus einer Ziffer I, welche die Totalrevision des DSGVO (im Folgenden «VE-DSG») und im Anhang die dadurch notwendigen Anpassungen weiterer Bundesgesetze beinhaltet. Ziffer II der Mantelerlasses enthält die Änderungen von Bundesgesetzen, die sich aus der Umsetzung der Richtlinie (EU) 2016/680 im Rahmen der Schengen-Verpflichtungen ergeben. Im vorliegenden Bericht werden die geänderten Erlasse jeweils mit «VE» bezeichnet, gefolgt von der Abkürzung des betreffenden Gesetzes (vgl. Ziff. 8.2 ff.).

1.1.3 Strategie «Digitale Schweiz»

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

² BÜRO VATTER/INSTITUT FÜR EUROPARECHT, Evaluation des Bundesgesetzes über den Datenschutz - Schlussbericht, Bern 11. März 2011, <https://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, BBI 2012 335.

⁴ In der Arbeitsgruppe waren die folgenden Bundesbehörden vertreten: der Beauftragte, die Bundeskanzlei (BK), das Bundesamt für Kommunikation (BAKOM), das Schweizerische Bundesarchiv (SBA), 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 <https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-d.pdf>.

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 Aktionsplan⁹ erarbeitet, der alle Massnahmen umfasst, die von der Bundesverwaltung umzusetzen sind. Der VE ist eine dieser Massnahmen (Ziff. 1.2 und 1.7 des Aktionsplans).

Im Rahmen der Erarbeitung dieser Strategie liess das BAKOM von der Berner Fachhochschule eine Studie zur Problematik von Big Data erstellen: «Big Data: Chancen, Risiken und Handlungsbedarf des Bundes»¹⁰. 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 VE vorgesehenen Massnahmen gehen in diese Richtung.

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 (NCS)*¹¹ vom 27. Juni 2012: 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.

Open Government Data Strategie Schweiz (OGD) vom 16. April 2014¹²: Mit dieser Strategie soll die Publikation von Daten, die von der Verwaltung beschafft werden, als Open Government Data (OGD), also als frei weiterverwendbare Behördendaten, 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» (NFP 75)*¹³: 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.

⁹ <https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/aktionsplan.html>.

¹⁰ «Big Data: Chancen, Risiken und Handlungsbedarf des Bundes», verfügbar (ausschliesslich auf Deutsch) unter: <https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/big-data.html>.

¹¹ https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html.

¹² https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn004-open_government_data_strategie_schweiz.html.

¹³ <http://www.nfp75.ch/de>.

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 gebildet. Gegebenenfalls führen die Arbeiten der Expertenkommission zu zusätzlichen Reformen im Bereich des Datenschutzes. Allerdings ist der Handlungsspielraum des schweizerischen Gesetzgebers aufgrund des europäischen Umfelds begrenzt. Soweit sich ein Bedarf nach zusätzlichen Reformen ergibt, könnten diese in einer nächsten Etappe umgesetzt werden. Zudem ist nicht auszuschliessen, dass auch in anderen Bereichen als dem Datenschutz (beispielsweise im Zivilrecht, im Immaterialgüterrecht, bei der Objektsicherheit, im Wettbewerbsrecht usw.) ein entsprechender Reformbedarf besteht. Die Arbeiten der Kommission werden voraussichtlich nicht vor 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»¹⁴ lancierten Aktivitäten weiterzuführen. Dieses Programm wurde von 2011 bis 2015 umgesetzt. Das EDI (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 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. Diese werden in fünf Bereiche aufgeteilt: Arbeitsmarkt, Forschung und Entwicklung, Sharing Economy, Digital Finance und Wettbewerbspolitik. Diese Bereiche werden im Rahmen des Berichts überprüft und wo nötig werden regulatorische Anpassungen angeregt, um mit attraktiven wirtschaftspolitischen Rahmenbedingungen ein positives Umfeld für die Digitale Wirtschaft zu schaffen.

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 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 einem 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). 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

¹⁴ <http://www.jeunesetmedias.ch/de/accueil.html>.

durch den Bericht des Bundesrates vom 9. Dezember 2011 über die Evaluation des Bundesgesetzes über den Datenschutz teilweise erfüllt.¹⁵

- 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 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.¹⁶
- 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 welcher der Bundesrat beauftragt wird, 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 Revision des DSG hinaus (vgl. Ziff. 1.1.4). Doch einige Massnahmen, die mit der Umsetzung dieser Motion zusammenhängen, können im Rahmen dieser Revision realisiert werden.
- Postulat Recordon 13.3989 «Verletzungen der Persönlichkeitsrechte im Zuge des Fortschritts der Informations- und Kommunikationstechnik»: Der Nationalrat 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 Herstellung» (Control by Design) in die Gesetzgebung eingeführt werden soll, so dass 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.

¹⁵ BBI 2012 335, hier 350

¹⁶ BBI 2012 335, hier 350

- 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»: Diesen Vorstoss hat der Nationalrat am 20. März 2015 angenommen. Es hat denselben Wortlaut wie das Postulat Comte 14.4284 «Videoaufnahmen durch Private. Die Privatsphäre besser schützen».
- Postulat Comte 14.4284 «Videoaufnahmen durch Private. Die Privatsphäre besser schützen»: Diesen Vorstoss hat der Ständerat am 19. März 2015 angenommen. 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.
- Postulat Derder 15.4045 «Recht auf Nutzung der persönlichen Daten. Recht auf Kopie»: Der Nationalrat hat diesen Vorstoss am 18. Dezember 2015 angenommen. Er 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.
- Motion Béglé 16.3379 «Förderung der Schweiz als universeller virtueller Datentresor». Mit dieser Motion wird der Bundesrat beauftragt, im Rahmen der Revision den Schutz der Daten von juristischen Personen (Ziff. 1) sowie Artikel 11 DSG beizubehalten, der eine fakultative Zertifizierung vorsieht (Ziff. 2). Nach Auffassung des Motionärs sind diese Bestimmungen von entscheidender Bedeutung, um ein optimales Datenschutzniveau zu gewährleisten und die Schweiz auf diese Weise als universellen virtuellen Datentresor zu positionieren. Der Nationalrat hat diese Motion am 30. September 2016 behandelt. Er hat der Ziffer 1 nicht zugestimmt, die Ziffer 2 hat er hingegen 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. In seiner Antwort schlägt der Bundesrat die Annahme vor und präzisiert, dass die Thematik der Wiedererlangung der Kontrolle über persönliche Daten unabhängig von der aktuellen Revision im Rahmen der Strategie «Digitale Schweiz» zu prüfen sei. Der Nationalrat hat diesem Vorstoss am 30. September 2016 zugestimmt.

1.2 Ausgangslage auf internationaler Ebene

1.2.1 Vorbemerkung

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. nachfolgende 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 Art. 13 der Bundesverfassung, sondern auch in verschiedenen völkerrechtlich verbindlichen Abkommen garantiert wird (Art. 8 der Europäischen Menschenrechtskonvention¹⁷, Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte¹⁸), 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) oder das Recht auf Familienleben (Art. 14 BV, Art. 8, 12 EMRK, Art. 23 UNO-Pakt II).

Für Einschränkungen des Schutzes der Privatsphäre sei insbesondere auf die Anforderungen an einen rechtmässigen Eingriff gemäss Art. 8 Abs. 2 EMRK verwiesen (gesetzliche Grundlage, Rechtfertigung aus einer 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.¹⁹ 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 (wie etwa über Ernährungsgewohnheiten, Gesundheitszustand etc.) 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 1995²⁰ zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (im Folgenden «Richtlinie 95/46/EG»). Diese Richtlinie wurde ergänzt durch den Rahmenbeschluss 2008/977/JAI²¹ vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (im Folgenden «Rahmenbeschluss 2008/977/JAI»).

¹⁷ EMRK, SR 0.101

¹⁸ UNO-Pakt II, SR 0.103.2

¹⁹ 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.

²⁰ ABl. L 281 vom 23.11.1995, S. 31.

²¹ ABl. L 350 vom 30.12.2008, S. 60.

Im Rahmen des Stockholmer Programms²² 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 Europäische Rat hat die Europäische Kommission gebeten, die Funktionsweise der Richtlinie 95/46/EG und des Rahmenbeschlusses 2008/977/JAI zu evaluieren und ihm gegebenenfalls neue Initiativen im Bereich des Datenschutzes vorzulegen. In ihrer Mitteilung vom 4. November 2010 mit dem Titel «Gesamtkonzept für den Datenschutz in der Europäischen Union»²³ 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) 2016/679²⁴ zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (im Folgenden «Verordnung [EU] 2016/679»), welche die Richtlinie 95/46/EG ersetzen wird (vgl. Ziff. 4 unten). Der zweite verabschiedete Erlass ist die Richtlinie (EU) 2016/680²⁵ zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (im Folgenden «Richtlinie [EU] 2016/680»), die den Rahmenbeschluss 2008/977 /JAI ersetzen wird (vgl. Ziff. 2 unten).

Für die Schweiz ist die Richtlinie (EU) 2016/680 Bestandteil des Schengen-Acquis. Aufgrund des Abkommens vom 26. Oktober 2004 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 (nachfolgend Schengen-Assoziierungsabkommen)²⁶ muss sie die Richtlinie daher umsetzen. Hingegen ist die Schweiz 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.

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.

Die Europäische Kommission hat in einem Angemessenheitsbeschluss vom 26. Juli 2000 bestätigt, dass die Schweiz über ein angemessenes Datenschutzniveau verfügt.²⁷ Diese Entscheidung beruht jedoch auf dem in der Richtlinie 95/46/EG festgelegten Schutzniveau. 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 von zentraler Bedeutung, dass die schweizerische Gesetzgebung den Anforderungen dieser Verordnung entspricht.

²² ABl. C 115 vom 4.5.2010, S. 1.

²³ COM (2010) 609 final.

²⁴ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1.

²⁵ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977 /JAI des Rates, ABl. L 119 vom 4.5.2016, S. 89.

²⁶ SR 0.362.31

²⁷ Entscheidung der Europäischen Kommission vom 26. Juli 2000 (ABl. L 215 vom 25.8.2000, S. 1).

1.2.2.3 Empfehlungen im Zusammenhang mit den Schengener Abkommen

Mit der Schengen-Assoziierung hat sich die Schweiz 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/JAI, entspricht.

Im Rahmen der Schengen-Evaluation überprüft die Europäische Union regelmässig die Schengen-Staaten und damit auch die Schweiz darauf, ob diese 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 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.

Der VE-DSG kommt den Empfehlungen des Rates insoweit nach, als der Beauftragte Verfügungskompetenzen erhält (siehe Art. 41-43 VE-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 Datenschutzgesetzes sind nach Auffassung des Bundesrates wirksam genug.

1.2.3 Europarat

Am 28. Januar 1981 hat der Europarat den ersten völkerrechtlichen Vertrag im Bereich des Datenschutzes verabschiedet: das Übereinkommen vom 28. Januar 1981²⁸ zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (im Folgenden «Übereinkommen SEV 108»), das von der Schweiz am 2. Oktober 1997 ratifiziert wurde. Dieses Übereinkommen wurde durch das Zusatzprotokoll vom 8. November 2001²⁹ zum Übereinkommen SEV 108 bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung (SEV 181, im Folgenden «Zusatzprotokoll») ergänzt, das die Schweiz am 20. Dezember 2007 ratifiziert hat. Das Übereinkommen 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 zur Revision des Übereinkommens SEV 108 erarbeitet (im Folgenden «E-SEV 108»). Die Arbeiten des vom Ministerkomitee eingesetzten Ad-hoc-Komitees wurden im Juni 2016 abgeschlossen. Das Änderungsprotokoll zum Übereinkommen SEV 108 wird vom Ministerkomitee voraussichtlich Anfang 2017 verabschiedet (vgl. Ziff. 3.2). Der vorliegende Bericht beruht auf dem Entwurf zur Revision des Übereinkommens (Stand September 2016)³⁰, der voraussichtlich keine substantziellen Änderungen mehr erfahren wird.

²⁸ SR 0.235.1

²⁹ SR 0.235.11

³⁰ Die französische Fassung kann unter folgender Adresse eingesehen werden: <http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Version%20consolidée%20convention%20108%20mode%20mise%20à%20jour%202016.pdf>. Eine Übersetzung auf Deutsch und Italienisch ist Bestandteil des Vernehmlassungsdossiers.

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.

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 Resolution³¹ 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.³² 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.

Am 8. März 2016 legte der Sonderberichterstatter seinen ersten Bericht vor. Der Sonderberichterstatter erachtet das Fehlen einer universell verbindlichen Definition von «Privatsphäre» als eines der Haupthindernisse für deren umfassenden rechtlichen Schutz. Der Bericht hält ferner im hier interessierenden Kontext u.a. fest, dass gerade das Risiko für die Verletzung des Rechts auf Privatsphäre durch die missbräuchliche Verwendung von Personendaten durch private Unternehmen nicht abschliessend geklärt sei.³³ Insgesamt habe sich die Befürchtung, dass Personendaten missbräuchlich verwendet werden, von den Staaten hin zu Unternehmen verschoben.³⁴ Der Sonderberichterstatter erachtet daher einen internationalen Dialog über das Sammeln von bzw. den Umgang mit Personendaten durch Unternehmen sowie deren Weitergabe an staatliche Stellen als notwendig. Im Rahmen des Projektes « Corporate online business models and personal data use » plant er hierfür die breite Konsultation von Unternehmen und der Zivilgesellschaft bis im Jahr 2017.³⁵

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.³⁶ Er spricht sich gegen Entwicklungen auf nationaler Ebene aus, die Unternehmen gesetzlich verpflichten, «Schlupflöcher» in ihre Produkte zu integrieren, um so einen späteren Zugang zu verschlüsselten Daten zu ermöglichen.³⁷ 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 identifizieren³⁸.

³¹ Resolution 68/167 vom 18. Dezember 2013, unter dem folgenden Link auf Französisch verfügbar: http://www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167.

³² UNHCHR «Das Recht auf Privatheit im digitalen Zeitalter», 2014.

³³ HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9.

³⁴ HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9.

³⁵ HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9 und Ziff. 46(f).

³⁶ HRC, Special Rapporteur Right to Privacy 2016, Ziff. 50.

³⁷ HRC, Special Rapporteur Right to Privacy 2016, Ziff. 30 f.

³⁸ HRC, Special Rapporteur Right to Privacy 2016, Ziff. 15 und Ziff. 46(e).

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-Richtlinien³⁹ 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)⁴⁰. Die revidierten Datenschutz-Richtlinien traten im Juli 2013 in Kraft und enthalten, unter Beibehaltung dieser acht datenschutzrechtlichen Grundprinzipien, verschiedene Präzisierungen und Erweiterungen; so wurden u.a. die Kriterien für Datenübermittlungen ins Ausland präziser definiert und die internationale Zusammenarbeit verstärkt⁴¹. 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 Daten⁴². 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 Revision

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 Vorlage zu den Zielen des Bundesrates für das Jahr 2016 und ist Teil der Legislaturplanung 2015–2019 (Ziff. 10.1). Sie setzt eine grosse Zahl der parlamentarischen Vorstösse um, die unter Ziffer 1.1.5 aufgeführt sind.

Mit dem VE 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

³⁹ OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten, 1980, online abrufbar unter: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>; OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten, 2013, online abrufbar unter: <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>.

⁴⁰ OECD, Datenschutz-Richtlinien 1980, Grundsätze 6-14; OECD, Privacy Framework 2013, S. 22 und S. 47 f.

⁴¹ OECD, Datenschutz-Richtlinien 2013, Grundsätze 16-18, 19 lit. g und 20-23.

⁴² OECD, Datenschutz-Richtlinien 2013, Grundsatz 16.

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 kann. 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 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 den vorliegenden erläuternden Bericht zu integrieren. So soll vermieden werden, dass zu einem späteren Zeitpunkt eine zweite Vernehmlassung stattfinden muss.

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 angemessenen 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 revidierten Datenschutzgesetzes

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 potentiellen 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. Unternehmen, 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 VE-DSG alle Technologien gleichberechtigt behandeln. Dadurch bleibt das Gesetz offen für weitere technologische Entwicklungen und verhindert keine Innovationen. Weil sie dem technologieneutralen Charakter des Erlasses widerspricht, wird beispielsweise die Anforderung der formellen gesetzlichen Grundlage für die «Abrufverfahren» im öffentlichen Sektor aufgegeben.

Die dritte Leitlinie besteht in der Modernisierung der Terminologie, insbesondere um die Vereinbarkeit mit dem europäischen Recht 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» wird um «genetische und biometrische Daten, die eine Person eindeutig identifizieren», erweitert.

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 gewährleistet ist, bleibt unverändert. Hingegen entscheidet nun der Bundesrat und nicht mehr der Verantwortliche, ob die Gesetzgebung eines Drittlandes diese Anforderung erfüllt. Fehlt es an einer solchen Gesetzgebung, sieht der VE-DSG verschiedene Möglichkeiten vor, mit denen ein geeigneter Schutz gewährleistet werden kann, so dass 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 ihnen 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 Vorentwurf umfassender ausgestaltet. Die Verantwortlichen werden auch dazu verpflichtet, bei gewissen Arten von Bearbeitungen eine Datenschutz-Folgenabschätzung durchzuführen. Technische Vorkehrungen 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 seine Kolleginnen und Kollegen im europäischen Ausland wird er jedoch nicht befugt sein, Verwaltungssanktionen auszusprechen. Dies wird ausgeglichen, indem andererseits der strafrechtliche Teil des VE-DSG erheblich ausgebaut wird.

1.4.2 Hauptsächliche Neuerungen

1.4.2.1 Änderung des Geltungsbereichs des künftigen DSG

Mit dem VE-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 in ausländische Staaten, in deren Gesetzgebung kein Schutz der Daten juristischer Personen vorgesehen ist, erleichtert werden.

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 (z. B. Entscheidungen, die ausschliesslich auf Algorithmen beruhen und ohne menschliches Eingreifen getroffen werden) ein sowie das Recht der betroffenen Person, in diesem Fall ihren Standpunkt geltend zu machen. Gemäss dem VE müssen der betroffenen 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 VE-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.

1.4.2.3 Förderung der Selbstregulierung

Die Revision soll die Entwicklung der Selbstregulierung und die Eigenverantwortung der Verantwortlichen fördern. Um deren Aufgaben zu erleichtern und eine bessere Einhaltung des Gesetzes sicherzustellen, hat der Beauftragte unter anderem die Aufgabe, Empfehlungen der guten Praxis zu erarbeiten. Dabei handelt es sich nicht um eine völlig neue Kompetenz, denn der Beauftragte veröffentlicht auf seiner Website bereits allgemeine Empfehlungen. Diese Aufgabe soll in Zukunft ausgebaut werden. Der Beauftragte muss für die Erarbeitung der Empfehlungen die interessierten Kreise einbeziehen. Diese können auch ihre eigenen Empfehlungen erarbeiten und sie vom Beauftragten genehmigen lassen.

Mit den Empfehlungen der guten Praxis können in Bereichen, in denen gegenwärtig zahlreiche Fragen aufgeworfen werden, genauere Regeln festgelegt werden. Ausserdem lassen sich bestimmte Begriffe sowie die Modalitäten einiger Rechte und Pflichten präzisieren, und die Eigenverantwortung des Verantwortlichen kann gefördert werden.

Die Empfehlungen der guten Praxis haben keinen bindenden Charakter. Hält ein Verantwortlicher sie jedoch ein, befolgt er damit diejenigen Gesetzesbestimmungen, die durch die Empfehlungen konkretisiert werden.

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

Die Stellung und die Unabhängigkeit des Beauftragten werden gestärkt. Die oder der Beauftragte kann zwei Mal wiedergewählt werden, und darf nur unter ganz bestimmten Bedingungen einer Nebenbeschäftigung nachgehen. Im Weiteren sieht der VE-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 seinen Kolleginnen und Kollegen im europäischen Ausland nicht befugt ist, Verwaltungssanktionen zu verhängen. Der Höchstbetrag der Bussen wird auf 500 000 Franken erhöht; die Liste der strafbaren Verhaltensweisen wird an die neuen Pflichten der Verantwortlichen und der Auftragsbearbeiter angepasst; es wird ein mit Freiheitsstrafe bedrohter Straftatbestand bei Verletzungen der beruflichen Schweigepflicht eingeführt und die Verfolgungsverjährungsfrist bei Übertretungen verlängert. Bei Übertretungen, die in einem Unternehmen begangen werden, können die

Strafverfolgungsbehörden – im vorliegenden Fall die Kantone – unter bestimmten Voraussetzungen darauf verzichten, die Verantwortlichen strafrechtlich zu belangen. Stattdessen wird das Unternehmen zur Bezahlung der Busse verurteilt.

1.5 Darstellung der Revision anderer Bundesgesetze

In den bereichsspezifischen Datenschutznormen für die polizeiliche und justizielle Zusammenarbeit im Rahmen der Schengen-Abkommen wird 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 VE 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.

Da die öffentlichen Register des Privatrechtsverkehrs nicht mehr vom Anwendungsbereich des DSG ausgenommen sind, muss auch die Bundesgesetzgebung zum Zivilstandswesen angepasst werden, insbesondere in Bezug auf die Aufsicht über die Einhaltung der Datenschutzerfordernisse und die Rechte der betroffenen Personen.

1.6 Weitere geprüfte Massnahmen

Im Rahmen der Revisionsarbeiten hat der Bundesrat weitere Massnahmen geprüft, aber schliesslich beschlossen, diese nicht in den VE aufzunehmen. Dabei handelt es sich namentlich um die folgenden Massnahmen.

1.6.1 Erlass verbindlicher Datenschutzvorschriften durch den Beauftragten

Die Möglichkeit, dem Beauftragten den Erlass verbindlicher Datenschutzvorschriften zu erlauben, wurde fallen gelassen. Diese Lösung hätte zwar den Vorteil, dass der Beauftragte seine Adressaten direkt verpflichten könnte. Doch sie würde zu zahlreichen Problemen im Zusammenhang mit dem Legalitätsprinzip führen (Delegation von Kompetenzen an den Beauftragten, Regelungsdichte). Im Vergleich mit der nun gewählten Lösung der Empfehlungen der guten Praxis, wäre auch das Verfahren zum Erlass solcher Normen langsamer, da jeweils das Verfahren zum Erlass von Verordnungen der Bundesverwaltung durchlaufen werden müsste. Im Übrigen würde diese Möglichkeit den betroffenen Kreisen nur einen geringen Spielraum lassen, was sich negativ auf die Einhaltung der fraglichen Vorschriften auswirken könnte.

1.6.2 Beweislastumkehr

Auf eine Beweislastumkehr nach dem Beispiel von Artikel 13a des Bundesgesetzes vom 19. Dezember 1986 über den unlauteren Wettbewerb (UWG)⁴³, wonach das Gericht von den Datenbearbeitenden im Einzelfall den Nachweis einer datenschutzkonformen Bearbeitung verlangen könnte, wenn dies unter Berücksichtigung der berechtigten Interessen der am Verfahren beteiligten Parteien angemessen erscheint, hat der Bundesrat verzichtet. 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 gezeigt, dass Vorschläge zur Beweislastumkehr auf starken Widerstand stossen.

1.6.3 Kollektive Rechtsdurchsetzung

In der Revision des DSG soll keine auf das Datenschutzrecht beschränkte Regelung der kollektiven Rechtsdurchsetzung (Erweiterung des Verbandsklagerechts und Einführung einer

⁴³ SR 214

Sammelklage bzw. eines Sammelvergleichs) eingeführt werden. Stattdessen werden die Instrumente der kollektiven Rechtsdurchsetzung im Rahmen der Umsetzung der Motion 13.3931 Birrer-Heimo in einem grösseren, möglichst sektorübergreifenden Kontext geprüft.

1.6.4 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 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.

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

Es wurde in Betracht gezogen, nicht den Beauftragten, sondern eine ausserparlamentarische Kommission mit der Erarbeitung und Genehmigung von Empfehlungen der guten Praxis zu beauftragen. Die Lösung mit dem Beauftragten hat jedoch den Vorteil, dass kein zusätzlicher Verwaltungsaufwand entsteht und keine weiteren Kosten verursacht werden. Auch kann rasch gehandelt werden.

1.6.6 Änderung der Organisation der Aufsichtsbehörde

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

1.6.7 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 der Beauftragten oder dem Beauftragten angegliederten Organs hohe Kosten verursachen, was im Widerspruch zur derzeitigen Budgetpolitik des Bundesrates stehen würde.

1.7 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 2002⁴⁴ über die Bundesversammlung (ParIG) festgelegt.

Das BJ und das Staatssekretariat für Wirtschaft (SECO) haben das Unternehmen PwC mit der Durchführung einer RFA⁴⁵ beauftragt. Diese kann als Grundlage zur Beurteilung der Auswirkungen der Revision dienen. Die Regulierungsfolgenabschätzung beruht im Wesentlichen auf den Ergebnissen einer Online-Unternehmensbefragung sowie auf Gesprächen mit Datenschutzfachleuten. In der RFA wird die Revisionsvorlage insgesamt sehr positiv aufgenommen.

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

1.7.1 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 neue Ängste aus und haben zu neuen Datenschutzrisiken geführt. Der VE ist hauptsächlich darauf ausgerichtet, die Kontrolle und Verfügungsfähigkeit über Daten zu verbessern sowie die Transparenz von Datenbearbeitungen zu erhöhen. 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, die Richtlinie (EU) 2016/680; zu berücksichtigen ist aber auch die Verordnung (EU) 2016/679.

1.7.2 Auswirkungen auf die einzelnen gesellschaftlichen Gruppen

Von den im VE vorgesehenen Änderungen sind alle in der Schweiz tätigen Unternehmen betroffen. Für die RFA wurden die Unternehmen, unter Berücksichtigung ihrer Branche und Grösse, entsprechend ihrer «datenschutzrechtlichen Exponierung» segmentiert. Es wurden die folgenden Segmente gebildet:

- 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 zeigen, dass die Unternehmen des Segments A von den im VE vorgesehenen Massnahmen generell nur geringfügig betroffen sind. Die Auswirkungen der Revision auf dieses Segment sind somit verhältnismässig gering. Im Rahmen der Gespräche haben einige Expertinnen und Experten jedoch geltend gemacht, die Unternehmen des Segments A seien von den im VE vorgesehenen Massnahmen stärker betroffen als Grossunternehmen, da sie in vielen Fällen nicht über eine spezielle Abteilung für die Anpassungsmassnahmen verfügten. Dies müssten sie mit entsprechenden Massnahmen ausgleichen, was für diese Unternehmen mit zusätzlichen Kosten verbunden sei. Die Unternehmen der Segmente B und C dagegen sind aufgrund ihrer Aktivitäten, ihrer Grösse und ihrer Öffnung gegenüber dem Ausland stärker betroffen.⁴⁶

⁴⁴ SR 171.10

⁴⁵ Die RFA ist auf der Website des Bundeamts für Justiz abrufbar: <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html>.

⁴⁶ Für eine detaillierte Übersicht über die Auswirkungen der einzelnen Massnahmen siehe die Übersichtstabelle auf den Seiten 50 ff. des Berichts.

1.7.3 Auswirkungen auf die Gesamtwirtschaft

Die Auswirkungen der Revision 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 zunächst festzuhalten, dass sich aus der Revision grundsätzlich keine Pflichten der betroffenen Personen ergeben. Deren Stellung soll vielmehr gestärkt werden. 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 Rechte der betroffenen Personen sowie ein Recht auf Datenportabilität (vgl. Ziff. 1.6.4). 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.

1.7.4 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 (vgl. Ziff. 1.6.5).

1.7.5 Zweckmässigkeit im Vollzug

Zur Begrenzung der mit der Revision 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 der Website oder in den 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, sollte der VE klar definierte Begriffe (Legaldefinitionen) verwenden und die Umstände klar bestimmen, aus denen eine Pflicht resultiert. So müsse beispielsweise angegeben werden, in welchen Fällen eine Folgenabschätzung der Datenbearbeitung vorzunehmen ist. Zur Sensibilisierung für die Probleme im Zusammenhang mit dem Datenschutz und Erleichterung der Umsetzung des Gesetzes sei eine zielgerichtete Kommunikation (beispielsweise mit Hinweisen, Broschüren, Leitfäden) und die Entwicklung von Empfehlungen der «guten Praxis» erforderlich. Diese Massnahmen könnten insbesondere für Unternehmen mit geringer datenschutzrechtlicher

Exponierung nützlich sein. Die Idee einer unabhängigen Expertenkommission wird 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, die Schweiz und Liechtenstein im Rahmen ihrer Mitwirkungsrechte) fanden in den Jahren 2012 bis 2015 unter dem Vorsitz der Europäischen Union 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 unten) 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.

Das 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). Artikel 30 und 31 verpflichten die Verantwortlichen, in gewissen Fällen der Aufsichtsbehörde eine Verletzung des Datenschutzes 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.

Das Kapitel VI verpflichtet die Schengen-Staaten, im Bereich des Datenschutzes unabhängige Aufsichtsbehörden einzusetzen. Die Artikel 45, 46 und 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 Auftragsverarbeiters, 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.

Das 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 die Schweiz über 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-Assoziierungsabkommens).

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 hat ihre Antwortnote daher erst am 1. September 2016 überreicht.

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 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 VE-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 VE-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 Bereiche, die in denen das DSG gilt. 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. 8.3).

Die Konkordanztabelle im Anhang des erläuternden Berichts enthält die jeweils übereinstimmenden Artikel des VE-DSG, E-SEV 108 und der Richtlinie (EU) 2016/680.

2.4 Hauptsächliche notwendige Gesetzesänderungen

Zusätzlich zu den erforderlichen Änderungen des DSG müssen die folgenden Bundesgesetze angepasst werden: das Schweizerische Strafgesetzbuch vom 21. Dezember 1937⁴⁷ (StGB), die Strafprozessordnung vom 5. Oktober 2007⁴⁸ (StPO), das Bundesgesetz vom 20. März 1981⁴⁹ über internationale Rechtshilfe in Strafsachen (IRSG), das Bundesgesetz vom 3. Oktober 1975⁵⁰ zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen, das Schengen- Informationsaustausch-Gesetz vom 12. Juni 2009⁵¹ (SIaG) und das Bundesgesetz vom 7. Oktober 1994⁵² über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten (ZentG). Die Bestimmungen der Richtlinie (EU) 2016/680, die in den VE-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 Entwurf zur Revision des Übereinkommens SEV 108 (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 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. 8^{bis} 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

⁴⁷ SR 311.0

⁴⁸ SR 312

⁴⁹ SR 351.1

⁵⁰ SR 351.93

⁵¹ SR 362.2

⁵² SR 360

automatisierten Verarbeitung ihrer Daten ergeht, ohne dass die betroffene Person ihre Standpunkt geltend machen kann (Art. 8 Bst. a). Auch das Auskunftsrecht der betroffenen Person muss ausgebaut werden. Die geltenden Bedingungen für die Einwilligung der betroffenen Person müssen ebenfalls 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 der Betroffene 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. 12^{bis}) 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. 49 Staaten haben das gegenwärtige Übereinkommen ratifiziert, davon zwei Länder, die dem Europarat nicht angehören (Uruguay, Mauritius). Ausserdem sind mehrere Staaten, die Mitglied des Europarates sind, im Begriff, das Übereinkommen zu ratifizieren (Marokko, Tunesien, Senegal). 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 Unterzeichnung des Entwurfs für die Änderung des Übereinkommens 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.⁵³ Schliesslich ist darauf hinzuweisen, dass die

⁵³ 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»).

im E-SEV 108 vorgesehenen Massnahmen mit den Zielen übereinstimmen, die der Bundesrat in seinem Beschluss vom 9. Dezember 2011⁵⁴ aufgrund der Evaluation des Datenschutzgesetzes festgehalten hat.

Was das Verfahren für die Ratifizierung des künftigen Übereinkommen SEV 108 betrifft, ist gemäss Artikel 4 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 VE-DSG stimmt weitgehend mit den Anforderungen des Änderungsprotokolls überein, so dass zum gegebenen Zeitpunkt eine Ratifizierung möglich ist, ohne dass die Schweizer Gesetzgebung weiterer Anpassungen bedürfte.

3.3 Hauptsächliche notwendige Gesetzesänderungen

Die Bestimmungen E-SEV 108 sind nicht direkt anwendbar. Um das Änderungsprotokoll dieses Erlasses ratifizieren zu können, muss die Schweiz bestimmte bundesrechtliche Bestimmungen anpassen. Die Bestimmungen E-SEV 108, die in den VE-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, so dass 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 bis 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 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

⁵⁴ BBI 2012 255

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 bis 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 Datenschutzgesetzes 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. Dies bedeutet jedoch nicht, dass sie keine Auswirkungen in den Bereichen haben, in denen die Schweiz als Drittstaat betrachtet wird. 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 Kommission⁵⁵ ein angemessenes Datenschutzniveau. Dieser Beschluss kann jedoch jederzeit widerrufen werden. Wenn die Schweiz erneut einen Angemessenheitsbeschluss der Europäischen Union erhalten 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 sind künftig massgebend für die Beurteilung, ob die schweizerische Gesetzgebung einen angemessenen Datenschutz gewährleistet. Der VE sollte ein angemessenes Schutzniveau im Sinn der Verordnung garantieren.

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

Wie die nachfolgenden Beispiele zeigen, haben nicht nur europäische Staaten Datenschutzgesetze verabschiedet.⁵⁶

5.1 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.⁵⁷ Sie hat eine Unterstützungs-, Beratungs- und Aufsichtsfunktion. Gemäss Artikel 29 des Dekrets 1558/2001⁵⁸ kann sie auch Verwaltungs- und Verfahrensvorschriften zum Register der Personendatenbanken (im Folgenden «Register») 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, Verhaltenskodexe 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 und/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 fünfzügigen Frist oder bei einer abschlägigen Antwort kann die interessierte Person eine Beschwerde einreichen.

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

⁵⁵ ABI. L 215 vom 25.8.2000, S. 1.

⁵⁶ Die Angaben beruhen auf einem Rechtsgutachten des Schweizerischen Instituts für Rechtsvergleichung vom 3. August 2016.

⁵⁷ 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: http://www.jus.gob.ar/media/33481/ley_25326.pdf.

⁵⁸ Decreto 1558/2001, Protección de los datos personales, verfügbar unter: http://www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf.

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 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.

5.2 Neuseeland

In Neuseeland wird der Datenschutz hauptsächlich durch den «Privacy Act 1993»⁵⁹ geregelt. Dieses Gesetz wird gegenwärtig revidiert. Der Entwurf zu einem neuen «Privacy Act» wird voraussichtlich noch vor Ende 2016 in die Vernehmlassung gegeben und 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 Commissioner» (im Folgenden «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 Zulässigkeitsklärungen 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»⁶⁰ 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. Diese sind künftig verpflichtet, dem PC bestimmte Datenschutzverstösse zu melden. Ausserdem verlangt eine neue IPP von den «Agencies», angemessene Massnahmen zu treffen, damit beim Austausch von Daten mit ausländischen Staaten ein annehmbarer Datenschutz gewährleistet ist.

⁵⁹ Der «Privacy Act 1993» ist unter folgender Adresse verfügbar:
<http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html>.

⁶⁰ Als «Agency» gelten praktisch alle Personen und Organisationen, die über Personendaten verfügen.

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.

5.3 Südkorea

Südkorea verfügt seit 2011 über eine Gesetzgebung im Bereich des Datenschutzes. Dabei handelt es sich um den sogenannten «Personal Information Protection Act»⁶¹ (im Folgenden «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 Verbreitung, die Fälschung oder die Vernichtung von Daten zu verhindern. Die Informationen müssen so bearbeitet werden, dass die Risiken einer Verletzung der Privatsphäre auf das mögliche 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.

⁶¹ Die entsprechenden Gesetzesbestimmungen sind auf Englisch unter folgender Adresse verfügbar: <http://www.law.goper.kr/eng/engMain.do>.

5.4 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»)⁶² 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 Verwirklichung 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).

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 zu 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.

5.5 Singapur

Die zuständige Aufsichtsbehörde ist die «Personal Data Protection Commission» (im Folgenden «PDPC»). Diese wurde 2013 geschaffen, um den 2012 in Kraft getretenen Personal Data Protection Act (PDPA)⁶³ umzusetzen. Die PDPC übt unter anderem eine

⁶² Der APPI ist auf Englisch unter folgender Adresse verfügbar: <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>.

⁶³ 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>.

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).

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 Singapurische 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 dies jedoch gestützt auf ihre gesetzlich verankerte Befugnis, Massnahmen zur Sensibilisierung für den Datenschutz zu ergreifen (Art. 6 PDPA), tun.

6 Umsetzung

Im Rahmen der Regulierungsfolgenabschätzung wurde angetönt, unbestimmte Rechtsbegriffe seien nach Möglichkeit zu vermeiden. Beim Datenschutzgesetz handelt es sich indes um eine technologieneutrale Rahmengesetzgebung, welche auf eine Vielzahl unterschiedlich gelagerter Fälle anwendbar bleiben und sich dynamisch weiterentwickeln können muss. Dem Bedürfnis nach exakteren, bereichsspezifischen Ausführungsbestimmungen dienen jedoch die Empfehlungen der guten Praxis.

Im Weiteren wird die Verordnung zum Datenschutzgesetz angepasst, um das Gesetz nicht mit Detailregelungen zu überlasten.

Im VE ist zwar nicht ausdrücklich eine Überprüfung seiner Umsetzung vorgesehen, doch die Wirksamkeit seiner 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 Annahme des Änderungsprotokolls zum Übereinkommen SEV 108 durch unser Land ist auch für die Kantone bindend. Diese müssen ihre kantonalen Gesetzgebungen insoweit anpassen, als sie die Anforderungen dieser Instrumente nicht erfüllen.

7 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 Vergessen, ob im Internet oder anderweitig, besteht im DSG bereits. Durch die ausdrückliche Erwähnung des Rechts auf Löschung im VE-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 Empfehlungen der guten Praxis erarbeitet werden.
- 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 VE-DSG enthält Massnahmen zum verbesserten Schutz der Persönlichkeitsrechte.
- Postulate FDP-Liberale Fraktion 14.4137 und Comte 14.4284 «Videoaufnahmen durch Private. Die Privatsphäre besser schützen». Gemäss dem VE-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.
- Motion Comte 14.3288 «Identitätsmissbrauch. Eine strafbare Handlung für sich». Mit der Einführung von Artikel 179^{decies} im StGB wurde diese Motion umgesetzt.
- Postulat Béglé 16.3383 «Elektronische Daten: Information der Geschädigten im Falle eines Hackerangriffs». Nach Art. 17 VE-DSG muss eine unbefugte Datenbearbeitung dem Beauftragten und unter bestimmten Umständen auch der betroffenen Person gemeldet werden. Der Inhalt 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, soweit nicht ein Spezialgesetz etwas anderes vorsieht. Der VE-DSG sieht verschiedene Pflichten des Verantwortlichen und des Auftragsbearbeiters vor, die auch für medizinische Daten gelten (Art. 13, 15, 16, 17, 18 und 19) und den Forderungen des Postulats entsprechen. Weitere Massnahmen wie beispielsweise die Präzisierung der Anforderungen für die Einwilligung (Art. 4 Abs. 6) sowie die Erarbeitung von Empfehlungen der guten Praxis, sollten auch im Bereich der medizinischen Daten zu einem verbesserten Schutz führen.

Die folgenden parlamentarischen Vorstösse werden teilweise abgeschrieben:

- Postulat Derder 14.3655 «Die digitale Identität definieren und Lösungen für ihren Schutz finden». Der Bundesrat hat die Möglichkeit, die digitale Identität im Rahmen der Revision 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 bei den Arbeiten der Expertenkommission «Zukunft der Datenbearbeitung und Datensicherheit» oder im Rahmen der Strategie «Digitale Schweiz» 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 VE-DSG insofern teilweise erfüllt, als die betroffenen Personen durch seinen Inhalt künftig besser geschützt werden. Der Gegenstand des Postulats reicht über den Rahmen der Revisionsarbeiten hinaus. Es geht dabei im Wesentlichen um Aspekte im Zusammenhang mit der Produktsicherheit und der Sicherheit des Internets. Deshalb schlägt der Bundesrat vor, das Postulat im Rahmen der Arbeiten der Expertenkommission «Zukunft der Datenbearbeitung und Datensicherheit» zu erfüllen.
- Postulat Schwaab 14.3782 «Richtlinien für den <digitalen Tod>»: Artikel 12 VE-DSG sieht einerseits ein Einsichtsrecht in Daten einer verstorbenen Person vor, andererseits erlaubt er den Erben, die Löschung von Daten des Erblassers zu verlangen. Damit werden wesentliche Forderungen des Postulats umgesetzt. Weitere Elemente sind im Rahmen der Revision des Erbrechts zu verwirklichen.
- 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. 1.6.4).
- Postulat Béglé 16.3386 «Kontrolle über persönliche Daten. <Informationelle Selbstbestimmung> fördern». Aus denselben Gründen wie beim Recht auf Datenportabilität (vgl. 1.6.4) sieht der VE-DSG auch keine Präzisierung der Wiedererlangung der Kontrolle über persönliche Daten vor. Die Frage wird in der Expertenkommission «Zukunft der Datenbearbeitung und Datensicherheit» oder im Rahmen der Strategie «Digitale Schweiz» geprüft.

8 Gesetzesänderungen

8.1 Erläuterung des VE-DSG

8.1.1 Zweck, Geltungsbereich und Begriffe

8.1.1.1 Art. 1 Zweck

Der Zweck des künftigen DSG entspricht dem Zweck des geltenden Rechts (Art. 1 DSG). Das DSG konkretisiert auf Gesetzesesebene 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.⁶⁴

Die Bestimmung wird lediglich redaktionell geändert, indem ausdrücklich der Schutz auf natürliche Personen beschränkt wird. Diese Anpassung erfolgt aufgrund des geänderten Geltungsbereichs (vgl. Ziff. 8.1.1.2).

8.1.1.2 Art. 2 Geltungsbereich

Der Anwendungsbereich des Datenschutzgesetzes wird durch den Vorentwurf teilweise erweitert, dies insbesondere, um den Anforderungen 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) anzupassen und diejenige betreffend öffentliche Register des Privatrechtsverkehrs (Art. 2 Abs. 2 Bst. d DSG) aufzuheben.

Zudem ist darauf hinzuweisen, dass der VE-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.⁶⁵

Absatz 1 Anwendung für natürliche Personen

Das Datenschutzgesetz 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 VE-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)⁶⁶ (Persönlichkeitsverletzungen wie beispielsweise Rufschädigung), das UWG, das Bundesgesetz vom 9. Oktober 1992⁶⁷ über das Urheberrecht und verwandte Schutzrechte (URG) oder durch die Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen sowie Art. 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.⁶⁸ Diese Lösung hat auch den Vorteil, dass die Bekanntgabe von Daten juristischer Personen ins Ausland nicht mehr davon abhängt, ob im Empfängerland ein angemessener Schutz gewährleistet ist (Art. 5 VE-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 Regulierungsfolgenabschätzung zur Revision des Datenschutzgesetzes befragt wurden, den Verzicht auf den Schutz von Daten juristischer Personen befürworteten.⁶⁹ Der Nationalrat hat einer Motion, welche den Schutz von Daten juristischer Personen beibehalten wollte, nicht zugestimmt (vgl. Ziff. 1.1.5 Motion Béglé 16.3379).

Das Bundesgesetz vom 17. Dezember 2004⁷⁰ über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) räumt allen Personen das Recht ein, amtliche Dokumente der Bundesbehörden

⁶⁴ BGE 140 I 2 E. 9.1

⁶⁵ Vgl. hierzu BBI 1988 413, 444 und MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, N 286 ff.

⁶⁶ SR 210

⁶⁷ SR 231.1

⁶⁸ Zu dieser Frage siehe DECHSLER CHRISTIAN, Plädoyer für die Abschaffung des Datenschutzes für juristische Personen, AJP 2016, S. 80 ff., S. 85–86.

⁶⁹ Vgl. S. 46 der RFA.

⁷⁰ SR 152.3

einzusehen, für die das Öffentlichkeitsprinzip gilt. Der neue Geltungsbereich des VE-DSG hat zur Folge, dass der Zugang zu amtlichen Dokumenten, die Informationen über juristische 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 das Risiko besteht, dass die Privatsphäre der juristischen Person beeinträchtigt wird, beispielsweise deren guter Ruf. Artikel 9 BGÖ gilt nicht mehr für Dokumente, die Daten einer juristischen Person enthalten. 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 verletzen könnte, werden im Vorentwurf einige Bestimmungen des BGÖ angepasst (vgl. Ziff. 8.2.5).

Die Aufhebung des Schutzes von Daten juristischer Personen bewirkt ebenfalls, dass diese aufgrund des VE-DSG kein Einsichtsrecht mehr geltend machen können, aber gegebenenfalls aufgrund des Öffentlichkeitsgesetzes Einsicht in öffentliche Dokumente verlangen können, wenn diese Informationen enthalten können, die sie betreffen.

Absatz 2 Ausnahmen vom Geltungsbereich

Das Datenschutzgesetz ist wie bisher nicht anwendbar auf Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden (Art. 2 Abs. 2 Bst. a VE-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 VE-DSG), dies aus denselben Gründen wie sie der Bundesrat bereits in der Botschaft vom 23. März 1988⁷¹ angeführt hat. Schliesslich übernimmt Buchstabe d dieser Bestimmung die Ausnahme betreffend das Internationale Komitee vom Roten Kreuz, wobei im VE-DSG nunmehr präzisiert wird, dass die Ausnahme für alle institutionellen Begünstigten nach Artikel 2 Absatz 2 des Gaststaatgesetzes vom 22. Juni 2007⁷², die in der Schweiz Immunität geniessen, gilt. Anzumerken ist, dass das IKRK auch vom Anwendungsbereich des Datenschutzgesetzes ausgeschlossen ist, weil es einer Internationalen Organisation angehört.

Buchstabe c Ausnahmen für eidgenössische Justizbehörden

Nach Absatz 2 Buchstabe c ist die Bearbeitung von Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit erfolgt, ebenfalls vom Anwendungsbereich ausgenommen.

Die Ausnahme erfolgt zum einen, weil die Unterstellung dieser Behörden unter die Aufsicht des Beauftragten die Gewaltenteilung und die Unabhängigkeit der Justiz beeinträchtigen würde. Zum anderen rechtfertigt sie sich dadurch, dass die Rechte der Parteien und Verfahrensbeteiligten in diesem Fall alleine vom Prozessrecht beherrscht sind (z.B. über das Recht auf Akteneinsicht), das ihnen einen zum Datenschutzgesetz gleichwertigen Schutz bietet. Dies gilt insbesondere auch für die Rechte der Parteien zur Kenntnisnahme der ins Verfahren einflussenden Daten und zur allfälligen Berichtigung bestimmter Daten sowie für die Datenbearbeitung im Rahmen der gerichtlichen Verfahren im Allgemeinen. So regelt das Prozessrecht nicht nur den Ablauf der Verfahren, sondern auch den Persönlichkeitsschutz der Parteien, die Daten ins Verfahren einbringen. Das Prozessrecht wirkt darüber hinaus auf bereits abgeschlossene Verfahren. Die Akten eines bereits abgeschlossenen Verfahrens können lediglich nach den Vorschriften des Prozessrechts abgeändert werden (Berichtigung, Erläuterung, Revision), da die Akten mit dem Ergebnis eines Verfahrens übereinstimmen müssen. Damit die Aktenlage nicht nachträglich durch prozessfremde Instrumente verändert werden kann, sieht das Prozessrecht eigenständige Verfahren zur Aktenpflege vor. Zusammenfassend bildet das wesentliche Abgrenzungskriterium für die Anwendbarkeit des Datenschutzgesetzes, insbesondere bei abgeschlossenen Verfahren, ob aus prozessrechtlicher Perspektive ein unmittelbarer individueller Bezug zu einem Verfahren vorliegt. Im Umkehrschluss ergibt sich daraus, dass das Datenschutzgesetz anwendbar ist

⁷¹ BBl 1988 II 413, 441

⁷² SR 192.12

auf Datenbearbeitungen durch die administrativen Dienste dieser Behörden, wie beispielsweise die Bearbeitung von Daten über das Personal.⁷³ In diesem Bereich unterstehen die Behörden der Aufsicht des Beauftragten (vgl. aber Absatz 3).

Anders als im bisherigen Recht schlägt der Bundesrat vor, den Begriff der «Rechtsprechungstätigkeit» zu verwenden und nicht mehr von hängigen Verfahren zu sprechen. Denn der Begriff des «hängigen Verfahrens» wird nicht allen Arten von Verfahren gerecht. Namentlich gibt es den Begriff der «Rechtshängigkeit» lediglich im Zivilprozessrecht.

Unter den Begriff der «unabhängigen eidgenössischen Justizbehörden» fallen beispielsweise die Bundesanwaltschaft, die Militärjustiz oder die unabhängigen Beschwerdeinstanzen nach Artikel 47 des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968 (VwVG)⁷⁴. Hingegen fallen kantonale Behörden nicht unter diese Ausnahme, da Datenbearbeitungen durch kantonale Behörden durch das kantonale Datenschutzrecht geregelt werden, wenn das Bundesrecht nichts anderes vorsieht. Falls Personendaten durch eine Behörde bearbeitet werden, welche nicht als «unabhängige eidgenössische Justizbehörde» zu qualifizieren ist, gilt diese Ausnahme nicht. Im Bereich des Strafverfahrens fällt demnach die Bearbeitung von Daten durch die eigenössischen Polizeibehörden in den Anwendungsbereich des VE-DSG; die bereichsspezifischen Datenschutznormen bleiben jedoch vorbehalten. Dasselbe gilt für die Datenbearbeitung durch Bundesbehörden im Rahmen eines Verwaltungsstrafverfahrens. Schliesslich ist hervorzuheben, dass der neue Wortlaut der Ausnahme nach Buchstabe c keine Auswirkungen hat auf erstinstanzliche Verwaltungsverfahren. Diese fallen wie nach der derzeitigen Regelung weiterhin in den Anwendungsbereich des Datenschutzgesetzes.

Aufhebung der Ausnahme für öffentliche Register (Artikel 2 Absatz 2 Buchstabe d DSG)

Nach Auffassung des Bundesrates ist diese Ausnahme mit den Anforderungen von Artikel 3 E-SEV 108 nicht mehr vereinbar. Die Änderung betrifft ausschliesslich öffentliche Register des Privatrechtsverkehrs, die von Bundesbehörden geführt werden, d. h. Infostar, Zefix, das Luftfahrzeugbuch des Bundesamts für Zivilluftfahrt und das Markenregister des Eidgenössischen Instituts für Geistiges Eigentum. 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 nicht behindern. Die Aufhebung von Artikel 2 Absatz 2 Buchstabe c DSG hat daher auf die folgenden Register keine Auswirkungen:

- Das Grundbuch ist ein öffentliches Register, das in die Zuständigkeit der Kantone fällt. Gemäss den bundesrechtlichen Bestimmungen zum Grundbuchrecht (Art. 942 ff. ZGB, Art. 955 ZGB und Grundbuchverordnung vom 23. September 2011⁷⁵ [GBV]) müssen die Grundbuchämter der Kantone Grundbücher führen. Die Kantone sind für allen Schaden verantwortlich, der aus der Führung dieser Register entsteht (Art. 955 ZGB).
- Im Verkehrsbereich fällt die Führung des Schiffsregisters in die Zuständigkeit der Kantone (Art. 1 und 4 der Schiffsregisterverordnung vom 16. Juni 1986⁷⁶). Die GBV gilt für die Führung des Schiffsregisters, sofern die Bundesgesetzgebung zum Schiffsregister nichts anderes vorsieht.
- Gemäss Artikel 927 des Obligationenrechts (OR)⁷⁷ muss jeder Kanton ein Handelsregister führen, die Amtsstellen bestimmen, denen die Führung des Handelsregisters obliegt, und eine kantonale Behörde vorsehen, die mit der administrativen Aufsicht über das

⁷³ Vgl. bereits BBI 1988 II 443

⁷⁴ SR 172.0121

⁷⁵ SR 211.432.1

⁷⁶ SR 747.111

⁷⁷ SR 220

Handelsregisteramt betraut ist (Art. 3 und Art. 4 Abs. 1 der Handelsregisterverordnung vom 17. Oktober 2007⁷⁸).

- Für die Führung der Betreibungs- und Konkursregister sind die Kantone zuständig (Art. 8 Abs. 1 des Bundesgesetzes vom 11. April 1889⁷⁹ über Schuldbetreibung und Konkurs).
- Das öffentliche Register über die Eigentumsvorbehalte wird von den Betreibungsämtern geführt (Art. 715 ZGB).

Absatz 3 Eidgenössische Gerichte

Nach Artikel 2 Absatz 3 ist das Datenschutzgesetz nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Diese Ausnahme gilt aus denselben Gründen, wie jene für die unabhängigen eidgenössischen Justizbehörden (vgl. den Kommentar betreffend Art. 2 Abs. 2 Bst. c).

Soweit die Bearbeitung von Personendaten durch die eidgenössischen Gerichte unter das Datenschutzgesetz fällt, sind sie von der Aufsicht durch den Beauftragten ausgenommen (Art. 3 Abs. 3 Satz 2 VE-DSG). Die Ausnahme ist im Hinblick darauf zu betrachten, dass der Beauftragte im VE-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, werden die eidgenössischen Gerichte eine eigenständige Form der Datenschutzaufsicht in die Wege leiten. Deren Ausgestaltung liegt in deren Zuständigkeit und ist noch Gegenstand von Gesprächen.

Absatz 4 Aufsicht über den Bundesrat

Absatz 4 entspricht Artikel 27 Absatz 1 zweiter Satz DSG, wonach der Bundesrat von der Aufsicht durch den Beauftragten ausgenommen ist. Dieser Grundsatz bleibt unverändert.

Darüber hinaus ist auch die Bundesversammlung von der Aufsicht durch den Beauftragten ausgenommen.

Räumlicher Geltungsbereich

Im Gegensatz zur Verordnung (EU) 2016/679 (Art. 3) enthält der VE-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.⁸⁰

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.⁸¹ 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

⁷⁸ SR 221.411

⁷⁹ SR 281.1

⁸⁰ 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").

⁸¹ <http://www.ejpd.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-11/ber-br-d.pdf>.

haben, wie beispielsweise Irland oder die Vereinigten Staaten. Schliesslich weist der Bundesrat darauf hin, dass die Pflicht zur Bezeichnung eines Zustellungsdomizils im VwVG und im Verwaltungsgerichtsgesetz vom 17. Juni 2005⁸² vorgesehen ist.

8.1.1.3 Art. 3 Begriffe

Buchstabe a Personendaten

Der Begriff der Personendaten bleibt im Vergleich zum bisherigen Recht unverändert. Es handelt sich dabei um alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Eine natürliche Person ist bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, beispielsweise über den Hinweis auf ihren Namen, eine Identifikationsnummer, Standortdaten, eine Online-Identität oder mehrere spezifische Aspekte, die ihre physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder gesellschaftliche Identität betreffen. Wie auch nach dem aktuellen Recht reicht die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei bestimmbar. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Die zur Verfügung stehenden technischen Möglichkeiten werden in Bezug darauf geprüft, wie hoch der zeitliche und finanzielle Aufwand für ihre Anwendung ist. Mit Blick auf die immer gezielteren Technologien zur Datenauswertung und deren konstante Weiterentwicklung verschwimmt die Grenze zwischen Personendaten und anderen Daten indes zusehends. Daten, bei denen heute noch eine rein theoretische Möglichkeit der Identifizierung anzunehmen ist, können morgen vielleicht bereits einer bestimmbar Person zugeordnet werden.

Darauf hinzuweisen ist, dass das Datenschutzgesetz 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. Ist darüber hinaus von Daten die Rede, handelt es sich um Daten, die keine Personendaten sind, wie dies beispielsweise beim Profiling der Fall ist.

Buchstabe c Besonders schützenswerte Personendaten

Der Begriff «besonders schützenswerte Personendaten» (Bst. c) wird auf genetische Daten (Ziff. 3) und biometrische Daten, die eine natürliche Person eindeutig identifizieren (Ziff. 6), 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. k des Bundesgesetzes vom 8. Oktober 2004⁸³ über genetische Untersuchungen beim Menschen).

Bei den biometrischen Daten, um die es hier geht, handelt es sich um Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums, die durch ein spezifisches technisches Verfahren gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen. Dazu gehören beispielsweise Gesichtsbilder oder Fingerabdruckdaten. Fotos fallen somit nur unter den Begriff der biometrischen Daten, wenn sie mit spezifischen technischen Mitteln so bearbeitet werden, dass eine eindeutige Identifizierung oder Authentisierung eines Individuums möglich ist.

Wie im E-SEV 108 (Art. 6 Abs. 1), in der Richtlinie (EU) 2016/680 (Art. 10) und in der Verordnung (EU) 2016/679 (Art. 9) umfassen die besonders schützenswerten Personendaten auch solche, welche das Sexualleben der betroffenen Person betreffen. Diese Daten werden durch den Begriff der Intimsphäre erfasst.

⁸² SR 173.32

⁸³ SR 810.12

Buchstabe d Bearbeiten

Der Begriff des Bearbeitens in Buchstabe d bleibt inhaltlich unverändert. 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 Abs. 1 der Verordnung [EU] 2016/679 und Art. 3 Abs. 2 der Richtlinie [EU] 2016/680). Wie im aktuellen Recht ist die Liste der möglichen Bearbeitungsvorgänge nicht abschliessend, so dass zahlreiche Operationen darunter fallen können (Organisation, Sortieren, Verändern, Auswerten von Daten etc.).

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

Buchstabe 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. Seit dem Inkrafttreten des DSG im Jahr 1992 kam ihm keine grosse Bedeutung zu und heute scheint er durch die Entwicklung neuer Technologien überholt. An seiner Stelle wird im VE der Begriff des «Profiling» verwendet. Der Begriff findet sich in Art. 3 Ziff. 4 der Richtlinie (EU) 2016/680 und Art. 4 Ziff. 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. So ist Profiling definiert als jede Auswertung von Personendaten oder nicht-personenbezogenen Daten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen. Der VE-DSG führt als Beispiele für persönliche Merkmale, die analysiert werden können, die Arbeitsleistung, die wirtschaftliche Lage, die Gesundheit, die Intimsphäre oder auch die Mobilität auf. Diese Analyse kann beispielsweise erfolgen, um herauszufinden, ob eine Person für eine bestimmte Tätigkeit geeignet ist.

Die Begriffsdefinition erfasst die Auswertung von Personendaten sowie anderen Daten und trägt damit der Tatsache Rechnung, dass es durch die technische Entwicklung (Big Data) vermehrt möglich wird, Daten ohne persönlichen Bezug so auszuwerten, dass anschliessend Personendaten vorliegen. Ohne Bedeutung ist dabei, ob der Verantwortliche, der das Profiling betreibt, dies für eigene Zwecke tut oder für einen Dritten. Ebenfalls bezieht Profiling sowohl die automatisierte als auch die nicht-automatisierte Auswertung von Daten mit ein (zur Abgrenzung zur automatisierten Einzelentscheidung vgl. Ziff. 8.1.3.3). Dies erscheint sachgerecht, weil der Automatisierungsgrad der Verarbeitung (z.B. mit oder ohne Algorithmus) kein sachgerechtes Kriterium dafür ist, welche Aktivitäten den besonderen Schutz der betroffenen Person erfordern. Vielmehr ist massgebend, dass Daten im Hinblick auf die Untersuchung zentraler Persönlichkeitsmerkmale ausgewertet werden. Auf diese Weise ergibt sich auch keine Schutzlücke durch die terminologische Umstellung vom Persönlichkeitsprofil auf das Profiling. Darüber hinaus erlaubt es der neue Begriff, den verschiedenen Bundesorganen gezielter eine gesetzliche Grundlage zu gewähren. Nur jene Bundesorgane, welche tatsächlich Profiling betreiben, sollen eine entsprechende Kompetenz erhalten.

Daten, welche aufgrund eines Profilings entstehen, sind grundsätzlich Personendaten im Sinne von Artikel 3 Buchstabe a VE-DSG. Je nach Gegenstand kann es sich dabei auch um besonders schützenswerte Personendaten handeln.

Buchstabe h Verantwortlicher

Der VE-DSG sieht die Einführung dieses Begriffs vor, damit die gleiche Terminologie wie im E-SEV 108 (Art. 2 Bst. b), in der Richtlinie (EU) 2016/680 (Art. 3 Ziff. 8) und in der Verordnung (EU) 2016/679 (Art. 4 Ziff. 7) verwendet wird. Als «Verantwortlicher» gilt die

private Person oder das Bundesorgan, die oder das über den Zweck, die Mittel und den Umfang der Bearbeitung von Daten entscheidet. Damit es sich um einen «Verantwortlichen» handelt, müssen zwei kumulative Kriterien erfüllt sein: Die private Person oder das Bundesorgan muss zum einen festlegen, zu welchen Zwecken die Daten bearbeitet werden; zum anderen muss diese bzw. dieses darüber bestimmen, mit welchen Mitteln dies erfolgt. Diese Begriffsdefinition unterscheidet sich somit teilweise von jener des «Inhabers der Datensammlung», welche die zweite Bedingung nicht voraussetzt. Das entscheidende Kriterium besteht nicht mehr darin, wer über den Inhalt der Datensammlung entscheidet, sondern wer über die Mittel zur beabsichtigten Datenbearbeitung bestimmt.

Buchstabe i 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) 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. Ein Arbeitnehmer mit einem Arbeitsvertrag ist gegenüber seinem Arbeitgeber hingegen kein Auftragsbearbeiter.

Unveränderte Begriffe

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

Aufgehobene Begriffe

- Inhaber der Datensammlung: Dieser Begriff wird durch den Begriff «Verantwortlicher» ersetzt.
- Datensammlung: Der VE-DSG sieht vor, auf diesen Begriff zu verzichten. Dies entspricht der Lösung im E-SEV 108, in dem stattdessen der Begriff 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 Server zugegriffen wird, um anhand der erhobenen Daten bestimmte Aspekte der Persönlichkeit eines Individuums zu beurteilen. Nach dem derzeitigen Recht fallen solche Aktivitäten wie auch das Profiling nicht unter die Gesetzesbestimmungen, die das Bestehen einer Datensammlung voraussetzen – wie beispielsweise das Auskunftsrecht (Art. 8 DSGVO) oder die Informationspflicht (Art. 14 DSGVO) –, 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.⁸⁴
- Gesetz im formellen Sinn: Der VE-DSG sieht vor, diese Begriffsdefinition aufzuheben, da sie nicht nötig ist.

8.1.2 Allgemeine Datenschutzbestimmungen

8.1.2.1 Art. 4 Grundsätze

Absätze 1 und 2 Rechtmässigkeit und Verhältnismässigkeit

Die Absätze 1 und 2 betreffend die Grundsätze der Rechtmässigkeit, von Treu und Glauben und der Verhältnismässigkeit bleiben mit Ausnahme einer redaktionellen Änderung in der französischen Version von Absatz 2 unverändert.

⁸⁴ 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 DSGVO N 32; VPB 62.57.

Absatz 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 Ziff. 4 Bst. b), ist im VE-DSG vorgesehen, dass Daten nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden dürfen. Diese neue Formulierung hat im Vergleich zum geltenden Recht keine materiellen Änderungen zur Folge. Die Beschaffung der Daten und 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 unzulässig sind. 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.

Der VE-DSG sieht zur terminologischen Annäherung an die europäischen Texte (Art. 5 Abs. 4 Bst. b E-SEV 108, Art. 4 Abs. 1 Bst. b der Richtlinie [EU] 2016/680 und Art. 5 Bst. b der Verordnung [EU] 2016/679) im selben Absatz weiter vor, dass Daten nicht in einer Weise weiterbearbeitet werden dürfen, die mit dem anfänglichen Zweck nicht vereinbar ist. Dies ist der Fall, wenn die Weiterbearbeitung aus Sicht der betroffenen Person berechtigterweise als unerwartet, unangebracht oder beanstandbar erscheinen kann. Dabei sind etwa folgende Fälle denkbar:

- die Weiterverwendung von Adressen, die beim Unterschriftensammeln für eine politische Kampagne erfasst wurden, zu Werbezwecken;
- 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;
- 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;⁸⁵
- die Beschaffung von IP-Adressen von Anschlussinhabern, die Raubkopien zum Herunterladen anbieten, durch ein Privatunternehmen⁸⁶.

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.⁸⁷ 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.

Gemäss Absatz 4 dürfen Daten nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person erlaubt, als dies für den Zweck ihrer Bearbeitung erforderlich ist. Der Bundesrat schlägt vor, diese Anforderung im Hinblick auf die Übereinstimmung mit dem E-SEV 108 (Art. 5 Abs. 1 Bst. e), der Richtlinie (EU) 2016/680 (Art. 4 Abs. 1 Bst. e) und der Verordnung (EU) 2016/679 (Art. 5 Abs. 1 Bst. e) ausdrücklich zu erwähnen. Sie ergibt sich bereits aus dem Verhältnismässigkeitsgrundsatz (Art. 4 Abs. 2 DSG). Im Einzelfall kann sich aus bestimmten Zwecken indes auch eine längere nicht-anonymisierte Aufbewahrungsdauer ergeben. Dies gilt insbesondere bei öffentlichen Archiven, die aufgrund ihrer gesetzlich festgelegten Aufgabe Daten auch längerfristig aufbewahren können.

⁸⁵ VPB 69.106 E. 5.6.

⁸⁶ BGE 136 II 508 E. 4.

⁸⁷ MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, N 731.

Absatz 5 Richtigkeit

Absatz 5 VE-DSG übernimmt den Grundsatz der Richtigkeit der Daten, der gegenwärtig in Artikel 5 DSGVO 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. Eine materielle Änderung erfolgt hingegen nicht. So muss jede Person, die Daten bearbeitet, nach wie vor prüfen, ob die bearbeiteten Personendaten richtig und aktuell sind (Vergewisserungspflicht). Falls sie unvollständig oder veraltet sind, müssen die Personendaten korrigiert und ergänzt werden, soweit sie für die Bearbeitung erforderlich sind (Sorgfaltspflicht). Ansonsten müssen die Daten gelöscht werden (Löschungspflicht). Diese Pflichten gelten grundsätzlich für alle Personen, die Daten bearbeiten, und alle Arten der Datenbearbeitung, weil sowohl sie als auch die betroffene Person ein erhebliches Interesse daran haben, dass nur aktuelle und zutreffende Daten bearbeitet werden.

Diese Pflichten sind in Bezug auf die Tätigkeit von Archiven, Museen, Bibliotheken und anderen Gedächtnisinstitutionen indes 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 NBibG⁸⁸). 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 alleine darauf bezieht, dass die fraglichen Dokumente originalgetreu wiedergegeben 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.

Um sich den Begrifflichkeiten der genannten europäischen Regelungen anzupassen, wird darüber hinaus im französischen Text der Begriff "correct" durch "exact" ersetzt; auf Deutsch und Italienisch stimmt die verwendete Terminologie bereits jetzt überein. Zudem wird präzisiert, dass die Daten aktuell sein müssen. Dies bringt keine materiellen Änderungen mit sich. Denn bereits nach dem aktuellen Recht, müssen Daten nach den gegebenen Umständen vervollständigt und aktualisiert werden.⁸⁹

Absatz 6 Einwilligung

Sofern für die Bearbeitung von Daten eine Einwilligung erforderlich ist, ist eine solche gemäss Absatz 6 erster Satz nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Diese Neuformulierung ermöglicht eine terminologische Annäherung an den E-SEV 108 (Art. 5 Abs. 2) und an die Verordnung (EU) 2016/679 (Art. 4 Ziff. 11 und Art. 6 Ziff. 1 Bst. a). Wie bereits nach dem bestehenden Recht, muss die Einwilligung für eine spezifische Bearbeitung oder eine Bearbeitungskategorie gegeben werden und den gesamten Zweck der Bearbeitung abdecken. Mit dieser Formulierung ist die Einwilligung weiterhin an keine Formvorschrift gebunden und kann durch konkludentes Handeln gegeben werden. Bleibt die betroffene Person gänzlich untätig, liegt hingegen keine Einwilligung vor.

Gemäss dem zweiten Satz von Artikel 6 VE-DSG muss die Einwilligung ausdrücklich erfolgen, wenn es um die Bearbeitung besonders schützenswerter Personendaten und das Profiling geht. Dabei werden in der französischen und italienischen Version des Textes die Begriffe «explicite» und «esplicito» durch die Begriffe «exprès» und «espresso» ersetzt. Durch diese Änderung wird der in der Lehre ausgetragenen Kontroverse über die Art der Einwilligung⁹⁰ ein Ende gesetzt und es werden die Anforderungen des Übereinkommens SEV 108 (Art. 5 Abs. 2) erfüllt; die Verordnung (EU) 2016/679 (Art. 4 Ziff. 11 und Art. 6 Ziff. 1 Bst. a) sieht eine ähnliche Regelung vor. Eine ausdrückliche Einwilligung muss durch eine

⁸⁸ Bundesgesetz vom 18. Dezember 1992 über die Schweizerische Nationalbibliothek, SR 432.21

⁸⁹ MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, N 753 f.; Vgl. auch BBI 1988 413, 450

⁹⁰ Bestimmte Autoren stellen den Ausdruck «ausdrücklich» dem konkludenten Handeln gegenüber, während andere die Meinung vertreten, eine ausdrückliche Einwilligung könne sich aus konkludentem Handeln ergeben, wenn die Absicht der betroffenen Person klar ist. Für eine Zusammenfassung der Meinungen zu dieser Frage: VASELLA DAVID, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter 16. November 2015.

schriftliche Erklärung (einschliesslich auf elektronischem Weg), eine mündliche Äusserung oder Zeichen gegeben werden. Dies ist insbesondere möglich durch das Ankreuzen eines Kästchens oder das Anklicken einer Schaltfläche (z. B.: «weiter») auf einer Website, die Auswahl bestimmter technischer Parameter für die Dienste eines Informationsverarbeitungsunternehmens oder anderweitige Erklärungen.

8.1.2.2 Art. 5 Bekanntgabe ins Ausland

Diese Bestimmung entspricht den Anforderungen von Artikel 12 E-SEV 108, der den Grundsatz festhält, dass Daten nur ins Ausland übermittelt werden dürfen, wenn ein angemessenes Datenschutzniveau besteht (Abs. 2). Absatz 3 dieser Bestimmung definiert die Fälle, in denen diese Voraussetzung erfüllt ist. Durch die Regelung in Artikel 5 VE-DSG erfolgt auch eine Angleichung an das Recht der Europäischen Union (Art. 45 ff. der Verordnung [EU] 2016/679).

Absatz 1 Grundsatz

In Absatz 1 wird der in Artikel 6 Absatz 1 DSG verankerte Grundsatz übernommen, wobei allerdings die Passage «weil *eine Gesetzgebung* fehlt, die einen angemessenen Schutz gewährleistet» entfernt wird. Es handelt sich um eine redaktionelle Änderung, die durch den neuen Absatz 2 erforderlich wurde.

Absatz 2 Feststellung durch den Bundesrat

Gemäss Absatz 2 können Daten ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung im betreffenden Staat 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 Schutz⁹¹ gewährleistet. Gegebenenfalls hat er die Liste des Beauftragten mit den Staaten, die diese Anforderung erfüllen, beizuziehen (Art. 7 VDSG).⁹² Um eine einheitliche Anwendung des Absatz 2 sicherzustellen, wird die Angemessenheit der ausländischen Gesetzgebung in Zukunft durch den Bundesrat geprüft. Dieser erstellt eine Liste von Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet (Abs. 7). Im Rahmen seiner Prüfung muss der Bundesrat nicht nur untersuchen, ob der ausländische Staat über eine Gesetzgebung verfügt, die materiell den Anforderungen E-SEV 108 genügt, sondern auch wie diese Gesetzgebung angewendet wird. Das Ergebnis dieser Prüfung wird in einer Verordnung des Bundesrates veröffentlicht, die in die systematische Sammlung aufgenommen wird. Diese Verordnung ist als Positivliste konzipiert und enthält eine Aufzählung jener Staaten, die über eine Gesetzgebung verfügen, aufgrund der ein angemessener Schutz sichergestellt ist. Wenn ein ausländischer Staat nicht in dieser Liste des 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 jenes Staates den Anforderungen der Gewährleistung eines angemessenen Schutzes nicht entspricht. Mit der Revision wird die Liste des Bundesrates ein gesetzlich verbindliches Kriterium für die Verantwortlichen, die eine Bekanntgabe von Daten ins Ausland vorsehen, während die bisherige Liste des Beauftragten lediglich als Hilfsmittel gedacht war, das diesen zur Verfügung gestellt wurde.

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

⁹¹ BBI 2003 1940-1941

⁹² Die Liste des Beauftragten ist unter der folgenden Adresse abrufbar:
<http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de>.

Absatz 3 Keine Entscheidung durch den Bundesrat

Liegt keine Entscheidung des Bundesrates nach Absatz 2 vor, sieht Absatz 3 Buchstaben a–d vor, dass Personendaten ins Ausland bekannt gegeben werden können, wenn ein geeigneter Schutz besteht. Der VE-DSG folgt dem Beispiel der Europäischen Union und verwendet zwei verschiedene Begriffe in den Absätzen 2 und 3. Der Begriff des «angemessenen» Schutzes bleibt der Qualifizierung einer ausländischen Gesetzgebung vorbehalten.

Nach Buchstabe a kann ein geeigneter Schutz durch einen völkerrechtlichen Vertrag gewährleistet werden. Unter «völkerrechtlicher Vertrag» ist nicht nur ein internationales Datenschutzübereinkommen zu verstehen, dem der Empfängerstaat angehört, wie das Übereinkommen SEV 108 und sein Zusatzprotokoll, sondern auch jedes weitere 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 56 Buchstabe b VE-DSG abgeschlossen hat.

Absatz 3 Buchstaben b und c entsprechen 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.

Absatz 3 Buchstabe b Spezifische Garantien

Nach Absatz 3 Buchstabe b können Daten ins Ausland bekannt gegeben werden, wenn Garantien vorgesehen sind, die im Einzelfall einen geeigneten Schutz gewährleisten und über die der Beauftragte vorgängig informiert worden ist. Hat der Beauftragte Einwände gegen die spezifischen Garantien, muss er den Verantwortlichen oder den Auftragsbearbeiter innert dreissig Tagen seit Erhalt der Garantien informieren (Abs. 4). Artikel 6 Absatz 5 VDSG sieht dasselbe vor. Bestehen keine Einwände oder ist die Frist abgelaufen, so ist der Verantwortliche berechtigt, Daten ins Ausland bekannt zu geben. 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 Garantien einhält. Auch haftet er nach wie vor für Nachteile, die sich aus einer Verletzung der Garantien ergeben können.

Entsprechend der verwendeten Terminologie bezieht sich der Begriff der «Garantien, die im Einzelfall einen angemessenen Schutz gewährleisten» auf die Bekanntgabe ins Ausland in «Einzelfällen» und nicht auf die Bekanntgabe in standardisierter Form. Im privaten Sektor kann es sich bei diesen Garantien um Vertragsklauseln handeln, die im Rahmen eines Vertrags zwischen dem Verantwortlichen und dem Empfänger vereinbart werden. Im öffentlichen Sektor kann ein Bundesorgan, das einem ausländischen Staat die Zusage für die Zusammenarbeit erteilt, die Zusage an Bedingungen für den Bereich des Datenschutzes knüpfen. Im Gegensatz zu den standardisierten Garantien (siehe Bst. c) gelten die Garantien, die im Einzelfall einen geeigneten Schutz gewährleisten, nur für die Bekanntgabe, die im entsprechenden Vertrag vorgesehen ist. Beabsichtigt der Verantwortliche, erneut Daten bekannt zu geben, so muss er grundsätzlich neue Garantien festlegen.

Absatz 3 Buchstabe c Standardisierte Garantien

Nach Absatz 3 Buchstabe c können Daten gestützt auf standardisierte Garantien ins Ausland bekannt gegeben werden. Diese Garantien können entweder von interessierten Privatpersonen oder Kreisen erarbeitet (Ziff. 1) oder durch den Beauftragten ausgestellt oder anerkannt worden sein (Ziff. 2). Auch die Bundesorgane können auf diese Art von Garantien zurückgreifen. Der Begriff der «standardisierten Garantien» 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 Fall von Absatz 3 Buchstabe c Ziffer 1 müssen die Garantien vorgängig vom Beauftragten genehmigt werden. Diese Bedingung stellt gegenüber dem geltenden Recht, wonach der Beauftragte lediglich informiert werden muss (Art. 6 Abs. 3 DSGVO), eine Verschärfung dar. Sie entspricht der Anforderung von Artikel 12^{bis} Absatz 2 Buchstabe b E-SEV 108. Der Beauftragte verfügt über eine Frist von sechs Monaten, um dem Verantwortlichen mitzuteilen, ob er die ausgearbeiteten Garantien genehmigt oder nicht (Abs. 5 erster Satz). Diese Frist beginnt im Zeitpunkt, in dem der Beauftragte die vollständigen Akten erhalten hat, das heisst sämtliche Informationen, die erforderlich sind, um über die Gültigkeit der eingereichten standardisierten Garantien zu entscheiden. Es handelt sich dabei um eine Ordnungsfrist; falls sie nicht eingehalten wird, kommen die Vorschriften zur Rechtsverweigerung zur Anwendung. Der Verantwortliche darf keine Daten ins Ausland bekannt geben, bis er vom Beauftragten eine entsprechende beschwerdefähige Verfügung (Art. 5 VwVG) erhalten hat.

Nach Absatz 3 Buchstabe c Ziffer 2 kann der Verantwortliche auch auf standardisierte Garantien zurückgreifen, welche der Beauftragte erstellt oder anerkannt hat, beispielsweise Musterverträge oder Standardvertragsklauseln, wobei er ihn darüber informieren muss (Abs. 6). Sobald er seiner Informationspflicht nachgekommen ist, ist er berechtigt, Daten ins Ausland bekannt zu geben. Beschliesst ein Verantwortlicher, Daten gestützt auf standardisierte Garantien im Sinne von Absatz 2 Buchstabe c 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 Garantien insbesondere durch den Empfänger der Daten ergeben können. In der Verordnung ist daher die Pflicht des Beauftragten vorzusehen, eine Liste der erstellten oder anerkannten standardisierten Garantien zu veröffentlichen, wie es im Übrigen im geltenden Recht vorgesehen ist (Art. 6 Abs. 3 VDSG).

Absatz 3 Buchstabe d verbindliche unternehmensinterne Datenschutzvorschriften

Nach Absatz 3 Buchstabe d kann die Bekanntgabe von Daten ins Ausland auch gestützt auf verbindliche unternehmensinterne Datenschutzvorschriften erfolgen, die vorgängig durch den Beauftragten (Ziff. 1) oder durch eine ausländische Behörde, die für den Datenschutz zuständig ist (Ziff. 2), genehmigt wurden. Diese Bestimmung ersetzt Artikel 6 Absatz 2 Buchstabe g DSGVO. Absatz 2 Buchstabe d 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 3 Buchstabe d stellt insofern eine Verschärfung des geltenden Rechts dar, als die verbindlichen unternehmensinternen Datenschutzvorschriften neu genehmigt werden müssen. Der Beauftragte verfügt über eine Frist von sechs Monaten, um dem betreffenden Unternehmen mitzuteilen, ob er die vorgelegten verbindlichen unternehmensinternen Datenschutzvorschriften genehmigt oder nicht (Abs. 5). In der Zwischenzeit können keine Daten ins Ausland übermittelt werden. Der Entscheid des Beauftragten kann mit Beschwerde angefochten werden

Wurden die verbindlichen unternehmensinternen Datenschutzvorschriften durch eine ausländische Behörde genehmigt, die für den Datenschutz zuständig ist (Abs. 3 Bst. d Ziff. 2), muss das Unternehmen mit Sitz in der Schweiz diese dem Beauftragten mitteilen, damit er seinen Aufsichtspflichten nachkommen kann (Abs. 6). Diese Bestimmungen entsprechen den Bedürfnissen von Unternehmensgruppen, die sich über mehrere Länder erstrecken.

Die in Absatz 3 Buchstabe d 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 bekanntgebener 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. Gegebenenfalls kann der Bundesrat in der Ausführungsverordnung Kriterien definieren, welche die verbindlichen unternehmensinternen Vorschriften erfüllen müssen.

Absatz 7 Veröffentlichung der Liste

Die Liste des Bundesrates wird veröffentlicht (Abs. 7). Dabei ist hervorzuheben, dass diese künftige Ausführungsverordnung regelmässig aktualisiert werden muss. Der Bundesrat muss mit anderen Worten periodisch die Gesetzgebung derjenigen Staaten überprüfen, die auf der Liste stehen. Dabei kann er sich auch auf die Evaluationen des Europarates und der Europäischen Union stützen.

Ein Verstoß gegen Artikel 5 wird sanktioniert (Art. 50 Abs. 2 Bst. B und 51 Abs. 1 Bst. a VE-DSG).

8.1.2.3 Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen

Absatz 1 Ausnahmefälle

In Anlehnung an das geltende Recht (Art. 6 Abs. 2 DSG) regelt Artikel 6 Absatz 1 VE-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. Die Einwilligung der betroffenen Person ist gültig, wenn die Voraussetzungen nach Artikel 4 Absatz 6 VE-DSG erfüllt sind. Die betroffene Person ist insbesondere über die Risiken der Bekanntgabe zu informieren.

Buchstabe b entspricht Artikel 6 Absatz 2 Buchstabe c DSG.

Buchstabe c Ziffer 1 entspricht Artikel 6 Absatz 2 Buchstabe d erster Satzteil DSG. 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 bekanntgegeben 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, ausser dass der Ausdruck «vor Gericht», der als zu eng befunden wird, durch «vor einem Gericht oder einer Verwaltungsbehörde» ersetzt wird.

In Buchstabe d wird präzisiert, dass die Bekanntgabe auch zulässig ist, wenn sie notwendig ist, um das Leben oder die körperliche Unversehrtheit 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. Wegen der Aufhebung von Artikel 2 Absatz 2 Buchstabe d DSG über öffentliche Register des Privatrechtsverkehrs muss im Gesetz präzisiert werden, 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 geht in dieselbe Richtung und 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.

Absatz 2 Mitteilung an den Beauftragten

Absatz 2 verpflichtet den Verantwortlichen oder den Auftragsbearbeiter, dem Beauftragten mitzuteilen, wenn er Personendaten aufgrund der Buchstaben b, c und d bekannt gibt. Diese

Bestimmung gilt sowohl für private Verantwortliche als auch für Bundesorgane. Sie setzt die Anforderungen von Art. 12 Abs. 5 E-SEV 108 um.

Ein Verstoß gegen Artikel 6 wird gemäss Artikel 51 Absatz 1 Buchstabe a VE-DSG strafrechtlich sanktioniert.

8.1.2.4 Art. 7 Auftragsdatenbearbeitung

In den Absätzen 1, 2 und 4 erfolgen terminologische Änderungen, die infolge der neuen Begriffe (Auftragsbearbeiter, Verantwortlicher) erforderlich sind.

Nach Absatz 2 muss sich der Verantwortliche neu vergewissern, dass der Auftragsbearbeiter in der Lage ist, nicht nur die Datensicherheit zu gewährleisten, sondern auch die Rechte der betroffenen Person. Diese Erweiterung wird von der Richtlinie (EU) 2016/680 (Art. 22 Abs. 1) gefordert. Der Bundesrat ist der Auffassung, dass eine ausschliesslich bereichsspezifische Umsetzung in den Schengen-Bereichen nicht sinnvoll ist. Dies gilt umso mehr, als die Verordnung (EU) 2016/679 (Art. 28 Abs. 1) eine analoge Regelung vorsieht. Der Bundesrat erhält darüber hinaus die Möglichkeit, die weiteren Pflichten des Auftragsbearbeiters auf dem Verordnungsweg zu präzisieren.

Absatz 3 ist neu und sieht vor, dass der Auftragsbearbeiter die Datenbearbeitung ohne vorgängige schriftliche Zustimmung des Verantwortlichen keinem weiteren Auftragsbearbeiter übertragen darf. Dabei kann es sich um eine allgemeine Einverständniserklärung handeln. In diesem Fall informiert der Auftragsbearbeiter den Verantwortlichen über jede Änderung (Hinzuziehung oder Ersetzung anderer Auftragsbearbeiter), damit er Einspruch gegen diese Änderungen erheben kann. Es handelt sich hierbei um eine Anforderung der Richtlinie (EU) 2016/680 für den Schengen-Bereich (Art. 22 Absatz 2); die Verordnung (EU) 2016/679 (Art. 28 Absatz 2) sieht etwas Ähnliches vor. Der Bundesrat hat beschlossen, die Vorschrift auf alle Fälle von Auftragsdatenbearbeitung anzuwenden, wodurch die Transparenz der Datenbearbeitung und die Kontrolle der betroffenen Personen über ihre Daten erhöht werden. Nach Artikel 13 Absatz 4 ist der Verantwortliche darüber hinaus verpflichtet, die betroffene Person zu informieren, wenn die Bearbeitung einem Auftragsbearbeiter übertragen wird, und muss ihr die Daten oder Kategorien von Daten mitteilen, die bearbeitet werden.

8.1.2.5 Art. 8 Ausarbeitung von Empfehlungen der guten Praxis

Der allgemeine, technologieneutrale Charakter der Regeln des DSG kann insbesondere im Privatsektor für die Verantwortlichen und die Auftragsbearbeiter, aber auch für die betroffenen Personen eine grosse Unsicherheit in Bezug auf das richtige Verhalten mit sich bringen. Nach Ansicht des Bundesrates ist es daher zentral, die Möglichkeit vorzusehen, ergänzend zum Gesetz konzisere und dynamischere Regeln zu erlassen. Er schlägt deshalb vor, die Ausarbeitung und den Erlass von Empfehlungen der guten Praxis zu formalisieren. Solche Empfehlungen können in Bereichen, die heute zahlreiche Fragen aufwerfen, wie beispielsweise bei der Videoüberwachung, dem Cloud Computing oder sozialen Netzwerken präzisere Lösungen vorsehen. Sie können auch bereichsspezifisch einzelne Begriffe (z. B. das erhöhte Risiko nach Art. 16 VE-DSG) und die Modalitäten bestimmter Rechte und Pflichten präzisieren, wie beispielsweise die Modalitäten des Rechts, bei einer automatisierten Einzelentscheidung angehört zu werden (Art. 15 und 20 Abs. 3 VE-DSG), oder die Modalitäten der Informationspflicht (Art. 13 und 14 VE-DSG) und der Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen (Art. 16 VE-DSG). Die Empfehlungen können zuhanden des Privatsektors erlassen werden, aber auch zuhanden des öffentlichen Sektors.

Die Ausarbeitung von Verhaltensregeln und die Förderung der Selbstregulierung durch die Staaten sowie die Aufsichtsbehörde sind auch in den Artikeln 40 und 57 Absatz 1 Buchstabe m der Verordnung (EU) 2016/679 vorgesehen

Absatz 1 Erarbeitung durch den Beauftragten

Gemäss Absatz 1 erarbeitet der Beauftragte Empfehlungen der guten Praxis. Der Vorschlag, diese Aufgabe einer extraparlamentarischen Kommission zu übertragen, wurde während der Vorbereitungsarbeiten verworfen (vgl. Ziff. 1.6.5). Tatsächlich scheint der Beauftragte

angesichts der Struktur und Erfahrung dieser Institution am besten in der Lage zu sein, diese Aufgabe wirksam wahrzunehmen. Die Empfehlungen können einzelne Aspekte des Gesetzes konkretisieren, insbesondere betreffend die Transparenz der Datenbearbeitung, die Rechte der betroffenen Person und die Pflichten des Verantwortlichen sowie des Auftragsbearbeiters.

Es geht hier darum, eine Tätigkeit zu formalisieren und auszubauen, welche der Beauftragte im Rahmen seiner Informations- und Beratungsaufgaben (Art. 28, 30 und 31 DSGVO) bereits jetzt zum Teil wahrnimmt. Zur Ausarbeitung der Empfehlungen zieht der Beauftragte die verschiedenen interessierten Kreise wie Wirtschaft, Konsumentenschutzorganisationen und Patienten bei. Auch berücksichtigt er die Besonderheiten der einzelnen Datenbearbeitungsbereiche sowie das erhöhte Schutzbedürfnis von besonders verletzlichen Personen wie Minderjährigen, Behinderten oder älteren Menschen.

Absatz 2 Erarbeitung durch interessierte Kreise

Gemäss Absatz 2 können interessierte Kreise ebenfalls Empfehlungen der guten Praxis ausarbeiten, oder sie können jene des Beauftragten ergänzen oder ändern. Anschliessend können sie die Empfehlungen dem Beauftragten zur Genehmigung unterbreiten. Der Beauftragte genehmigt die vorgelegten Empfehlungen, wenn er zur Auffassung gelangt, dass sie die Datenschutzvorschriften – die auch in anderen Gesetzen als dem VE-DSG stehen können – einhalten. Der Bundesrat möchte konzertierte und breit abgestützte Branchenlösungen fördern, indem er den interessierten Kreisen ermöglicht, selbst aktiv zu werden und zur Regulierung der einzelnen Bereiche beizutragen. Besonders willkommen wären solche Lösungen im Internetbereich (Datenschutz beim Betrieb sozialer Netzwerke, Benutzung von Cookies usw.), wo die Rechte der betroffenen Personen durch eine rein staatliche Regulierung oftmals ungenügend geschützt werden.

Im Bereich des Internets und der Telekommunikation haben interessierte 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 Gesellschaft⁹³, 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)⁹⁴ der Swiss Internet Industry Association (Simsa) vom 1. Februar 2013, der Verhaltensregeln für Schweizer Hosting Provider aufstellt.

Absatz 3 Veröffentlichung

Absatz 3 sieht vor, dass die Empfehlungen der guten Praxis vom Beauftragten publiziert werden. Die Publikation kann auf seiner Website erfolgen.

8.1.2.6 Art. 9 Einhaltung der Empfehlungen der guten Praxis

Wenn der Verantwortliche oder der Auftragsbearbeiter die Empfehlungen der guten Praxis befolgt, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren (Art. 9 Abs. 1 VE-DSG). Diese Bestimmung soll deutlich machen, dass die Einhaltung der Empfehlungen der guten Praxis materiell der Einhaltung des Gesetzes entspricht. Die Bestimmung klärt dadurch zugleich die Natur dieser Empfehlungen, deren Aufgabe es ist, das Gesetz zu konkretisieren.

Absatz 2 hält fest, dass Datenschutzvorschriften auch auf andere Weise eingehalten werden können, als dies in den Empfehlungen der guten Praxis vorgesehen ist. Dies zeigt den freiwilligen Charakter der Empfehlungen auf. Die Verantwortlichen müssen die Empfehlungen nicht befolgen, um das Gesetz einzuhalten, sondern es ist ihnen freigestellt, dies zu tun. Die interessierten Kreise können allerdings auf Ebene ihrer Verbände etwas anderes vorsehen.

⁹³ https://asut.ch/asut/resources/documents/initiative_sectorielle_protection_jeunesse_m%C3%A9dias.pdf.

⁹⁴ http://simsa.ch/_Resources/Persistent/2260a505424ef1e0c8100899a6f38a06e4a4ecff/130201-simsa-cch-public-f.pdf.

8.1.2.7 Art. 10 Zertifizierung

Artikel 10 VE-DSG regelt die fakultative Zertifizierung, die gegenwärtig in Artikel 11 DSG geregelt ist. Der VE dehnt den Gegenstand des Zertifizierungsverfahrens auf sämtliche Arten von Datenbearbeitungsvorgängen aus. Neben Datenbearbeitungssystemen (Verfahren, Organisation) und Produkten (Programme, Systeme), ist es künftig auch möglich, bestimmte Dienstleistungen zu zertifizieren. Diese Ausweitung ermöglicht eine Annäherung an die Verordnung (EU) 2016/679, die ebenfalls eine Zertifizierung für alle Verarbeitungsvorgänge der Verantwortlichen oder Auftragsverarbeiter vorsieht (Art. 42).

Das Akkreditierungsverfahren für unabhängige Zertifizierungsstellen durch die schweizerische Akkreditierungsstelle, mit der auch der Beauftragte assoziiert ist, bleibt unverändert.⁹⁵

8.1.2.8 Art. 11 Datensicherheit

In Artikel 11 VE-DSG wird Artikel 7 DSG mit einigen redaktionellen Änderungen übernommen. 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. Es wird präzisiert, dass die Verantwortlichen und die Auftragsbearbeiter durch technische und organisatorische Massnahmen die Daten vor unbefugtem Bearbeiten oder Verlust schützen müssen. Unter den Verlust fällt auch die Vernichtung von Daten.

Aus dieser Pflicht können sich unterschiedliche Massnahmen ergeben. Möglicherweise müssen Daten pseudonomisiert und chiffriert werden. Allenfalls sind Garantien vorzusehen, welche die Vertraulichkeit, Vollständigkeit und Verfügbarkeit des Systems und der Bearbeitungsdienste gewährleisten oder sicherstellen, dass der Zugang zu den Daten und Systemen im Falle einer technischen oder physischen Störung innert angemessener Frist wieder zur Verfügung steht. Schliesslich kann die Pflicht bestehen, Verfahren zu entwickeln, mit denen die Wirksamkeit der technischen und organisatorischen Vorkehrungen zur Datensicherheit regelmässig untersucht, analysiert und beurteilt werden können.

8.1.2.9 Art. 12 Daten einer verstorbenen Person

Einige Elemente dieser Norm betreffend die Daten Verstorbener befanden sich bislang in Artikel 1 Absatz 7 VDSG. So war 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. Durch die Verordnungsbestimmung wurde das Auskunftsrecht somit auf Drittpersonen ausgeweitet, die Auskunft über Daten einer weiteren Drittperson verlangen konnten, ohne dass hierfür im Gesetz eine entsprechende Grundlage vorhanden gewesen wäre. Durch die Aufnahme ins Gesetz wird dieses Problem beseitigt. Systematisch wird die Norm nun den allgemeinen Datenschutzbestimmungen zugeordnet und dadurch vom Auskunftsrecht losgelöst, weil dieses auf die betroffene Person beschränkt bleiben soll.

Neben der Einsicht in die Daten einer verstorbenen Person beantwortet die vorgesehene Bestimmung teilweise das Postulat 14.3782 Schwaab «Richtlinien für den <digitalen Tod>», indem sie ein Recht auf Löschung bzw. Vernichtung der Daten des Verstorbenen durch die Erben vorsieht. Dies erlaubt es den Erben grundsätzlich, den «digitalen Tod» herbeizuführen, ausser dem stünden überwiegende Interessen Dritter bzw. der verstorbenen Person entgegen oder die verstorbene Person hätte dies ausdrücklich untersagt. Weitere Fragen, die sich im Zusammenhang mit dem Postulat ergeben, zum Beispiel betreffend die Übertragbarkeit oder eine mögliche Vererbung von Daten, werden im Rahmen der derzeit laufenden Revision des Erbrechts geprüft.

Absatz 1 Einsicht

Gemäss Absatz 1 muss der Verantwortliche kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse vorliegt. Für bestimmte

⁹⁵ 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).

Konstellationen wird das schutzwürdige Interesse in Absatz 2 fingiert (vgl. unten). Reine Neugier reicht hingegen als schutzwürdiges Interesse nicht aus. Parallel zum Einsichtsrecht nach dem VE-DSG sieht die laufende Revision des Erbrechts ein erbrechtliches Einsichtsrecht vor, das ausschliesslich für Personen gilt, die erbrechtliche Ansprüche geltend machen können und ihnen erlauben soll, im Rahmen des Erbgangs ihre Vermögensrechte geltend zu machen (Art 601a VE-ZGB).

Die Einsicht muss verweigert werden, wenn die verstorbene Person sie ausdrücklich untersagt hat (Bst. a); auf diese Weise wird dem Willen der verstorbenen Person Rechnung getragen. Aufgrund überwiegender Interessen des Verstorbenen kann insbesondere die Einsicht in besonders schützenswerte Personendaten verweigert werden. Auch die Einsicht in Akten eines Arztes bzw. einer Ärztin sowie eines Anwalts bzw. einer Anwältin kann verweigert werden, um überwiegende Interessen der verstorbenen Person zu schützen (Bst. b); ein allfälliges Amts- oder Berufsgeheimnis wird durch Absatz 3 jedoch grundsätzlich aufgehoben.

Ebenfalls darf keine Einsicht gewährt werden, wenn ihr überwiegende Interessen von Dritten entgegenstehen (Bst. b). Die Interessen von Angehörigen gemäss dem aktuellen Art. 1 Abs. 7 VDSG sind zu den Interessen Dritter zu zählen. Dazu gehört ebenfalls der Persönlichkeitsschutz von Drittpersonen. Wann diese Interessen überwiegen, ist im Einzelfall zu entscheiden, wobei unter anderem berücksichtigt werden kann, welche Bedeutung die fraglichen Daten für die jeweiligen Personen haben, ob durch die Einsicht zugleich Daten über diese Drittpersonen bekanntgegeben werden und zu welchem Zweck die Einsicht verlangt wird.

Absatz 2 Interessensfiktion

Nach Absatz 2 wird ein schutzwürdiges Interesse an der Einsicht fingiert bei Personen, die mit der verstorbenen Person in gerader Linie verwandt oder mit ihr im Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten. Das heisst, die betreffenden Personen müssen lediglich nachweisen, dass sie zur verstorbenen Person in einer solchen engeren Beziehung standen, und sind dadurch vom Nachweis eines schutzwürdigen Interesses befreit.

Die Interessenabwägung nach Absatz 1 Buchstaben a und b bleibt unabhängig von dieser Fiktion möglich.

Absatz 3 Geheimnisträger

Absatz 3 hebt grundsätzlich die verschiedenen Amts- und Berufsgeheimnisse auf, welche gegebenenfalls einem Einsichtsgesuch entgegengehalten werden können. Zu denken ist beispielsweise an den Sohn, der die medizinischen Daten seines verstorbenen Vaters einsehen möchte. Ihm könnte eine Ärztin das Arztgeheimnis nicht entgegenhalten.

Falls die Geheimnisträger gegebenenfalls eigene Interessen an der Wahrung ihres Amts- oder Berufsgeheimnisses haben, können diese Interessen im Rahmen der Abwägung nach Absatz 1 Buchstabe b berücksichtigt werden.

Absatz 4 Löschung

Gemäss Absatz 4 kann jeder Erbe verlangen, dass der Verantwortliche Daten des Erblassers kostenlos löscht oder vernichtet. Bewusst wurde dieser Anspruch auf die Erben beschränkt. Ebenfalls wurde er absichtlich so ausgestaltet, dass jeder Erbe die Löschung verlangen kann und dementsprechend nicht die Zustimmung der ganzen Erbengemeinschaft erforderlich ist, was insbesondere in prozessualer Hinsicht zahlreiche Schwierigkeiten vermeidet. Zudem können allfällige sich widersprechende Interessen der Erben gegeneinander abgewogen werden. Schliesslich bleibt das Recht auf Löschung auf diese Weise bestehen, selbst wenn die Erbengemeinschaft sich nach Abschluss des Erbgangs aufgelöst hat. Die Löschung bzw. Vernichtung muss verweigert werden, wenn der Erblasser sie zu Lebzeiten ausdrücklich untersagt hat (Buchstabe a) oder wenn ihr überwiegende Interessen des Erblassers oder von Dritten entgegenstehen (Buchstabe b).

Dieser Anspruch besteht unabhängig von einer Persönlichkeitsverletzung bzw. einer widerrechtlichen Datenbearbeitung gegenüber den Verantwortlichen.

Absatz 5 Vorbehalt spezieller Regelungen

Diese Bestimmung sieht einen Vorbehalt zugunsten eventueller spezieller Regelungen in anderen Bundesgesetzen vor. Vorbehalten bleiben damit zum Beispiel die Bestimmungen des BGÖ, welches den Zugang zu amtlichen Dokumenten der Bundesverwaltung regelt, oder das Bundesgesetz vom 26. Juni 1998⁹⁶ über die Archivierung, welches spezielle Bestimmungen zur Schutzfrist für Personendaten in Dokumenten enthält, die im Bundesarchiv archiviert worden sind.

8.1.3 Pflichten des Verantwortlichen und des Auftragsbearbeiters

Der 3. Abschnitt 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.

8.1.3.1 Art. 13 Informationspflicht bei der Beschaffung von Daten

In Artikel 13 VE-DSG wird neu die Informationspflicht bei der Beschaffung von Daten geregelt. Die Artikel 14 und 18a 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 7^{bis} 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 Datenschutzgesetz 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.

Absatz 1 Grundsatz

Gemäss Absatz 1 muss der Verantwortliche die betroffene Person über die Beschaffung von Personendaten informieren, selbst wenn die Daten bei Dritten beschafft werden. Der Verantwortliche muss die betroffene Person aktiv informieren. 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. Die Information kann individuell oder in allgemeiner Form erfolgen, zum Beispiel über allgemeine Geschäftsbedingungen oder eine standardisierte Datenschutzerklärung auf einer Website. Denkbar sind sogar Symbole oder Piktogramme, soweit sie die nötigen Informationen enthalten. Dabei können die Informationen auch auf mehreren Ebenen zugänglich gemacht werden (z. B. zunächst über ein Symbol, über das mit einem Mausklick weitere, ausführlichere Informationen abrufbar sind). Wird eine allgemeine Form gewählt, muss die Information allerdings leicht zugänglich, vollständig und genügend sichtbar gemacht sein. Die betroffene Person soll ohne eigenes Zutun darauf aufmerksam werden und nicht erst nach der Information suchen oder danach fragen müssen. Ebenso muss die Information verständlich abgefasst sein, so dass sie tatsächlich dem Zweck einer transparenten Datenbearbeitung dient.

Absatz 2 Zu übermittelnde 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

⁹⁶ SR 152.1

Buchstaben a–c konkretisieren diesen Grundsatz durch Mindestangaben, welche der betroffenen Person in jedem Fall mitgeteilt werden müssen. Dazu gehören die Identität und die Kontaktdaten des Verantwortlichen, die bearbeiteten Daten bzw. Kategorien der bearbeiteten Daten und der Bearbeitungszweck. Die Rechtsgrundlage des Bearbeitens ist – namentlich durch die Bundesorgane – ebenfalls mitzuteilen, soweit diese erforderlich ist, damit die betroffene Person ihre Rechte geltend machen kann. 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. Diese Flexibilität ist erforderlich, weil das Datenschutzgesetz 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 Empfehlungen der guten Praxis zu konkretisieren. Die betroffene Person muss spätestens im Zeitpunkt der Datenbeschaffung informiert werden, ausser im Falle von Absatz 5.

Absatz 3 Bekanntgabe an Dritte

Nach Absatz 3 muss die betroffene Person zusätzlich über die Empfänger bzw. Kategorien der Empfänger informiert werden, wenn vorgesehen ist, die Daten an Dritte bekanntzugeben. Falls der Verantwortliche die Identität des Empfängers kennt, muss er diese mitteilen. Diese Pflicht gilt auch, wenn sich der Empfänger im Ausland befindet.

Absatz 4 Übertragung an Auftragsbearbeiter

Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, muss der Verantwortliche der betroffenen Person gemäss Absatz 4 dessen Identität und Kontaktdaten mitteilen und sie darüber informieren, welche Daten oder Kategorien von Daten der Auftragsbearbeiter bearbeiten wird. Diese Pflicht gilt auch für Auftragsbearbeiter, die sich im Ausland befinden.

Absatz 5 Zeitpunkt der Information

Absatz 5 bestimmt den Zeitpunkt, in dem die betroffene Person informiert werden muss, wenn Daten nicht bei der betroffenen Person beschafft werden. In diesem Fall hat die Information spätestens mit der Speicherung der Daten durch den Verantwortlichen bzw. mit der ersten Bekanntgabe an Dritte zu erfolgen, falls eine Bekanntgabe vorgesehen ist. Der Begriff der Speicherung umfasst dabei nicht nur den technischen Vorgang der Aufzeichnung in einem Informatiksystem, sondern jede an die Beschaffung anschliessende Tätigkeit, mit der eine weitere Nutzung der Daten vorbereitet wird.

Ein Verstoß gegen die Informationspflicht wird sanktioniert (siehe Art. 50 Abs. 1, Bst. a und b, Ziff. 1 und 2 VE-DSG).

8.1.3.2 Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen

Artikel 14 VE-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. 3–5). Die beiden Konstellationen sind klar voneinander abzugrenzen. Die Vorschrift übernimmt dabei weitgehend geltendes Recht (Art. 9, Art. 14 Abs. 4 und 5, sowie 18b DSG), das der Klarheit halber in einer Bestimmung zusammengeführt wird.

Absätze 1 und 2 Ausnahmen von der Informationspflicht

Nach Absatz 1 ist der Verantwortliche von der Informationspflicht entbunden, wenn die betroffene Person bereits über die Informationen nach Artikel 13 verfügt. Davon ist auszugehen, wenn die betroffene Person zu einem früheren Zeitpunkt bereits informiert wurde und sich die Informationen, welche übermittelt werden müssen, in der Zwischenzeit nicht geändert haben. Wenn die betroffene Person die Daten selbst zugänglich gemacht hat, gilt sie grundsätzlich ebenfalls als über die Datenbeschaffung informiert. Allerdings müssen

ihr in diesem Fall möglicherweise weitere Informationen nach Artikel 13 zugänglich gemacht werden, welche für eine transparente Datenbearbeitung erforderlich sind.

Nach Absatz 2 entfällt die Informationspflicht in Bezug auf Daten, die nicht bei der betroffenen Person beschafft werden, wenn die Speicherung oder die Bekanntgabe ausdrücklich im Gesetz vorgesehen ist (Abs. 2, Bst. a), oder die Information nur mit unverhältnismässigem Aufwand oder gar nicht möglich ist (Abs. 2, Bst. b). 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 Vorkehrungen zu treffen, die unter den gegebenen Umständen von ihm erwartet werden können, um der Informationspflicht nachzukommen. Erst wenn diese vergeblich bleiben, darf der Verantwortliche davon ausgehen, die Information sei unmöglich.

Absätze 3 und 4 Einschränkung der Information

Die Absätze 3 und 4 legen fest, unter welchen Voraussetzungen der Verantwortliche auf die Übermittlung von Informationen verzichten, diese einschränken oder aufschieben kann. Dabei erfolgt teilweise eine Interessenabwägung in Bezug darauf, ob Informationen übermittelt werden müssen, wobei diese auch davon abhängt, ob es sich beim Verantwortlichen um ein Bundesorgan oder einen Privaten handelt. 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.

Jeder Verantwortliche kann gemäss Absatz 3 die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn dies in einem Gesetz im formellen Sinn vorgesehen ist (Bst. a). Dabei ist in erster Linie an öffentlich-rechtliche Vorschriften zu denken, welche sich an die Bundesorgane richten. Für Private dürften solche Befugnisse weniger vorkommen. Ebenfalls gilt eine Ausnahme von der Informationspflicht, wenn dies wegen überwiegender Interessen Dritter erforderlich ist (Bst. b). 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.

Absatz 4 regelt Konstellationen, unter denen spezifische Verantwortliche die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten können. Der private Verantwortliche kann nach Absatz 4, Buchstabe a die Übermittlung 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. Ein Bundesorgan kann nach Absatz 4, Buchstabe b die Übermittlung 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 Übermittlung ebenfalls einschränken, aufschieben oder darauf verzichten, wenn dadurch der Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage gestellt wird (Ziff. 2). Auf diese Weise soll sichergestellt werden, dass nicht über den Umweg des Datenschutzgesetzes die Vorschriften zum rechtlichen Gehör etc.

nach den Verfahrensgesetzen umgangen werden können und dadurch behördliche oder gerichtliche Verfahren vereitelt werden.

Absatz 5 Nachholen der Information

Gemäss Absatz 5 muss der Verantwortliche die Informationen mitteilen, sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben wegfällt. Dies gilt nicht, wenn die Mitteilung unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen ist (siehe hierzu den Kommentar zu Absatz 2).

8.1.3.3 Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung

Nach Artikel 15 VE-DSG besteht eine Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung. Dies entspricht den Anforderungen von Artikel 8 Buchstabe a E-SEV 108 sowie Artikel 3 Ziffer 3 und 11 der Richtlinie (EU) 2016/680. Artikel 4 Ziffer 3 i.V.m. Artikel 22 der Verordnung (EU) 2016/679 enthält eine ähnliche Bestimmung. Die Einführung dieses neuen Begriffs ist notwendig. Denn solche Entscheidungen sind in allen Wirtschaftsbereichen immer häufiger und werden teilweise auf der Grundlage falscher Daten getroffen.

Absatz 1 Information

Nach Absatz 1 muss der Verantwortliche die betroffene Person informieren wenn eine automatisierte Einzelentscheidung erfolgt und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat. Das heisst, der Verantwortliche muss die betroffene Person über eine automatisierte Einzelentscheidung unterrichten und für diese muss deutlich werden, dass es sich um eine solche Entscheidung handelt.

Eine automatisierte Einzelentscheidung besteht, wenn ohne menschliches Zutun eine Auswertung von Daten erfolgt, die zu einer konkreten Entscheidung gegenüber der betroffenen Person führt. 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. Eine solche Entscheidung hat rechtliche Wirkungen gegenüber der betroffenen Person, wenn sie die Rechtsstellung der betroffenen Person unmittelbar beeinflusst. Unter die erheblichen Auswirkungen auf die betroffene Person fallen insbesondere tatsächliche Konsequenzen einer automatisierten Einzelentscheidung, wobei diese einen gewissen Schweregrad erreichen müssen. Es sind verschiedene Beispiele für automatisierte Einzelentscheidungen denkbar. So kann eine solche vorliegen, wenn die Konditionen nach denen eine Person einen Leasingvertrag abschliessen kann (z.B. Zins, Vertragsdauer, Zahlungsfristen), alleine auf der Basis einer automatisierten Überprüfung der finanziellen Verhältnisse festgelegt werden. Ein anderes Beispiel wäre, wenn eine Krankenversicherung alleine aufgrund der Auswertung der Gesundheitsdaten durch einen Algorithmus mit einer bestimmten Person keinen Versicherungsvertrag abschliesst. Auch Verkehrsbussen, die automatisch aufgrund einer Bildaufnahme an den fraglichen Fahrzeughalter verschickt werden, fallen unter die automatisierten Einzelentscheidungen.

Eine automatisierte Einzelentscheidung kann auch auf einem Profiling im Sinne von Artikel 3 Buchstabe f VE-DSG beruhen. Für das Vorliegen einer automatisierten Einzelentscheidung ist jedoch ein Profiling nicht unbedingt erforderlich; die beiden Begriffe sind daher nicht deckungsgleich. Zentrales Abgrenzungskriterium ist die Automatisierung: Ein Profiling muss nicht über einen automatisierten Vorgang erfolgen, die automatisierte Einzelentscheidung jedoch schon. Ein weiteres Kriterium sind die Auswirkungen auf die betroffene Person. Bei der automatisierten Einzelentscheidung muss aufgrund einer Datenbearbeitung eine bestimmte Entscheidung gefällt werden. Beim Profiling werden Daten zu einem bestimmten Zweck ausgewertet, ohne dass diese Auswertung unmittelbare Wirkungen auf die betroffene Person haben muss.

Absatz 2 Anhörung

Der Verantwortliche muss der betroffenen Person nach Absatz 2 die Möglichkeit geben, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Daten zu äussern. Zusammen mit der Informationspflicht soll diese Anhörung sicherstellen, dass die betroffene Person nicht Entscheidungen unterworfen ist, die ohne menschliches Zutun erfolgen. Sie soll insbesondere die Möglichkeit haben, ihren Standpunkt zum Ergebnis der Entscheidung darzulegen und zu den Daten Stellung zu nehmen, auf denen die Entscheidung beruht. Dadurch soll unter anderem verhindert werden, dass die betroffene Person fälschlicherweise einen rechtlichen oder tatsächlichen Nachteil erleidet, weil 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 Informations- und Anhörungspflicht lässt die Vertragsfreiheit indes unberührt. Sollte der Verantwortliche der Anhörungspflicht nicht nachkommen, kann die betroffene Person diesen Anspruch mit einem Auskunftsgesuch nach Artikel 20 geltend machen.

Das Gesetz legt den Zeitpunkt der Information und Anhörung nicht fest. Dementsprechend kann die betroffene Person vor der Entscheidung oder nachträglich informiert und angehört werden. 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, soweit dies für die betroffene Person nicht mit zusätzlichen Kosten (z.B. Verfahrenskosten) verbunden ist.

Absatz 3 Ausnahmen

Nach Absatz 3 entfällt die Informations- und Anhörungspflicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht. Für Bundesorgane ist darunter ein Gesetz im Sinne von Artikel 27 des VE zu verstehen.

Ein Verstoß gegen die Informationspflicht wird sanktioniert (siehe Art. 50 Abs. 1 Bst. a und b Ziff 1 und 2 VE-DSG).

8.1.3.4 Art. 16 Datenschutz-Folgenabschätzung

Artikel 16 VE-DSG führt neu die Pflicht zum Erstellen einer Datenschutz-Folgenabschätzung ein. Diese Bestimmung verwirklicht die Anforderungen von Artikel 8^{bis} 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 Absatz 2 von Artikel 16. 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 verringern. 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 Einführung der Datenschutz-Folgenabschätzung ist insbesondere für die Bundesorgane keine Neuheit und hat in dieser Hinsicht kaum praktische Konsequenzen. Denn Bundesorgane sind bereits heute verpflichtet, dem Datenschutzverantwortlichen bzw. 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.

Absatz 1 Gründe für die Datenschutz-Folgenabschätzung

Nach Absatz 1 muss der Verantwortliche (bzw. der Auftragsbearbeiter) eine Datenschutz-Folgenabschätzung durchführen, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Der Verantwortliche ist dadurch verpflichtet, eine Prognose darüber zu machen, welche

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 und 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 Identität⁹⁷. 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 erhöhten Risiko ist grundsätzlich auszugehen, wenn die spezifischen Eigenschaften der geplanten Datenbearbeitung darauf schliessen lassen, dass die Verfügungsfreiheit der betroffenen Person über ihre Daten erheblich eingeschränkt wird oder werden kann. Dies ist insbesondere der Fall, wenn besonders persönlichkeitsnahe Daten in umfassender Form bearbeitet werden, wodurch die Identifikation der betroffenen Person sowie spezifischer Eigenschaften möglich ist. Das erhöhte 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. bei wenn die ausländische Gesetzgebung keinen angemessenen Schutz gewährleistet) oder wenn eine grosse oder gar unbegrenzte Anzahl Personen auf die Daten zugreifen können. Weitere Indizien für ein erhöhtes Risiko können sein, ob die gesammelten Daten im Missbrauchsfall die Persönlichkeit, die Würde oder das persönliche Fortkommen der betroffenen Person einschränken könnten. Auch eine systematische Überwachung einer Person und deren Verhaltens (z. B. des E-Mailverkehrs) oder einer öffentlichen Zone (z.B. eines belebten Platzes) kann ein erhöhtes Risiko darstellen. Führt die fragliche Datenbearbeitung voraussichtlich zu einem erhöhten Risiko, muss eine Datenschutz-Folgenabschätzung durchgeführt werden.

Absatz 2 Inhalt der Datenschutz-Folgenabschätzung

Nach Absatz 2 muss in der Datenschutz-Folgenabschätzung zunächst die geplante Bearbeitung dargelegt werden. So müssen beispielsweise die verschiedenen Bearbeitungsvorgänge, der Zweck der Bearbeitung oder die Aufbewahrungsdauer aufgeführt werden. Im Weiteren muss gemäss Absatz 2 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 die Risikobewertung, die bereits im Hinblick auf die Notwendigkeit einer Datenschutz-Folgenabschätzung vorzunehmen ist. So ist darzustellen, in welcher Hinsicht von der fraglichen Datenbearbeitung ein erhöhtes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person ausgeht und wie dieses Risiko zu bewerten ist. Schliesslich muss die

⁹⁷ Vgl. hierzu DIGGELMANN OLIVER, in: Waldmann/Belser/Epiney (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015, Art. 13 BV N 7.

Datenschutz-Folgenabschätzung nach Absatz 2 erläutern, mit welchen Massnahmen diese Risiken reduziert werden. Massgebend dafür sind insbesondere die Grundsätze nach Artikel 4 VE-DSG, aber auch die Pflicht zum Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen (Art. 18 VE-DSG) können relevant sein. Bei diesen Massnahmen darf auch eine Abwägung zwischen den Interessen der betroffenen Person und denjenigen des Verantwortlichen oder des Auftragsbearbeiters erfolgen. Diese Interessenabwägung ist in der Datenschutz-Folgenabschätzung ebenfalls aufzuführen und entsprechend zu begründen.

Absatz 3 Mitteilung an den Beauftragten

Nach Absatz 3 muss der Verantwortliche (bzw. der Auftragsbearbeiter) den Beauftragten über die Ergebnisse der Datenschutz-Folgenabschätzung sowie die Massnahmen informieren, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern. 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). Sie wird namentlich in den VE aufgenommen, weil sie dem Beauftragten erlaubt, präventiv und beratend tätig zu sein. Dies ist nicht zuletzt auch für den Verantwortlichen effizienter, da mögliche datenschutzrechtliche Schwierigkeiten bereits in einem frühen Stadium der Datenbearbeitung behoben werden können.

Absatz 4 Einwände des Beauftragten

Gemäss Absatz 4 teilt der Beauftragte dem Verantwortlichen innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit, falls er gegen die vorgesehenen Massnahmen Einwände hat. Nachdem er über eine Datenschutz-Folgenabschätzung benachrichtigt worden ist, überprüft der Beauftragte lediglich, ob die vorgeschlagenen Massnahmen zum Schutz der Grundrechte und der Persönlichkeit der betroffenen Person ausreichend sind. Hingegen nimmt er keine umfassende Prüfung des gesamten Bearbeitungsvorgangs vor; diese Prüfung ist bereits Gegenstand der Datenschutz-Folgenabschätzung. Erhält der Verantwortliche innerhalb der Dreimonatsfrist keine Nachricht vom Beauftragten, kann er grundsätzlich davon ausgehen, dass der Beauftragte keine Einwände gegen die vorgeschlagenen Massnahmen zum Grundrechtsschutz hat. Dem Datenschutzbeauftragten bleibt es indes unbenommen, zu einem späteren Zeitpunkt eine Untersuchung zu eröffnen, wenn die Voraussetzungen nach Artikel 41 VE-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.

Ein Verstoß gegen die Pflicht zur Erstellung und Mitteilung einer Datenschutz-Folgenabschätzung wird sanktioniert (siehe Art. 50 Abs. 1 Bst. c, 51 Abs. 1 Bst. d VE-DSG).

8.1.3.5 Art. 17 Meldung von Verletzungen des Datenschutzes

Artikel 17 VE-DSG führt die Pflicht zur Meldung von Verletzungen des Datenschutzes ein. Diese Bestimmung verwirklicht die Anforderungen von Artikel 7 Absatz 2 E-SEV 108 sowie von Artikel 30 der Richtlinie (EU) 2016/680. Der Artikel 33 der Verordnung (EU) 2016/679 enthält eine ähnliche Regelung.

Absatz 1 Begriff und Grundsatz

Nach Absatz 1 meldet der Verantwortliche dem Datenschutzbeauftragten eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person. Dabei ist vom Begriff der Bearbeitung im Sinne von Artikel 3 Buchstabe d VE-DSG auszugehen. Demzufolge gilt jede Art der unbefugten Bearbeitung als Verletzung des Datenschutzes, so dass beispielsweise auch die unbefugte Löschung eingeschlossen ist. Die Verletzung kann durch Dritte erfolgen, aber auch durch Mitarbeiter, die ihre Kompetenzen missbrauchen oder überschreiten. Durch eine unbefugte Datenbearbeitung kann die betroffene Person die Kontrolle über ihre Daten verlieren, oder

diese Daten werden missbraucht. Darüber hinaus kann eine unbefugte Datenbearbeitung auch zu einer Verletzung der Persönlichkeit der betroffenen Person führen, zum Beispiel indem geheime Informationen über sie bekannt werden. Dementsprechend gilt nach Artikel 23 Absatz 2 Buchstabe a eine Verletzung der Datensicherheit als Persönlichkeitsverletzung.

Auf diese Gefährdungen kann die betroffene Person nur reagieren, wenn sie von der Verletzung des Datenschutzes 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 2 an die betroffene Person. Die Meldung hat ab dem Zeitpunkt der Kenntnisnahme unverzüglich zu erfolgen. Der Verantwortliche muss grundsätzlich rasch 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 kann nur unterbleiben, wenn die Verletzung des Datenschutzes voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt. Dadurch soll verhindert werden, dass selbst unbedeutende Verletzungen gemeldet werden müssen. Die Ausnahme ist jedoch eng auszulegen. Der Verantwortliche muss eine Prognose in Bezug auf die möglichen Auswirkungen der Verletzung für die betroffene Person stellen und kann die Meldung nur unterlassen, wenn von der unbefugten Datenbearbeitung höchstwahrscheinlich keine Gefahr ausgeht.

Absatz 2 Mitteilung an die betroffene Person

Grundsätzlich muss die betroffene Person nicht benachrichtigt werden. Gemäss Absatz 2 muss sie jedoch über die Verletzung des Datenschutzes informiert werden, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt. Dabei besteht ein gewisser Ermessensspielraum. Bedeutsam ist insbesondere, ob durch die Information die Risiken für die Persönlichkeit und 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.

Absatz 3 und 4

Der Verantwortliche kann nach Absatz 3 die Meldung der betroffenen Person einschränken, aufschieben oder darauf verzichten, wenn einer der Gründe von Artikel 14 Absätze 3 und 4 vorliegt (vgl. Ziff. 8.1.3.2).

Eine unbefugte Datenbearbeitung kann auch beim Auftragsbearbeiter erfolgen. Daher ist er nach Absatz 4 verpflichtet, dem Verantwortlichen jede unbefugte Datenbearbeitung zu melden. Es ist es am Verantwortlichen, anschliessend eine Risikoabschätzung vorzunehmen und darüber zu entscheiden, inwieweit eine Meldepflicht gegenüber dem Beauftragten und der betroffenen Person besteht.

Ein Verstoss gegen die Meldepflicht bei einer Verletzung des Datenschutzes wird sanktioniert (siehe Art. 50 Abs. 2 Bst. d VE-DSG).

8.1.3.6 Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Artikel 18 VE-DSG führt die Pflicht zum Datenschutz durch Technik sowie durch datenschutzfreundliche Voreinstellungen ein. Die Bestimmung verwirklicht die Anforderungen von Artikel 8 Ziffer 3 E-SEV 108 sowie von Artikel 20 Absatz 1 der Richtlinie (EU) 2016/680. Der Artikel 25 der Verordnung (EU) 2016/679 enthält eine ähnliche Regelung.

Absatz 1 Datenschutz durch Technik

Absatz 1 verlangt vom Verantwortlichen und dem Auftragsbearbeiter, angemessene Massnahmen zu treffen, die bereits ab der Planung einer Datenbearbeitung das Risiko von

Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen vorbeugen. 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 Empfehlungen der guten Praxis) reduzieren, indem technische Vorkehrungen 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 Vorkehrungen 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 4 VE-DSG entsprechen. 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 4 VE-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.

Für die Datenbearbeitung durch Bundesorgane ist anzumerken, dass die Pflicht zum Datenschutz durch Technik geringe Auswirkungen haben dürfte, da die diese schon heute den von ihnen bezeichneten Datenschutzverantwortlichen oder, falls keine solche oder kein solcher besteht, dem Beauftragten unverzüglich alle Projekte zur automatisierten Bearbeitung von Personendaten melden müssen, damit die Erfordernisse des Datenschutzes bereits bei der Planung berücksichtigt werden (Art. 20 Abs. 2 VDSG).

Absatz 2 Datenschutzfreundliche Voreinstellungen

Gemäss *Absatz 2* sind der Verantwortliche und der Auftragsbearbeiter verpflichtet, mittels geeigneter Voreinstellungen dafür zu sorgen, dass grundsätzlich nur diejenigen Daten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind. 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 deutlich. So gehören entsprechende Voreinstellungen regelmässig zur datenschutzfreundlichen Ausgestaltung eines gesamten Systems. Spezifisch an datenschutzfreundlichen Voreinstellungen sind jedoch die Einflussmöglichkeiten der betroffenen Person. Während sie 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. 4 Abs. 6 VE-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 und der Auftragsbearbeiter können insbesondere durch die Zertifizierung oder eine Datenschutz-Folgenabschätzung aufzeigen, dass sie den Verpflichtungen nach den Absätzen 1 und 2 der Bestimmung nachkommen.

Ein Verstoß gegen die Pflichten nach Artikel 18 wird sanktioniert (vgl. Art. 51 Abs. 1 Bst. e VE-DSG).

8.1.3.7 Art. 19 Weitere Pflichten

Artikel 19 VE-DSG enthält verschiedene weitere Pflichten des Verantwortlichen bzw. des Auftragsbearbeiters.

Buchstabe a Dokumentationspflicht

Buchstabe a verpflichtet den Verantwortlichen und den Auftragsbearbeiter, seine Datenbearbeitungsvorgänge zu dokumentieren. Diese Dokumentationspflicht entspricht den Anforderungen von Artikel 8^{bis} Absatz 1 E-SEV 108 sowie von Artikel 25 der Richtlinie (EU) 2016/680. Der Artikel 30 der Verordnung (EU) 2016/679 enthält eine ähnliche Regelung. Dadurch wird für Private die bisherige Verpflichtung ersetzt, Datensammlungen beim Beauftragten zu registrieren (Bundesorgane müssen gemäss Art. 36 VE-DSG weiterhin ein Register führen). Die Meldung an das Register ist bürokratisch und mit einem erheblichen Verwaltungsaufwand auf Seiten des Verantwortlichen verbunden. Zugleich ist sie von geringem praktischem Nutzen. Denn für private Personen bestanden bereits bisher verschiedene Ausnahmen von der Registrierung. Die Dokumentationspflicht gilt hingegen einheitlich für alle Datenbearbeitungsvorgänge. Mit weniger Aufwand kann dadurch eine gleichmässiger Dokumentation aller privaten Datenbearbeitungsvorgänge erreicht werden. Das Gesetz sieht nicht vor, welche Angaben dokumentiert werden müssen; dies wird in der Verordnung konkretisiert. Die Dokumentation muss jedoch so ausgestaltet sein, dass der Verantwortliche und der Auftragsbearbeiter ihren Informations- und Meldepflichten nachkommen können. Beispielsweise müssen auch Verletzungen des Datenschutzes nach Artikel 17 dokumentiert werden. So bildet die Dokumentationspflicht auch ein zentrales Element zur Verwirklichung einer transparenten Datenbearbeitung. Ein Verstoß gegen die Dokumentationspflicht wird sanktioniert (vgl. Art. 51 Bst. f VE-DSG).

Buchstabe b Weitere Informationspflichten

Gemäss Buchstabe b sind der Verantwortliche und der Auftragsbearbeiter verpflichtet, Empfänger von Daten über eine allfällige Berichtigung, Löschung, Vernichtung, Verletzung des Datenschutzes oder Einschränkung der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 zu informieren. Diese Pflicht ergänzt verschiedene Datenschutzregeln für den Fall, dass Daten an Dritte weitergegeben wurden. Sie ist in Artikel 16 Absatz 5 der Richtlinie 2016/680 und Artikel 19 der Verordnung (EU) 2016/679 vorgesehen. So ist die Bearbeitung unzutreffender Daten grundsätzlich persönlichkeitsverletzend, weshalb sich jeder, der Daten bearbeitet, vergewissern muss, ob die Daten richtig sind (Art. 4 Abs. 5 VE-DSG). Auch die Löschung, Vernichtung oder Einschränkung der Bearbeitung impliziert grundsätzlich, dass die Bearbeitung der Daten nicht mehr rechtmässig ist. Die Informationspflicht gemäss dieser Bestimmung stellt sicher, dass diese Daten nicht durch Dritte, an welche die Daten übermittelt wurden, weiter bearbeitet werden, weil sie keine Kenntnis vom entsprechenden Vorgang haben.

Der Verantwortliche bzw. Auftragsbearbeiter kann von der Information absehen, wenn die Mitteilung unmöglich ist oder nur mit unverhältnismässigem Aufwand erfolgen kann. Diese Ausnahme ist restriktiv zu verstehen. Es darf nicht leichthin angenommen werden, die Mitteilung sei unmöglich oder der Aufwand sei unverhältnismässig. Der Verantwortliche oder Auftragsbearbeiter muss zumindest versucht haben, die betreffenden Empfänger zu informieren und muss dabei auf konkrete, nur mit erheblichem Einsatz überwindbare Schwierigkeiten gestossen sein. In Bezug auf die Verhältnismässigkeit des Aufwands ist zudem der Inhalt der fraglichen Mitteilung zu berücksichtigen. Je bedeutsamer die

Berichtigung, Löschung, Vernichtung oder Einschränkung für den Schutz der betroffenen Person ist, je gravierender die Verletzung des Datenschutzes ist, umso grösser ist der Aufwand, der vom Verantwortlichen oder Auftragsbearbeiter erwartet werden kann.

Ein Verstoss gegen diese Pflichten wird sanktioniert (Art. 50 Abs. 3 Bst. a VE-DSG).

8.1.4 Rechte der betroffenen Person

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

8.1.4.1 Art. 20 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 unmündige oder entmündigte Personen selbständig, ohne Zustimmung ihres gesetzlichen Vertreters, geltend machen können. Aus dem Charakter des höchstpersönlichen Rechts ergibt sich auch, dass gemäss niemand im Voraus auf das Auskunftsrecht verzichten kann (Art. 20 Abs. 6 VE-DSG).

Absatz 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 aktuellen Recht.

Absatz 2 Mitzuteilende Informationen

Die betroffene Person erhält nach Absatz 2 zunächst diejenigen Informationen, die ihr aufgrund der Informationspflicht mitgeteilt werden müssen (vgl. Art. 13 Abs. 2 bis 4 VE-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. In jedem Fall müssen ihr die Informationen in den Buchstaben a bis c mitgeteilt werden. Dies sind zunächst die Identität und die Kontaktdaten des Verantwortlichen (Bst. a), die bearbeiteten Personendaten (Bst. b) und der Zweck der Bearbeitung (Bst. c). Der betroffenen Person muss darüber hinaus mitgeteilt werden, wie lange die Daten aufbewahrt werden, oder, wenn dies nicht möglich ist, nach welchen Kriterien die Dauer festgelegt wird (Bst. d). Diese Information erlaubt der betroffenen Person insbesondere nachzuvollziehen, ob der Verantwortliche die Daten entsprechend den Grundsätzen in Artikel 4 VE-DSG aufbewahrt. Da die Aufbewahrungsdauer im Rahmen der Informationspflicht nicht immer mitgeteilt werden muss, soll die betroffene Person sie im Rahmen des Auskunftsrechts in jedem Fall erhalten. Ebenfalls wird der betroffenen Person mitgeteilt, ob eine automatisierte Einzelentscheidung vorliegt (Bst. e), wobei sie zusätzlich die Informationen nach Absatz 3 erhalten muss. Schliesslich erhält die betroffene Person die verfügbaren Angaben über die Herkunft der Daten (Bst. f). Diese Pflicht besteht bereits nach geltendem Recht.

Absatz 3 Mitteilung bei einer Entscheidung aufgrund der Datenbearbeitung

Wenn aufgrund einer Datenbearbeitung eine Entscheidung erfolgt ist, erhält die betroffene Person nach Absatz 3 zusätzlich Informationen über das Ergebnis der Entscheidung, deren Zustandekommen sowie deren Auswirkungen und Tragweite. Dies gilt insbesondere im Falle einer automatisierten Einzelentscheidung, wie beispielsweise die Gewährung eines Kredits oder den Abschluss einer Versicherung, die alleine auf der Analyse der Finanz- oder Gesundheitsdaten der betroffenen Person beruht (vgl. Ziff. 8.1.3.3). Dabei gehen die Informationen über diejenigen hinaus, welche die betroffene Person nach Artikel 15 VE-DSG erhält. Mit Hilfe des Auskunftsrechts soll sie erweiterte Informationen zur fraglichen Entscheidung erhalten. Dadurch soll die betroffene Person nachvollziehen können, wie die Entscheidung zustande gekommen ist und welche Folgen sie nach sich zieht. Das heisst, ihr muss mitgeteilt werden, welche Daten hierfür berücksichtigt wurden und welche Bedeutung diese für die Entscheidung haben.

Der Verantwortliche kann die Auskunft nach Artikel 21 verweigern, einschränken oder aufschieben. Private Verantwortliche können in diesem Rahmen auch eigene Interessen wie zum Beispiel die Wahrung von Geschäftsgeheimnissen geltend machen. Dabei ist jedoch eine differenzierte Interessenabwägung nötig. So muss der Verantwortliche einen allfälligen Algorithmus, der zur fraglichen Entscheidung geführt hat, nicht im Einzelnen offenlegen und kann sich in dieser Hinsicht auf die Wahrung von Geschäftsgeheimnissen berufen. Aber er muss der betroffenen Person das Ergebnis der Einzelentscheidung in einer Weise begründen, dass diese nachvollziehen kann, wie es aufgrund der fraglichen Daten zu diesem bestimmten Ergebnis kam. Darüber hinaus muss die betroffene Person Auskunft darüber erhalten, wie sich die Entscheidung auf ihre rechtliche oder tatsächliche Stellung auswirkt und welche Bedeutung der Entscheidung hierbei zukam. Falls die betroffene Person erst aufgrund des Auskunftsrechts vom Vorliegen einer automatischen Einzelentscheidung erfahren hat, muss sie darüber hinaus die Gelegenheit erhalten, sich dazu zu äussern (vgl. Art. 15 Abs. 2 VE-DSG).

Absatz 4 und 5

Aus dem geltenden Recht unverändert übernommen wurde Absatz 4, wonach der Verantwortliche Informationen über die Gesundheit der betroffenen Person durch einen von ihr bezeichneten Arzt mitteilen lassen kann. Der Absatz erfuhr lediglich eine redaktionelle Überarbeitung.

Abgesehen von redaktionellen Änderungen bleibt Absatz 5 ebenfalls unverändert. Demnach bleibt der Verantwortliche grundsätzlich auskunftspflichtig, selbst wenn er die Bearbeitung an einen Auftragsbearbeiter delegiert.

Ein Verstoß gegen die Pflichten nach Artikel 20 VE-DSG wird sanktioniert (siehe Art. 50 Abs. 1 Bst. a VE-DSG).

8.1.4.2 Art. 21 Einschränkung des Auskunftsrechts

Der Verantwortliche kann gemäss Absatz 1 die Auskunft unter den Voraussetzungen nach Artikel 14 Absätze 3 und 4 des VE verweigern, einschränken oder aufschieben. Hierfür kann auf die Kommentierung von Artikel 14 VE-DSG verwiesen werden (vgl. Ziff. 8.1.3.2). Die Gründe für die Einschränkung des Auskunftsrechts sind dieselben geblieben; sie werden im VE jedoch neu im Zusammenhang mit der Informationspflicht aufgezählt.

Falls der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies gemäss Absatz 2 entsprechend begründen. Als Gründe kommen grundsätzlich nur die Voraussetzungen nach Artikel 14 Absätze 3 und 4 in Frage. 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. Neu sieht Absatz 2 in Satz 2 vor, dass das Bundesorgan auf eine Begründung verzichten kann, wenn dadurch die Interessen gemäss Artikel 14 Absatz 4 Buchstabe b des VE gefährdet sein könnten. Diese Bestimmung verhindert, dass das Bundesorgan durch die Begründung gerade das preisgeben muss, was durch die Verweigerung der Auskunft verschwiegen werden soll.

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.

8.1.4.3 Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende

Art. 22 VE-DSG übernimmt den aktuellen Art. 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.⁹⁸ Darüber hinaus muss es sich um ein periodisch erscheinendes

⁹⁸ BARRELET DENIS/WERLY STÉPHANE, Droit de la communication, 2. Aufl., Bern 2011, N 1769.

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.⁹⁹

Die Einschränkung des Auskunftsrechts für Medienschaffende wird, abgesehen von redaktionellen Anpassungen, unverändert übernommen.

8.1.5 Besondere Bestimmungen für die Bearbeitung von Daten durch private Personen

Der 5. Abschnitt 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 23 VE-DSG konkretisiert Persönlichkeitsverletzungen im Bereich des Datenschutzes, Artikel 24 VE-DSG definiert spezifische Rechtfertigungsgründe und Artikel 25 VE-DSG regelt die Rechtsansprüche, die 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 Sektor ihre Rechte kaum wahrnehmen. Dies wird hauptsächlich auf die Kostenrisiken eines Prozesses zurückgeführt¹⁰⁰, welche durch Anpassungen bei der Kostenregelung im Zivilprozess aufgefangen werden sollen (vgl. Ziff. 8.2.9).

8.1.5.1 Art. 23 Persönlichkeitsverletzungen

Der Begriff der Persönlichkeitsverletzung ist in Artikel 28 ZGB nicht definiert. Artikel 23 des Entwurfs konkretisiert diesen Begriff für Verletzungen der Persönlichkeit durch Datenbearbeitung.

Absatz 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.

Absatz 2 Fiktionen von Persönlichkeitsverletzungen

Absatz 2 nimmt u.a. Bezug auf die Einhaltung der Grundsätze der Datenbearbeitung und fingiert für vier Konstellationen eine Persönlichkeitsverletzung. Nach Buchstabe a liegt eine Persönlichkeitsverletzung vor, wenn Daten entgegen den Grundsätzen der Artikel 4, 5, 6 und 11 VE-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, wird nun jedoch durch Artikel 8 Buchstabe d E-SEV 108 verlangt. Nach Buchstabe c liegt ebenfalls eine Persönlichkeitsverletzung vor, wenn besonders schützenswerte Daten an Dritte bekanntgegeben werden. Schliesslich erfolgt nach Buchstabe d eine Persönlichkeitsverletzung im Falle von Profiling ohne ausdrückliche Einwilligung der betroffenen Person.

⁹⁹ BARRELET DENIS/WERLY STÉPHANE, Droit de la communication, 2. Aufl., Bern 2011, N 1420.

¹⁰⁰ Vgl. S. 90 f. und 219 des Schlussberichts zur Evaluation des Bundesgesetzes über den Datenschutz vom 10. März 2011.

Die Aufzählung ist nicht abschliessend. Das heisst, eine Persönlichkeitsverletzung durch die Bearbeitung von Daten kann auch auf anderem Wege als durch die Verwirklichung dieser vier 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 erfolgte¹⁰¹. 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 VE werden die Rechtfertigungsgründe nun ausschliesslich in Artikel 24 geregelt.

Absatz 3 Keine Persönlichkeitsverletzung

Nach Absatz 3 liegt hingegen keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht hat und deren Bearbeitung nicht ausdrücklich untersagt hat. Diese Regelung, die identisch aus dem bisherigen Recht übernommen wurde, ist folgerichtig. Denn die individuelle Verfügungsfreiheit über personenbezogene Daten wird unter diesen Umständen nicht verletzt. Die Bestimmung kommt indes nur zum Tragen, wenn die Bearbeitung dieser Daten auch rechtmässig erfolgt, d. h., insbesondere die Grundsätze der Artikel 4, 5, 6 und 11 eingehalten werden.

8.1.5.2 Art. 24 Rechtfertigungsgründe

Artikel 24 konkretisiert die Rechtfertigungsgründe für persönlichkeitsverletzende Datenbearbeitungen. Die Norm bleibt abgesehen von kleinen Änderungen unverändert.

Absatz 1 Grundsatz

Absatz 1 hält den Grundsatz fest, wonach jede Persönlichkeitsverletzung – d. h. jede persönlichkeitsverletzende Datenbearbeitung – grundsätzlich widerrechtlich ist, 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. 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 der bearbeitenden Person liegt ein Interesse an der Datenbearbeitung vor. Nur wenn das Interesse an der Datenbearbeitung überwiegt gegenüber dem Interesse der betroffenen Person, ist die Persönlichkeitsverletzung gerechtfertigt.

Absatz 2 Mögliche überwiegende Interessen der bearbeitenden Person

Absatz 2 konkretisiert, wann möglicherweise ein überwiegendes Interesse der bearbeitenden Person gegeben sein kann. Die Formulierung macht deutlich, dass es sich dabei nicht um absolute Rechtfertigungsgründe handelt. Massgebend ist vielmehr die Interessenabwägung im Einzelfall.

Dieser Katalog bleibt weitgehend unverändert zum bisherigen Recht. Die Aufzählung ist nicht abschliessend. Sie 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 namentlich 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 anschliessend die Interessen des konkreten Einzelfalls gegeneinander abgewogen werden.

¹⁰¹ Vgl. hierzu BGE 136 II 508 E. 5.2.3.

Absatz 2 Buchstabe c Prüfung der Kreditwürdigkeit

Neu setzt Buchstabe c Ziffer 3 voraus, dass die betroffene Person volljährig ist. Diese Anpassung erfolgt, um den Schutz von Minderjährigen zu verbessern, was eines der Ziele der Revision ist. Grundsätzlich dürfte sich die Tragweite dieser Änderung aufgrund der beschränkten Handlungsfähigkeit minderjähriger Personen in Grenzen halten. Allerdings hat sich in der Praxis gezeigt, dass dennoch Missbräuche vorkommen können, wie dies zum Beispiel das Verfahren des Beauftragten gegen das Unternehmen Moneyhouse deutlich macht.¹⁰²

Absatz 2 Buchstabe e Bearbeitung zu Forschungszwecken

Leicht verschärft wurde der Rechtfertigungsgrund der Bearbeitung zu nicht personenbezogenen Zwecken, insbesondere in der Forschung, Planung und Statistik, in Buchstabe e. Die Verwendung von Daten zu diesen Zwecken ist neu nur zulässig, wenn die Voraussetzungen der Ziffern 1 bis 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 ist müssen die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt. Wenn es zur Datenbearbeitung für Forschung, Planung oder Statistik nicht mehr erforderlich ist, über personenbezogene Daten zu verfügen, müssen diese anonymisiert werden. Dies ergibt sich grundsätzlich bereits aus der Vorschrift in Artikel 4 Absatz 4. Ein Verstoss gegen dieselbe führt gemäss Artikel 23 Absatz 2 Buchstabe a zu einer Persönlichkeitsverletzung, die sich durch einen der Gründe in Artikel 24 rechtfertigen lässt. Durch die Vorschrift in Artikel 24 Absatz 2 Buchstabe e Ziffer 1 ist es nun nicht mehr möglich, einen Verstoss gegen Artikel 4 Absatz 4 mit der Bearbeitung zu Zwecken der Forschung, Planung oder Statistik zu rechtfertigen.

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 23 Absatz 2 Buchstabe c zu einer Persönlichkeitsverletzung, die sich durch einen der Gründe in Artikel 24 rechtfertigen lässt. Die Vorschrift in Ziffer 2 schliesst es nunmehr aus, die Bekanntgabe nicht anonymisierter, besonders schützenswerter Personendaten 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).

8.1.5.3 Art. 25 Rechtsansprüche

Artikel 25 regelt die Rechtsansprüche, welche die betroffene Person gegenüber privaten Personen geltend machen kann.

Absatz 1 Klagen

Absatz 1 enthält die Verweisung auf die Klagen nach Artikel 28 ff. ZGB, welche bereits im bisherigen Recht bestand. Analog zu Artikel 28a 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 28a 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 Berichtigung, Löschung oder Vernichtung von Daten verlangen.

¹⁰² Vgl. <https://www.edoeb.admin.ch/datenschutz/00626/00747/01022/index.html?lang=de>. Das Verfahren ist noch nicht abgeschlossen.

Obschon es sich implizit bereits aus dem bisherigen Recht ergab, wurde im VE 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 Vergessen bzw. Vergessenwerden», wie es generell aus dem zivilrechtlichen Persönlichkeitsschutz abgeleitet wird.¹⁰³ Demnach wäre auch in der Schweiz beispielsweise ein ähnlicher Entscheid möglich, wie ihn der Europäische Gerichtshof gegenüber Google gefällt hat.¹⁰⁴ Ein solches Recht auf Vergessen gilt indessen nicht absolut.¹⁰⁵ Vielmehr wird in der Rechtsprechung grundsätzlich das Interesse der betroffenen Person abgewogen gegen die Meinungs- und Informationsfreiheit, aus denen sich regelmässig ein 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.

Absatz 2 Bestreitungsvermerk

Absatz 2 enthält den so genannten Bestreitungsvermerk, der unverändert aus dem bisherigen Recht übernommen wurde. Demnach kann bei Daten ein entsprechender Vermerk angebracht werden, wenn weder die Richtigkeit noch die Unrichtigkeit der Daten dargetan werden kann. Darüber hinaus kann die betroffene Person in diesem Fall verlangen, dass die Datenbearbeitung eingeschränkt wird. Dieses Recht auf Einschränkung der Datenbearbeitung entspricht den Anforderungen von Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680; eine ähnliche Regelung ist in Artikel 18 (EU) 2016/679 enthalten. Im E-SEV 108 ist dies nicht vorgesehen. Die Einschränkung der Bearbeitung bedeutet, dass die bestrittenen Daten gekennzeichnet werden, damit ihre künftige Bearbeitung darauf beschränkt bleibt, ihre Richtigkeit oder Unrichtigkeit festzustellen. Die Kennzeichnung muss klar sein. Sie kann in der Praxis bedeuten, dass die Daten vorübergehend in ein anderes Bearbeitungssystem verschoben werden, dass den Benutzerinnen und Benutzern der Zugriff auf die Daten verunmöglicht wird oder dass veröffentlichte Daten vorübergehend von einer Website entfernt werden. In Systemen für eine automatisierte Datenbearbeitung sollte die Einschränkung der Bearbeitung grundsätzlich mit technischen Mitteln gewährleistet werden, so dass die Daten nicht Gegenstand weiterer Bearbeitungen sein können und nicht verändert werden.

Absatz 3 Mitteilung an Dritte oder Veröffentlichung

Absatz 3 sieht wie das bisherige Recht vor, dass das Urteil, die Berichtigung, die Vernichtung, das Verbot der Bearbeitung bzw. der Bekanntgabe an Dritte oder der Bestreitungsvermerk Dritten mitgeteilt wird oder veröffentlicht wird. Diese Regelung konkretisiert Artikel 28a Absatz 2 ZGB im Bereich des Datenschutzes.

Aufgehoben wird hingegen die Bestimmung betreffend das vereinfachte Verfahren für Auskunftsbegehren. Diese Regelung ist mit Einführung der ZPO¹⁰⁶ obsolet geworden.

8.1.6 Besondere Bestimmungen für die Bearbeitung von Daten durch Bundesorgane

8.1.6.1 Art. 26 Verantwortliches Organ und Kontrolle

Im Vergleich zu Artikel 16 DSG erfährt Artikel 26 wenige Änderungen. In Absatz 1 wird aus redaktionellen Gründen «in Erfüllung seiner Aufgaben» entfernt.

Aus denselben Gründen wird in Absatz 2 «besonders regeln» 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

¹⁰³ Vgl. hierzu insbesondere BGE 109 II 353; BGE 111 II 209 sowie BGE 122 II 449.

¹⁰⁴ 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.

¹⁰⁵ BGE 111 II 209 E. 3c.

¹⁰⁶ Schweizerische Zivilprozessordnung vom 19. Dezember 2008, SR 272.

dieser Änderung wird Artikel 21 der Richtlinie (EU) 2016/680 umgesetzt. Artikel 26 der Verordnung (EU) 2016/679 sieht eine analoge Regelung vor.

8.1.6.2 Art. 27 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 VE-DSG in Artikel 27 Absatz 2 die gesetzliche Grundlage für die Bearbeitung besonders schützenswerter Personendaten, das Profiling und den Erlass einer automatisierten Einzelentscheidung. In Absatz 3 sind die Ausnahmen zu den Anforderungen an die gesetzliche Grundlage vorgesehen.

Absatz 1 Gesetzliche Grundlage

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

Absatz 2 Grundlage in Gesetz im formellen Sinn

Absatz 2 präzisiert, dass eine Grundlage in einem Gesetz im formellen Sinn erforderlich ist, wenn es um die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 geht. Allerdings reicht eine Grundlage in einem Gesetz im materiellen Sinn, 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 zur Anwendung kommen kann, muss auf Gesetzesebene die Natur der Aufgaben, welche die Bearbeitung von Personendaten erfordern, ausreichend konkretisiert sein. Die zweite Voraussetzung (Bst. b) ist neu. Sie hat den Vorteil, dass sie die Tragweite des zweiten Satzes von Absatz 2 auf präzisere Weise einschränkt als die aktuelle Regelung in Artikel 17 Absatz 2 Buchstabe a DSG. Letzere ist nur ausnahmsweise anwendbar, was auch dazu führen kann, den Ermessensspielraum zu nutzen, um Ausnahmefälle anzunehmen, wo gar keine vorliegen.

Absatz 3 Ausnahmen

Absatz 3 sieht die Ausnahmen zur gesetzlichen Grundlage gemäss den Artikeln 1 und 2 vor. So kann ein Bundesorgan im Einzelfall ausnahmsweise Personendaten bearbeiten, ohne dass eine gesetzliche Grundlage vorliegt, 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. Dieser Entscheid ist nicht anfechtbar. Gemäss Buchstabe b können Bundesorgane Personendaten ohne gesetzliche Grundlage bearbeiten, wenn die betroffene Person ihre Einwilligung gemäss Artikel 4 Absatz 6 VE-DSG gibt oder wenn sie ihre Personendaten allgemein zugänglich gemacht und die Bearbeitung nicht ausdrücklich untersagt hat. 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.

8.1.6.3 Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen

Die vorliegenden Änderungen des aktuellen Artikels 17a 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 17a DSG können zudem in die künftigen Ausführungsverordnung aufgenommen werden.

Abgesehen davon, dass der Begriff «Persönlichkeitsprofile» durch «Profiling» ersetzt wird, stimmen die Voraussetzungen nach den Absätzen 1 und 2 mit jenen von Artikel 17a Absatz

1 DSG überein. Ausserdem wird in Buchstabe c präzisiert, dass eine Testphase «insbesondere aus technischen Gründen» erforderlich ist. Diese Änderung ist durch die Aufhebung von Artikel 17a 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 einigen redaktionellen Änderungen abgesehen, im Vergleich zum geltenden Recht unverändert.

8.1.6.4 Art. 29 Bekanntgabe von Personendaten

Artikel 29 VE-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 27 Absatz 1 und 2 VE-DSG entspricht. Aus dieser Präzisierung folgt, dass Artikel 29 nicht auf die in Artikel 27 Absatz 3 vorgesehenen Ausnahmen verweist. Dementsprechend sind die Fälle, in denen Bundesorgane befugt sind, Personendaten ohne gesetzliche Grundlage bekannt zu geben, in Artikel 29 Absatz 2 Buchstaben a–e VE-DSG abschliessend aufgezählt.

Der Begriff der «Personendaten» in Absatz 1 umfasst auch besonders schützenswerte Personendaten. Die Ausnahmen von Absatz 2 Buchstaben a–e gelten daher 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 27 Absatz 3 Buchstabe c VE-DSG eingefügt (vgl. Ziff. 8.1.6.2).

Artikel 29 Absatz 3 VE-DSG entspricht mit Ausnahme einer punktuellen Änderung Artikel 19 Absatz 1^{bis} DSG. Mit einer Anpassung des Wortlauts von Artikel 29 Absatz 3 soll die Koordination zwischen BGÖ und DSG verbessert werden. Dabei ist bezüglich der Voraussetzung des überwiegenden öffentlichen Interesses an der Datenbekanntgabe (Art. 29 Abs. 3 Bst. b Ve-DSG) klarzustellen, dass diese Voraussetzung nicht nur zusätzlich (alternativ), sondern auch selbstständig zu Artikel 29 Absätze 1 und 2 gilt. Vorgeschlagen wird, im Einleitungssatz von Artikel 29 Absatz 3 VE-DSG den Ausdruck «auch» (für den es in der französischen Version keine Entsprechung gibt) durch ein satzeinleitendes «Darüber hinaus/en outre» zu ersetzen, um deutlich zu machen, dass die Rechtsgrundlage nach Absatz 3 zu denen in Absatz 1 dazukommt.

Artikel 29 Absatz 4 bleibt im Vergleich zu Artikel 19 Absatz 2 DSG unverändert.

Dagegen wird die gesetzliche Grundlage für "Abrufverfahren" (Art. 19 Abs. 3 DSG) bei Bundesorganen aufgehoben, weil sie dem technologieneutralen Charakter des Datenschutzgesetzes widerspricht und im digitalen Zeitalter überholt erscheint.

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

8.1.6.5 Art. 30 Widerspruch gegen die Bekanntgabe von Daten

Diese Bestimmung bleibt, von einigen redaktionellen Änderungen abgesehen, im Vergleich zum geltenden Recht unverändert.

8.1.6.6 Art. 31 Angebot von Unterlagen an das Bundesarchiv

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

8.1.6.7 Art. 32 Bearbeiten für Forschung, Planung und Statistik

Diese Bestimmung entspricht weitgehend Artikel 22 DSGVO. Sie erfährt zwei Änderungen in Absatz 2 betreffend die Verweisungen auf die Artikel 4 Absatz 3, 27 Absatz 1 und 2 und 29 Absatz 1 VE-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.

8.1.6.8 Art. 33 Privatrechtliche Tätigkeit von Bundesorganen

Diese Bestimmung entspricht Artikel 23 DSGVO. Sie bleibt materiell unverändert.

8.1.6.9 Art. 34 Ansprüche und Verfahren

Artikel 34 entspricht weitgehend dem heutigen Artikel 25 DSGVO. Er erfährt einige kleinere Änderungen und Anpassungen. Nachfolgend werden nur diese erklärt.

Absatz 2 Bestreitungsvermerk

Absatz 2 enthält den so genannten Bestreitungsvermerk, der unverändert aus dem bisherigen Recht übernommen wurde. Demnach kann bei Daten ein entsprechender Vermerk angebracht werden, wenn weder die Richtigkeit noch die Unrichtigkeit der Daten dargetan werden kann. Darüber hinaus kann die betroffene Person in diesem Fall verlangen, dass die Datenbearbeitung eingeschränkt wird. Dieses Recht auf Einschränkung der Datenbearbeitung entspricht den Anforderungen von Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680; eine ähnliche Regelung ist in Artikel 18 der Verordnung (EU) 2016/679 enthalten. Im E-SEV 108 ist dies nicht vorgesehen. Die Einschränkung der Bearbeitung bedeutet, dass die bestrittenen Daten gekennzeichnet werden, damit ihre künftige Bearbeitung darauf beschränkt bleibt, ihre Richtigkeit oder Unrichtigkeit festzustellen. Die Kennzeichnung muss klar sein. Sie kann in der Praxis bedeuten, dass die Daten vorübergehend in ein anderes Bearbeitungssystem verschoben werden, dass den Benutzerinnen und Benutzern der Zugriff auf die Daten verunmöglicht wird oder dass veröffentlichte Daten vorübergehend von einer Website entfernt werden. In Systemen für eine automatisierte Datenbearbeitung sollte die Einschränkung der Bearbeitung grundsätzlich mit technischen Mitteln gewährleistet werden, sodass die Daten nicht Gegenstand weiterer Bearbeitungen werden können und nicht verändert werden.

Absatz 3 Begehren

Absatz 3 sieht weitere Begehren vor, welche die betroffene Person an das Bundesorgan richten kann.

Heute fließt der Anspruch der betroffenen Person, die Löschung ihrer Daten zu verlangen, implizit aus Artikel 25 DSGVO. 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 34 Absatz 3 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 25 VE-DSG eingeführt, so dass die Regelung gegenüber privaten und öffentlichen Verantwortlichen übereinstimmt (vgl. Ziff. 8.1.5.3). An der konkreten Rechtslage ändert sich indessen nichts. Vorbehalten bleibt Absatz 4.

In Buchstabe a dieser Bestimmung wird der letzte Teilsatz betreffend die Sperrung der Bekanntgabe an Dritte gelöscht, weil der Widerspruch gegen die Bekanntgabe von Daten abschliessend durch Artikel 30 VE-DSG geregelt ist.¹⁰⁷ Der Widerspruch nach Artikel 30 VE-DSG ist nicht an die widerrechtliche Bearbeitung gebunden, was bei den Ansprüchen nach Artikel 34 der Fall ist. Die Löschung hat keine praktischen Konsequenzen. Denn die

¹⁰⁷ Vgl. hierzu BANGERT JAN, Kommentar zu Art. 25/25bis DSGVO, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Auflage, Basel 2014, N 62 f.

betroffene Person, die Ansprüche nach Artikel 34 geltend macht, kann zugleich nach Artikel 30 Widerspruch gegen die Bekanntgabe an Dritte einlegen.

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 30 zu veröffentlichen. Artikel 30 sieht dies nicht vor, aber es erscheint sinnvoll, dass die betroffene Person dies zumindest im Falle der widerrechtlichen Bekanntgabe verlangen kann.

Absatz 4 Bestände öffentlicher Gedächtnisinstitutionen

Nach Absatz 4 kann die Berichtigung, Löschung oder Vernichtung von Daten nicht verlangt werden in Bezug auf die Bestände von öffentlich zugänglichen Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderen öffentlichen Gedächtnisinstitutionen. Die Bestimmung bezieht sich damit auf öffentliche Institutionen, deren Tätigkeit sich insbesondere darauf bezieht, 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. 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 4 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 nachweisen. Diese Ausnahme ist insbesondere im Hinblick auf die zunehmende Tendenz zu betrachten, umfangreiche öffentliche Archive für jedermann im Internet zugänglich zu machen. Dadurch reduziert sich der Aufwand für gezielte Recherchen, während gleichzeitig der Kreis der Personen, die auf das fragliche Archiv 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 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 Einzelfällen wäre auch denkbar, den Zugang zu einem Dokument lediglich Personen zu gewähren, die ihn für ihre wissenschaftliche oder journalistische Tätigkeit benötigen.

8.1.6.10 Art. 35 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Daten enthalten

Diese Bestimmung entspricht Artikel 25^{bis} DSG. Sie bleibt unverändert.

8.1.6.11 Art. 36 Register der Datenbearbeitungstätigkeiten

Wie in den Erläuterungen zu Artikel 19 VE-DSG aufgezeigt, wird Artikel 11 a Absatz 3 DSG, der für private Personen die Pflicht zur Anmeldung bestimmter Datensammlungen beim Beauftragten oder bei der Beauftragten vorsieht, aufgehoben und durch eine Pflicht zur Dokumentation der Datenbearbeitungen ersetzt. Dagegen wird die Pflicht der Bundesorgane, ihre Datensammlungen anzumelden, mit Ausnahme einiger Änderungen beibehalten.

So sieht Artikel 36 Absatz 1 vor, dass der Beauftragte ein Register der ihm von den Bundesorganen gemeldeten Datenbearbeitungstätigkeiten führt. Dieses Register soll wie heute im Internet der Öffentlichkeit zugänglich sein (Abs. 2). Die Pflicht des Bundesorgans, eine Datenbearbeitungstätigkeit zu melden, entspricht im Wesentlichen seiner Pflicht, eine Datensammlung anzumelden. Es handelt sich um eine terminologische Anpassung infolge der Aufhebung des Begriffs der «Datensammlung» (Art. 3 Bst. g DSG) in der vorliegenden Revision. Die neue Terminologie entspricht auch jener in Artikel 24 der Richtlinie (EU) 2016/680 und in Artikel 30 der Verordnung (EU) 2016/679.

Auch wenn Artikel 36 etwas von den europäischen Vorschriften abweicht, so führt er im Wesentlichen zum selben Ergebnis. Denn diese Bestimmung erlaubt es der Öffentlichkeit und dem Beauftragten, eine Übersicht über die Datenbearbeitungstätigkeiten der Bundesorgane zu erhalten. Der Inhalt der Meldung wird zum Grossteil jenem nach Artikel 16 VDSDG entsprechen, der gegebenenfalls mit weiteren Informationen wie denen in Artikel 24 der Richtlinie (EU) 2016/680 zu ergänzen sein wird.

Der Verwaltungsaufwand der Bundesorgane bleibt unverändert.

8.1.7 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte bzw. -beauftragter

8.1.7.1 Art. 37 Ernennung und Stellung

Das Wahlverfahren der oder des Beauftragten bleibt nach Absatz 1 unverändert, weil es mit den Anforderungen der Richtlinie (EU) 2016/680 und E-SEV 108 übereinstimmt. Was Artikel 53 der Verordnung (EU) 2016/679 angeht, so hat er denselben Wortlaut wie Artikel 43 der Richtlinie (EU) 2016/680.

Die Absätze 2, 4 und 5 bleiben im Verhältnis zum aktuellen Recht unverändert (Art. 26 Abs. 2, 4 und 5 DSG). 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 12^{bis} 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.

8.1.7.2 Art. 38 Wiederwahl 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. Artikel 54 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 enthält eine ähnliche Regelung.

Neu kann das Mandat der oder des Beauftragten nur zwei Mal erneuert werden. 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. Die oder der Beauftragte soll nicht aus Furcht, nicht wiedergewählt zu werden, in der Erfüllung des gesetzlichen Auftrags zurückgehalten werden. Das Arbeitsverhältnis endet automatisch bei Erreichen des Alters nach Artikel 21 des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG)¹⁰⁸ (Art. 10 Abs. 1 in Verbindung mit Art. 14 Abs. 1 BPG).

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

¹⁰⁸ SR 831.10

8.1.7.3 Art. 39 Nebenbeschäftigung

In Artikel 39 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 Beauftragten; die Stellvertreterin oder der Stellvertreter sowie das Sekretariat unterstehen dem BPG.

Nach Artikel 26b 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 39 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, der Verwaltung, 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.

8.1.7.4 Art. 40 Aufsicht

Absatz 1 hält den Grundsatz fest, wonach der Beauftragte die für die Überwachung der Einhaltung der Datenschutzvorschriften des Bundes zuständige Behörde ist. Er übt unabhängig und unparteiisch die Aufsicht über Private und über Bundesorgane aus. Gewisse Bundesbehörden beaufsichtigen Private oder ausserhalb der Bundesverwaltung stehende Organisationen. Dies ist etwa der Fall des Bundesamts für Gesundheit (BAG) in Bezug auf die Krankenversicherungen, der Eidgenössischen Finanzmarktaufsicht (FINMA) in Bezug auf die Banken oder andere Finanzdienstleisterinnen oder des Bundesamts für Kommunikation (BAKOM) in Bezug auf die Eidgenössische Kommunikationskommission (ComCom). Der Begriff «Organisationen ausserhalb der Bundesverwaltung» entspricht der in Art. 1 Abs. 2 Bst. e VwVG verwendeten Bezeichnung. Im Rahmen eines Aufsichtsverfahrens, das allenfalls zu einer Entscheidung der zuständigen Behörde führen kann, können sich datenschutzrechtliche Fragen stellen. Um dieser Problematik Rechnung zu tragen, sieht Abs. 2 vor, dass die Aufsichtsbehörde den Beauftragten zur Stellungnahme einlädt. Hat der Beauftragte ebenfalls ein Verfahren nach Art. 41 gegen die selbe Partei eröffnet, müssen sich die Aufsichtsbehörde und der Beauftragte auf zwei Ebenen koordinieren: 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. 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.

8.1.7.5 Art. 41 Untersuchung

Während Artikel 27 DSG dem Beauftragten die Aufgabe überträgt, die Datenbearbeitung durch Bundesorgane zu überwachen, bestimmt Artikel 29 Absatz 1 DSG, dass dieser von sich aus oder auf Meldung Dritter hin eine Untersuchung gegen eine Privatperson eröffnet, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Bst. a), Datensammlungen gemäss Artikel 11a DSG registriert werden müssen (Bst. b) oder eine Informationspflicht nach Artikel 6 Absatz 3 besteht (Bst. c). Die Überwachungskompetenzen des Beauftragten gegenüber dem Privatsektor erfüllen derzeit nicht die Anforderungen E-SEV 108. So sieht deren Artikel 12^{bis} keine Begrenzung der Ermittlungs- und Eingriffsbefugnisse der Aufsichtsbehörde gegenüber den

Verantwortlichen vor. Aus diesem Grund sind die in Artikel 29 Absatz 1 DSGVO aufgezählten Fälle zu streichen.

Die neuen Ermittlungsbefugnisse des Beauftragten sind ein entscheidendes Element im Hinblick auf Artikel 45 der Verordnung (EU) 2016/679, um sicherzustellen, dass die Europäische Kommission den Angemessenheitsbeschluss gegenüber der Schweiz erneuert bzw. aufrechterhält.

Absatz 1 Eröffnung der Untersuchung

Gemäss Artikel 40 Absatz 1 VE-DSG kann der Beauftragte von Amtes wegen oder auf Anzeige hin eine Untersuchung eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Diese Untersuchung kann sich sowohl gegen ein Bundesorgan als auch gegen eine private Person richten. Die Anzeige kann durch einen Dritten oder durch die betroffene Person erfolgen. Die Person, die Anzeige erstattet, hat im Verfahren jedoch keine Parteistellung (Art. 44 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. 5).

Artikel 40 lässt dem Beauftragten einen gewissen Handlungsspielraum, da es sich um eine Kann-Bestimmung handelt, welche diesen auch bei Anzeichen für einen Verstoß nicht zur Eröffnung einer Untersuchung verpflichtet. Es obliegt folglich dem Beauftragten, über die Zweckmässigkeit einer solchen Untersuchung zu befinden. So kann er beispielsweise auf die Eröffnung einer Untersuchung verzichten, wenn er der Auffassung ist, dass die Beratung des Verantwortlichen ausreicht, um eine problematische Situation zu beseitigen. Hingegen kann sich der Beauftragte veranlasst sehen, eine Untersuchung zu eröffnen, wenn die fraglichen Datenbearbeitungen eine grössere Anzahl von Personen betreffen und demnach ein allgemeines Interesse der Öffentlichkeit besteht. Der Beauftragte handelt mit anderen Worten, wenn in seinen Augen ein ausreichendes öffentliches Interesse für eine Untersuchung vorliegt, interveniert jedoch nicht, wenn nur die Privatsphäre einer Einzelperson betroffen ist. In letzterem Fall kann die betroffene Person bei einem Zivilgericht gegen die private Person Klage erheben oder den Beschluss des Bundesorgans bei der zuständigen Beschwerdestelle anfechten. Dies entspricht dem geltenden Recht.

Absatz 2 Mitwirkungspflichten

Absatz 2 regelt die Mitwirkungspflichten der privaten Person und des Bundesorgans. Die Verfahrenspartei hat dem Beauftragten sämtliche Auskünfte zu erteilen und alle Unterlagen zur Verfügung zu stellen, welche dieser für die Untersuchung benötigt. Da der Beauftragte dem Amtsgeheimnis nach Artikel 22 des Bundespersonalgesetzes untersteht, ist die Wahrung der Vertraulichkeit sichergestellt (Art. 37 Abs. 2 VE-DSG)¹⁰⁹. Artikel 41 Absatz 2 entspricht Artikel 27 Absatz 3 und Artikel 29 Absatz 2 DSGVO. Im Gegensatz zum geltenden Recht enthält der VE-DSG mit Artikel 50 Absatz 2 Buchstabe c eine Strafbestimmung für private Personen, die ihre Mitwirkungspflichten verletzen.

Absatz 3 Untersuchungsmassnahmen

Der Beauftragte ist im Rahmen der Untersuchung befugt, Untersuchungsmassnahmen gegen die private Person oder das Bundesorgan zu ergreifen. Diese Bestimmung erfüllt die Anforderungen von Artikel 12^{bis} 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 für die Mitgliedstaaten eine analoge Regelung vor.

Damit die Ermittlungsmassnahmen verhältnismässig sind, müssen die Voraussetzungen von Absatz 3 erfüllt sein. So kann der Beauftragte nur entsprechende Massnahmen ergreifen,

¹⁰⁹ BG 1C_41/2016 vom 22. März 2016.

wenn die private Person oder das Bundesorgan ihren Mitwirkungspflichten nicht nachkommen und die Versuche des Beauftragten, Auskünfte und Unterlagen zu erhalten, vergeblich geblieben sind. Er hat das Recht, ohne Vorankündigung die Räumlichkeiten der privaten Person oder des Bundesorgans zu inspizieren (Bst. a) und Zugang zu allen notwendigen Daten und Informationen zu verlangen (Bst. b). Zur Durchführung der Untersuchungsmassnahmen kann der Beauftragte die Amtshilfe der Behörden des Bundes und der Kantone anfordern (siehe Art. 46 VE-DSG). Die in Absatz 3 vorgesehenen Massnahmen können nur ergriffen werden, wenn eine Untersuchung eröffnet wurde.

Absatz 4 Abklärungen ausserhalb eines Untersuchungsverfahrens

Absatz 4 präzisiert, dass der Beauftragte auch ausserhalb eines Untersuchungsverfahrens überprüfen kann, ob eine private Person oder ein Bundesorgan die eidgenössischen Datenschutzvorschriften einhalten. Hier geht es beispielsweise darum, Informationen vom Verantwortlichen zu erhalten, um eine bestimmte Situation abzuklären, von welcher der Beauftragte Kenntnis erlangt hat. Im Rahmen dieser Abklärungen kann der Beauftragte den Verantwortlichen beraten. Ergeben sich aus den Abklärungen Anzeichen für einen Verstoß gegen die Datenschutzvorschriften, kann der Beauftragte eine Untersuchung nach Absatz 1 eröffnen.

8.1.7.6 Art. 42 Vorsorgliche Massnahmen

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 43 VE-DSG dem Beauftragten Verfügungskompetenzen erteilt, braucht es das Bundesverwaltungsgericht für die Anordnung vorsorglicher Massnahmen nicht mehr und die entsprechende Bestimmung kann demzufolge gestrichen werden.

Der Beauftragte hat gemäss Absatz 1 selbst die Möglichkeit, vorsorgliche Massnahmen anzuordnen, um einen Status quo zu erhalten, bedrohte rechtliche Interessen zu schützen oder Beweismittel zu sichern. Die Fälle, in denen er solche Massnahmen anordnen kann, wurden im Vergleich zum geltenden Recht erweitert. Das entscheidende Kriterium ist künftig nicht mehr nur die Gefahr für die betroffene Person, einen nicht wiedergutzumachenden Nachteil zu erleiden. Vorsorgliche Massnahmen können neu auch ergriffen werden, wenn eine Gefahr für die Untersuchung besteht, zum Beispiel durch Absprachen oder durch die Vernichtung bestimmter Beweise.

Der Beauftragte kann zum Beispiel die private Person oder das Bundesorgan anweisen, die Datenbearbeitung für die Dauer der Untersuchung zu unterbrechen, oder die Beschlagnahme von Material anordnen.

Zur Vollstreckung der vorsorglichen Massnahmen kann der Beauftragte andere Behörden des Bundes und der Kantone beiziehen (Absatz 2).

Gemäss Artikel 44 Absatz 3 kommt Beschwerden gegen Verfügungen über vorsorgliche Massnahmen des Beauftragten keine aufschiebende Wirkung zu.

8.1.7.7 Art. 43 Verwaltungsmassnahmen

Artikel 43 VE-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 (Bst. i) und die Anordnung, die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation auszusetzen (Bst. j).

Artikel 43 Absatz 1 VE-DSG entspricht weitgehend den Anforderungen von Artikel 12^{bis} Absatz 2 Buchstabe c E-SEV 108, wonach jeder Vertragsstaat die Aufsichtsbehörde mit der

Befugnis ausstatten soll, Entscheidungen zu erlassen und verwaltungsrechtliche Sanktionen zu verhängen. Allerdings schlägt der Bundesrat vor, dem Beauftragten keine Kompetenz zu geben, um Verwaltungssanktionen auszusprechen, sondern ihm vielmehr Verfügungskompetenz zu geben und die Strafbestimmungen des VE-DSG auszubauen (Ziff. 8.1.8).

Gemäss Artikel 43 Absatz 1 VE-DSG kann der Beauftragte einer privaten Person oder einem Bundesorgan auferlegen, eine gegen Datenschutzvorschriften verstossende Datenbearbeitung ganz oder teilweise zu unterbrechen, zu ändern oder abzubrechen sowie die Daten zu vernichten. Artikel 43 gewährt dem Beauftragten allerdings einen gewissen Handlungsspielraum, da es sich um eine Kann-Bestimmung handelt und dieser nicht verpflichtet ist, Verwaltungsmassnahmen zu ergreifen. So kann der Beauftragte beispielsweise, bevor er solche Massnahmen ergreift, den Verantwortlichen beraten, wie das Fehlverhalten behoben werden kann. Will der Beauftragte eine Massnahme ergreifen, hat er dabei die Verhältnismässigkeit zu wahren. Gegebenenfalls hat er die Änderung der Bearbeitung und nicht deren Abbruch anzuordnen und die Massnahme nur auf den problematischen Teil der Bearbeitung zu beschränken.

Absatz 2 erfüllt die Anforderungen von Artikel 12 Absatz 6 E-SEV 108, welcher vorsieht, dass die Aufsichtsbehörde die Bekanntgabe von Personendaten an einen anderen Staat untersagen oder unterbrechen kann.

Der Beauftragte informiert ausschliesslich die Parteien des Untersuchungsverfahrens über seinen Entscheid. Gegebenenfalls informiert er gemäss Artikel 48 VE-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. 44).

Wer einer Verfügung des Beauftragten nicht Folge leistet, kann gemäss Artikel 50 Absatz 2 Buchstabe e mit einer Busse bestraft werden.

8.1.7.8 Art. 44 Verfahren

Nach Absatz 1 unterstehen das Untersuchungsverfahren sowie jenes zum Erlass der Massnahmen nach den Artikeln 42 und 43 dem Verwaltungsverfahrensgesetz. Die private Person oder das Bundesorgan, das in der Untersuchung Partei ist, hat Anspruch auf Gewährung des rechtlichen Gehörs (Art. 29 ff. VwVG).

Absatz 2 präzisiert, dass nur das Bundesorgan sowie die private Person, gegen das bzw. die eine Untersuchung eröffnet wurde, Verfahrenspartei sein können. Dementsprechend können lediglich diese gegen Verfügungen und Massnahmen, die der Beauftragte gegen sie ergriffen hat (Art. 42 und 43), 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 25 VE-DSG tun, d. h. vor dem zuständigen Zivilgericht. Im öffentlichen Sektor muss die betroffene Person gegen das verantwortliche Bundesorgan vorgehen (Art. 34), indem sie dessen Entscheid bei der zuständigen Beschwerdeinstanz anfechtet. Dies bleibt unverändert zum geltenden Recht.

Gemäss Absatz 3 kommt Beschwerden gegen Verfügungen des Beauftragten über vorsorgliche Massnahmen nach Artikel 42 keine aufschiebende Wirkung zu.

Nach Absatz 4 kann der Beauftragte Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten, wie er dies bereits aktuell gemäss Artikel 27 Absatz 6 und 29 Absatz DSG tun kann.

8.1.7.9 Art. 45 Anzeigepflicht

Der VE verpflichtet den Beauftragten, Straftaten, von denen er in Ausübung seines Amtes Kenntnis erhält, den Strafbehörden zu melden. Stellt er zum Beispiel fest, dass eine private Person eine Straftat im Sinne der Artikel 50 ff. VE-DSG begangen hat, muss er diesen Fall

den zuständigen kantonalen Strafverfolgungsbehörden anzeigen (Art. 3 und 104 StGB). Diese Vorschrift hat mit Blick auf Artikel 22a BPG den Vorteil, dass die Anzeigepflicht auf Übertretungen ausgedehnt wird. Im Übrigen gilt Artikel 22a BPG.

Artikel 45 VE-DSG erfüllt die Anforderungen von Artikel 47 Absatz 5 der Richtlinie (EU) 2016/680 und von Artikel 12^{bis} Absatz 1 Buchstabe d E-SEV 108, die im Wesentlichen vorsehen, dass die Aufsichtsbehörde Verletzungen der Datenschutzbestimmungen den zuständigen Justizbehörden zur Kenntnis bringen darf. Die Verordnung (EU) 2016/679 sieht in Artikel 58 Absatz 5 eine analoge Regelung vor.

8.1.7.10 Art. 46 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 den Vollzug des Gesetzes 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 45 geht (Bst. b), und den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss den Artikeln 41 Absatz 3, 42 und 43 VE-DSG (Bst. c) bekannt zu geben hat.

Die in den Absätzen 1 und 2 genannte Bekanntgabe von Informationen kann spontan oder auf Anfrage erfolgen.

8.1.7.11 Art. 47 Amtshilfe zwischen schweizerischen und 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.

Absatz 1 Amtshilfeersuchen an ausländische Behörden

Gemäss Absatz 1 darf der Beauftragte eine ausländische Behörde um Amtshilfe ersuchen. Es ist dafür nicht erforderlich, dass bereits eine Untersuchung im Sinne von Artikel 41 Absatz 1 VE-DSG eröffnet wurde. Der Beauftragte muss das entsprechende Ersuchen an sein ausländisches Pendant stellen, d. h. an die im entsprechenden Land zuständige Datenschutzbehörde. Um die in Absatz 1 genannten Personendaten bekannt geben zu können, muss er sicherstellen, dass die Voraussetzungen von Artikel 5 VE-DSG erfüllt sind.

Absatz 1 Buchstaben a–g bestimmt, welche Informationen der Beauftragte der ausländischen Behörde bekannt geben darf, um Amtshilfe zu erhalten. Um die Identität der betroffenen Personen weiterleiten zu dürfen, benötigt der Beauftragte die Einwilligung jeder einzelnen Person (Abs. 1 Bst. c Ziff. 1). Für die Einwilligung gelten die Anforderungen von Artikel 4 Absatz 6 VE-DSG. Ohne Einwilligung darf die Identität nur bekannt gegeben werden, wenn dies für die Wahrnehmung der gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde unumgänglich ist (Abs. 1 Bst. c Ziff. 2). Diese Voraussetzungen entsprechen den in Artikel 29 Absatz 2 Buchstaben a und b VE-DSG vorgesehenen Fällen.

Absatz 2 Amtshilfe an ausländische Behörden

Absatz 2 regelt die Amtshilfe der Schweiz an ausländische Behörden. Die erste Voraussetzung dafür ist im Einleitungssatz von Absatz 2 enthalten, nämlich, dass die um

Hilfe ersuchende Behörde in ihrem Land eine Aufsichtsbehörde in Sachen Datenschutz sein muss. In den Buchstaben a–e des Absatzes 2 sind fünf weitere Voraussetzungen genannt. Gemäss dem Grundsatz der Zweckbindung darf die ausländische Behörde, die Informationen und Personendaten nicht für andere Zwecke verwenden als denjenigen, die im Amtshilfeersuchen genannt sind (Bst. a). Ebenfalls muss der Grundsatz der Gegenseitigkeit zwischen der Schweiz und dem ausländischen Staat gewährleistet sein (Bst. b). Ausserdem muss die ausländische Behörde die Wahrung des Amts- und Berufsgeheimnisses garantieren (Bst. c) und sich verpflichten, die erhaltenen Informationen nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln (Bst. d). Ferner hat sie die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten (Bst. e).

Der Beauftragte kann das Amtshilfeersuchen beispielsweise ablehnen, wenn die Voraussetzungen von Artikel 5 VE-DSG nicht eingehalten sind oder wenn einer der in Artikel 29 Absatz 6 VE-DSG vorgesehenen Gründe einer Bekanntgabe von Personendaten entgegensteht.

Die Bekanntgabe erfolgt von Fall zu Fall und in der Regel unverzüglich und kostenfrei.

Die Übermittlung von Informationen kann spontan oder auf Anfrage der ausländischen Behörde erfolgen (Art. 5 oder 25a VwVG).

8.1.7.12 Art. 48 Information

Absatz 1 entspricht 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. 29 Abs. 3 und 5 VE-DSG). Zudem gelten die Voraussetzungen von Artikel 29 Absatz 6 VE-DSG.

Die Pflicht der Aufsichtsbehörde zur Erstellung eines Tätigkeitsberichts ist in Artikel 49 der Richtlinie (EU) 2016/680 und in Artikel 12^{bis} Absatz 5^{bis} E-SEV 108 vorgesehen. Die Verordnung (EU) 2016/679 enthält in Artikel 59 eine analoge Regelung.

8.1.7.13 Art. 49 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 12^{bis} Buchstabe e E-SEV 108.

Der Beauftragte hat insbesondere die Aufgabe, die Organe des Bundes und der Kantone sowie private Personen in Datenschutzfragen zu informieren 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.

Aufhebung von Artikel 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 überflüssig. Gemäss VE hat der Beauftragte die Kompetenz, Kontrollmassnahmen (Art. 40) und vorsorgliche Massnahmen

(Art. 41) zu ergreifen. Es ist für ihn also nicht mehr notwendig, sich für vorsorgliche Massnahmen an das Bundesverwaltungsgericht zu wenden.

8.1.8 Strafbestimmungen

Der Bundesrat hat sich dafür entschieden, dem Beauftragten nicht die Kompetenz zu verleihen, Verwaltungssanktionen auszusprechen. Um die Rechtmässigkeit und die Akzeptanz solcher Verfügungen sowie die Wahrung der Verfahrensrechte sicherzustellen, hätte die Organisation des Beauftragten verändert werden müssen, beispielsweise analog zur Schweizerischen Wettbewerbskommission. Darauf wurde insbesondere mit Blick auf die Kosten verzichtet. Es scheint darüber hinaus vorteilhafter, Zuwiderhandlungen im Rahmen eines Strafverfahrens zu ahnden, welches die Garantien des Strafprozessrechts bietet. Der Entscheid für diesen Weg, der abweicht von dem, was für die grosse Mehrheit der ausländischen Aufsichtsbehörden gilt,¹¹⁰ macht allerdings eine erhebliche Stärkung des strafrechtlichen Teils des Gesetzes notwendig. Die Sanktionen müssen abschreckend sein, so wie vom E-SEV 108 (Art. 10)¹¹¹ und der Richtlinie (EU) 2016/680 (Art. 57) vorgesehen. Ein zu mildes Strafsystem könnte zur Folge haben, dass die schweizerische Regelung von der Europäischen Union nicht mehr als angemessen erachtet würde (Art. 45 Verordnung [EU] 2016/679). Die Verordnung (EU) 2016/679 (Art. 83) sieht bei der Verletzung zahlreicher Pflichten die Möglichkeit vor, zusätzlich zu oder an Stelle von Verwaltungsmassnahmen (Art. 58) hohe Geldbussen zu verhängen, wobei dies auch bei fahrlässigem Verhalten gilt. Daher ist vorgesehen, insbesondere die Geldbusse auf maximal 500'000 Franken zu erhöhen. Soweit sich eine Strafbestimmung vor allem an natürliche Personen richtet, soll die Bussenhöhe jedoch innerhalb vernünftiger Grenzen bleiben; insbesondere wäre es nicht sinnvoll, deren Höhe aufgrund des Umsatzes zu bestimmen, wie dies für Verwaltungssanktionen gegenüber Unternehmen vorgesehen ist. Juristische Personen können aufgrund von Artikel 53 VE-DSG direkt strafrechtlich verfolgt werden (vgl. den Kommentar zu Art. 53 VE-DSG).

8.1.8.1 Art. 50 Verletzung der Auskunft-, Melde- und Mitwirkungspflichten

Artikel 50 VE-DSG übernimmt im Wesentlichen Artikel 34 DSG, ergänzt ihn aber, um insbesondere die neuen Pflichten des Verantwortlichen und des Auftragsbearbeiters zu berücksichtigen.

Höhe der Busse

Mit dieser Bestimmung wird der maximale Betrag der Busse für diese Übertretung, der heute gemäss Artikel 106 Absatz 1 StGB bei 10 000 Franken liegt, auf 500 000 Franken erhöht. Der Bundesrat ist angesichts der fehlenden Kontrolle der betroffenen Personen über ihre Daten, der mangelnden Transparenz der Datenbearbeitung und der immer mächtigeren Wirtschaftsakteure der Auffassung, dass es hoher Bussen bedarf. Bussen von ähnlicher Höhe finden sich auch in anderen Bundesgesetzen wie im Bundesgesetz über Glücksspiele und Spielbanken vom 18. Dezember 1998¹¹² (SBG; Art. 56) oder im Bundesgesetz über die Banken und Sparkassen vom 8. November 1934¹¹³ (BankG; Art. 49). Es sei zudem darauf hingewiesen, dass die Verordnung (EU) 2016/679 (Art. 83) die Möglichkeit gibt, Geldbussen von bis zu zehn Millionen Euro oder, im Fall eines Unternehmens, von bis zu zwei Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs oder von bis zu zwanzig Millionen Euro oder vier Prozent des weltweit erzielten Jahresumsatzes zu verhängen. Dies spricht ebenfalls für eine Erhöhung des Bussenbetrags im DSG, da dieser ein Teil der massgebenden Kriterien sein dürfte, anhand derer entschieden wird, ob die Schweizer Gesetzgebung ein ausreichendes Schutzniveau im Sinne von Artikel 45 der Verordnung (EU) 2016/679 bietet. Denkbar wäre natürlich auch, diese Übertretungen als Straftaten zu betrachten, wodurch sie mit einer Geldstrafe oder mit einer Freiheitsstrafe bis zu drei Jahren sanktioniert werden könnten. Angesichts der geringeren Schwere dieser

¹¹⁰ Die Behörden der EU-Mitgliedstaaten können in der Regel selbst Bussen verhängen. Dies gilt auch für die Behörden Argentiniens, Singapurs, Kolumbiens und der Türkei.

¹¹¹ Siehe Ziffern 95 und 96 des Entwurfs des erläuternden Berichts von CAHDATA vom 2. Juni 2016.

¹¹² SR 935.52

¹¹³ SR 952.0

Übertretungen im Vergleich zu den Verstössen, für die Artikel 52 einschlägig ist (siehe Anmerkungen zu Art. 52), verzichtet der Bundesrat allerdings auf diesen Schritt.

Vor diesem Hintergrund ist es angemessen, die Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten weiterhin als Übertretung zu klassifizieren, gleichzeitig aber die dafür vorgesehenen Sanktionen deutlich zu erhöhen. Zu beachten ist zudem, dass es sich beim genannten Betrag um einen Höchstbetrag handelt und dass die tatsächliche Strafe vom Gericht unter Berücksichtigung der wirtschaftlichen Lage des Täters (Art. 106 Abs. 3 in Verbindung mit Art. 47 StGB) festgelegt wird. Ferner ist gemäss Artikel 52 StGB bei geringfügigen Fällen von einer Strafverfolgung oder Bestrafung abzusehen.

Absatz 1

Absatz 1 betrifft die Verletzung der Auskunftspflichten. Gemäss Buchstabe a sind private Personen zu bestrafen, die im Rahmen ihrer Informations- (Art. 13 und 15 VE-DSG) und Auskunftspflichten (Art. 20 VE-DSG) vorsätzlich eine falsche oder unvollständige Auskunft erteilen. Abgesehen von der Anpassung an die neuen einschlägigen Bestimmungen entspricht dies im Wesentlichen dem geltenden Recht (Art. 34 Abs. 1 Bst. a DSG).

Nach Absatz 1 Buchstabe b werden private Personen bestraft, die es vorsätzlich unterlassen, die betroffene Person nach Artikel 13 Absätze 1 und 5, Artikel 15 sowie Artikel 17 Absatz 2 VE-DSG zu informieren oder ihr die Angaben nach Artikel 13 Absätze 2, 3 und 4 VE-DSG zu liefern. Der VE-DSG übernimmt auch hier im Wesentlichen das geltende Recht (Art. 34 Abs. 1 Bst. b DSG) und passt es lediglich an die neu ausgestalteten Informationspflichten an.

Absatz 1 Buchstabe c sanktioniert die private Person, die es vorsätzlich unterlässt, dem Beauftragten nach Artikel 16 Absatz 3 die Ergebnisse der Datenschutz-Folgenabschätzung mitzuteilen. Die Datenschutz-Folgenabschätzung ist ein wichtiges Instrument, das dem Beauftragten erlaubt, seine Aufsichtsfunktion wahrzunehmen. Daher ist eine Sanktion für den Verstoß gegen diese Pflicht gerechtfertigt. Die Verordnung (EU) 2016/679 sieht ebenfalls Sanktionen vor (Art. 83 Abs. 4 Bst. a).

Absatz 2

Gemäss Absatz 2 Buchstabe a werden private Personen bestraft, die es unterlassen, den Beauftragten über die Garantien, namentlich die vertraglichen (Art. 5 Abs. 3 Bst. b VE-DSG), oder die verbindlichen unternehmensinternen Datenschutzvorschriften (Art. 5 Abs. 3 Bst. c, Ziff. 2 und Abs. 6 VE-DSG) zu informieren, oder die ihm nicht mitteilen, dass sie von standardisierten Garantien Gebrauch machen (Art. 5 Abs. 3 Bst. d Ziff 2 und Abs. 6 VE-DSG). Der VE-DSG entspricht hier teilweise dem geltenden Artikel 34 Absatz 2 Buchstabe a DSG, passt ihn jedoch an die neuen Pflichten bei der grenzüberschreitenden Kommunikation an. Absatz 2 Buchstabe b sanktioniert private Personen, die dem Beauftragten die standardisierten Garantien (Art. 5 Abs. 3 Bst. c Ziffer 1) oder die verbindlichen unternehmensinternen Vorschriften (Art. 5 Abs. 3 Bst. d Ziffer 1) nicht zur Genehmigung vorlegen. Diese Bestimmung ist neu, da diese Pflichten im geltenden Recht noch nicht existieren. Die Verordnung (EU) 2016/679 sieht in diesen Fällen eine Verwaltungsbusse von bis zu zehn Millionen Euro oder im Fall eines Unternehmens von bis zu zwei Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (Art. 83 Abs. 5 Bst. c) vor.

Buchstabe c entspricht dem geltenden Artikel 34 Absatz 2 Buchstabe b DSG. Allerdings wurde «Abklärung des Sachverhalts» durch «Untersuchung» ersetzt.

Die Buchstaben d bestraft die Verletzung der neuen Pflichten, dem Beauftragten Verletzungen des Datenschutzes zu melden (Art. 17 Abs. 1 VE-DSG). Der Bundesrat ist der Ansicht, dass der Beauftragte seine Aufsichtsfunktion nur wahrnehmen kann, wenn diese Pflichten erfüllt werden, und demzufolge deren Verletzung strafbar sein muss. Die Verordnung (EU) 2016/679 sieht ebenfalls die Sanktionierung entsprechender Pflichtverletzungen vor (Art. 83 Abs. 4 Bst. a).

Nach Buchstabe e wiederum wird bestraft, die private Person, die einer Verfügung des Beauftragten nicht Folge leistet. Diese Bestimmung ist wichtig um sicherzustellen, dass die Massnahmen des Beauftragten tatsächlich befolgt werden. In den Augen des Bundesrates reicht Artikel 292 StGB in diesem Zusammenhang nicht aus, da er eine zu geringe Busse enthält. Auch die Verordnung (EU) 2016/679 sieht die Bestrafung eines solchen Verhaltens vor (Art. 83 Abs. 4 Bst. e).

Absatz 3

Absatz 3 Buchstabe a sanktioniert die Verletzung der Pflicht, die Empfänger, denen Daten übermittelt wurden, über jede Berichtigung, Löschung oder Vernichtung von Daten, jede Verletzung des Datenschutzes oder jede Einschränkung der Bearbeitung zu informieren (Art. 19 Bst. b VE-DSG). Strafbar ist nach Buchstabe b auch die Verletzung der Pflicht, den Verantwortlichen über Verletzungen des Datenschutzes zu informieren (Art. 17 Abs. 4 VE-DSG). Die Verordnung (EU) 2016/679 sieht hierfür eine Verwaltungsbusse von bis zu zehn Millionen Euro oder im Fall eines Unternehmens von bis zu zwei Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs vor (Art. 83 Abs. 4 Bst. a).

Die genannten Handlungen sind auch strafbar, wenn der Täter fahrlässig handelt. In diesem Fall beträgt die Busse höchstens 250 000 Franken. Die Verordnung (EU) 2016/679 enthält eine entsprechende Bestimmung (Art. 83 Abs. 2 Bst. b).

8.1.8.2 Art. 51 Verletzung der Sorgfaltspflichten

Diese Bestimmung ist neu. Sie ist notwendig, weil der VE-DSG eine Reihe neuer Pflichten vorsieht, die nicht von den aktuell geltenden Strafbestimmungen abgedeckt werden. Der Bundesrat ist der Auffassung, dass ein wirksamer Schutz der Persönlichkeit und der Grundrechte der betroffenen Personen nur möglich ist, wenn die Verantwortlichen und die Auftragsbearbeiter ihren Pflichten voll und ganz gerecht werden. Um diese zur strikten Einhaltung des Datenschutzgesetzes anzuhalten, schlägt der Bundesrat eine Vervollständigung der Strafbestimmungen des Gesetzes vor. Die Verordnung (EU) 2016/679 sieht vor, dass alle Verstösse auch bei Fahrlässigkeit sanktioniert werden können (Art. 83 Abs. 4 Bst. a und Abs. 5 Bst. c). Dies gilt angesichts der bestehenden Disziplinar massnahmen jedoch nicht für die Bundesorgane.

Artikel 50 Absatz 1 VE-DSG sieht eine Busse von bis zu 500 000 Franken vor für private Personen, die vorsätzlich bestimmte Pflichten verletzen. Die Begründung hierfür entspricht jener bei Artikel 50 (siehe oben).

Gemäss Buchstabe a wird bestraft, wer bei der Übermittlung von Daten ins Ausland gegen Artikel 5 Absätze 1 und 2 verstösst, ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind.

Buchstabe b sanktioniert die Übergabe der Datenbearbeitung an einen Auftragsbearbeiter entgegen Artikel 7 Absätze 1 und 2.

Nach Buchstabe c wird bestraft, wer nicht die notwendigen Massnahmen zum Schutz gegen unbefugte Datenbearbeitungen oder Verlust trifft (Art. 11).

Buchstabe d stellt die Nichtvornahme einer Datenschutz-Folgenabschätzung nach Artikel 16 VE-DSG unter Strafe.

Gemäss Buchstabe e ist es strafbar, keine Vorkehrungen im Sinne von Artikel 18 zu treffen.

Und Buchstabe f sanktioniert das Fehlen einer Dokumentation der Datenbearbeitung gemäss Artikel 19 Buchstabe a VE-DSG.

8.1.8.3 Art. 52 Verletzung der beruflichen Schweigepflicht

Mit dieser Bestimmung soll der in Artikel 321 StGB vorgesehene Schutz der beruflichen Schweigepflicht vervollständigt werden. Durch die zunehmende berufliche Spezialisierung, aber auch durch die neuen Informationsbearbeitungsmethoden ist Artikel 321 StGB lückenhaft geworden. Artikel 52 VE-DSG sieht deshalb eine Schweigepflicht auch für Berufe vor, die nicht unter Artikel 321 StGB fallen, für deren Ausübung der Schutz der

Vertraulichkeit aber ebenfalls unerlässlich ist. Der Gesetzgeber bevorzugt diese Lösung gegenüber einer Ausdehnung des Anwendungsbereichs von Artikel 321 StGB, da er es nicht für zweckmässig erachtet, auch das Zeugnisverweigerungsrecht zu erweitern, welches die Verfahrensgesetze in der Regel für die in Artikel 321 StGB erwähnten Berufe vorsehen.¹¹⁴

Seit Inkrafttreten des DSG wurden im Bereich der Informations- und Kommunikationstechnologien immense Fortschritte gemacht und hat deren Bedeutung deutlich zugenommen. Elektronische Kommunikationsmöglichkeiten sind weit verbreitet und stellen inzwischen das bevorzugte, wenn nicht gar einzige Mittel dar, um Informationen zu übertragen und aufzubewahren. Die technischen Mittel sind vorhanden und die Kosten für sie derart gering, dass es heute immer mehr Menschen möglich ist, enorme Datenmengen zu verarbeiten. Während in der Vergangenheit beim Speichern von Daten früher oder später physische Grenzen erreicht wurden, ist es heute kaum mehr notwendig, alte elektronische Daten zu vernichten, um Platz für neue zu schaffen. Informationen haben auf diese Weise nahezu ewig Bestand. Aufgrund des steten und rasanten technologischen Fortschritts dürfte sich diese Entwicklung künftig noch verstärken. Dies stellt allerdings eine Gefahr für den Schutz der Privatsphäre dar und macht entsprechende Schutzmassnahmen notwendig.

Vor diesem Hintergrund erscheint es einerseits angebracht, den Geheimnisschutz auf alle Arten von Personendaten auszudehnen. Massgebend ist demnach, ob es sich um geheime Daten handelt. Dies entspricht Artikel 321 StGB, der ebenfalls alleine darauf abstellt, ob die fragliche Information geheim ist oder nicht, während ohne Bedeutung ist, was genau Inhalt des Geheimnisses war. Dadurch wird auch verhindert, dass der strafrechtliche Schutz durch die Aufhebung des Begriffs des Persönlichkeitsprofils geschwächt wird.

Ferner scheint es notwendig, den Wortlaut der Strafbestimmung anzupassen, um der oben beschriebenen Realität besser Rechnung zu tragen. Die heutigen Möglichkeiten haben die Datenbearbeitung allein zu Erwerbszwecken erheblich erleichtert. Diesbezüglich ist insbesondere auf die Onlinehändler und sozialen Netzwerke hinzuweisen, die derartige Informationen zu Werbezwecken kaufen und verkaufen. Mehr als noch bei beruflichen Aktivitäten, welche die Kenntnis solcher Daten erfordern, besteht im Rahmen kommerzieller Aktivitäten die Gefahr, dass in das geschützte Rechtsgut eingegriffen wird. Mit der Strafandrohung von Absatz 1 Buchstabe b sollen derartige Verletzungen verhindert werden

Darüber hinaus entspricht eine Busse in keiner Weise mehr der Schwere möglicher Eingriffe, insbesondere im Hinblick auf Artikel 321 StGB. Dieses Missverhältnis gilt es deshalb durch die Einführung einer Straftat zu beseitigen, welche mit bis zu drei Jahren Haft oder Geldstrafe geahndet werden kann.

8.1.8.4 Art. 53 Übertretungen in Geschäftsbetrieben

In dieser Bestimmung wird die Regelung von Artikel 7 des Bundesgesetzes vom 22. März 1974¹¹⁵ über das Verwaltungsstrafrecht (VStrR) übernommen, aber der Bussenbetrag, oberhalb dessen es nicht mehr möglich ist, eine juristische Person an Stelle einer natürlichen Person zu verfolgen, auf 100 000 Franken erhöht. Artikel 102 StGB ist auf Übertretungen nicht anwendbar. Aus den bereits erwähnten Gründen müssen die Verstösse gegen das vorliegende Gesetz jedoch mehrheitlich Übertretungen sein. Da zu befürchten ist, dass diese Verstösse hauptsächlich in Geschäftsbetrieben erfolgen, ist es gerechtfertigt, das Prinzip von Artikel 7 VStrR anzuwenden, damit die Wirksamkeit der neuen Bestimmungen nicht schon von vornherein eingeschränkt wird. Eine ausdrückliche Verweisung ist erforderlich, da das VStrR in der Sache nicht anwendbar ist. Für die Straftaten nach Artikel 52 VE-DSG bleibt jedoch allein Artikel 102 StGB anwendbar.

¹¹⁴ Botschaft DSG, BBl 1988 II 413, 485; NIGGLI Marcel Alexander/MAEDER Stefan, Kommentar zu Art. 35 DSG in: Maurer-Lambrou/Blechta (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, Art. 35 DSG N 1.

¹¹⁵ SR 313.0

8.1.8.5 Art. 54 Anwendbares Recht und Verfahren

Die Verfolgung und Beurteilung der strafbaren Handlungen obliegt wie heute den Kantonen, welche entsprechend die StPO anwenden. Artikel 54 stellt eine punktuelle Verweisung dar, die für das anwendbare Verfahrensrecht keine Bedeutung hat.

8.1.8.6 Art. 55 Verfolgungsverjährung für Übertretungen

Die Erfahrung hat gezeigt, dass Datenschutzuntersuchungen meist kompliziert und mühsam sind. Die übliche Verjährungsfrist für Übertretungen beträgt drei Jahre (Art. 109 StGB). Um zu vermeiden, dass die Mehrzahl der Strafverfahren von vornherein zum Scheitern verurteilt ist, sieht der VE-DSG eine Erhöhung der Verjährungsfrist auf fünf Jahre vor.

Was die Straftaten im Sinne von Artikel 52 angeht, besteht hingegen keine Notwendigkeit, von der üblichen Verjährungsfrist von zehn Jahren (Art. 97 Abs. 1 Bst. c StGB) abzuweichen.

8.1.9 Abschluss von Staatsverträgen

Art. 56 Abschluss von Staatsverträgen

Artikel 56 VE-DSG ersetzt Artikel 36 Absatz 5 DSG, der unter Berücksichtigung der geltenden Grundsätze in Bezug auf die Kompetenzdelegation zu unbestimmt ist. Gemäss Artikel 56 VE-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 auf Kooperationsabkommen nach dem Modell des Abkommens zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Union über die Zusammenarbeit bei der Anwendung ihres Wettbewerbsrechts¹¹⁶. Nach Buchstabe b kann der Bundesrat ausserdem Staatsverträge über die gegenseitige Anerkennung eines angemessenen Schutzniveaus für die grenzüberschreitende Bekanntgabe von Daten abschliessen. Diese Bestimmung bezieht sich namentlich auf ein allfälliges Abkommen mit den Vereinigten Staaten zum Ersatz des geltenden «U.S-Swiss Safe Harbor Framework».

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, 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.

8.1.10 Schluss- und Übergangsbestimmungen

8.1.10.1 Art. 57 Vollzug durch die Kantone

Diese Bestimmung entspricht Artikel 37 DSG, lediglich die Verweisungen auf die neuen Bestimmungen des VE-DSG werden angepasst. Darüber hinaus sei auf die Erläuterungen in der Botschaft des Bundesrates vom 19. Februar 2003 zur Änderung des DSG und auf den Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll zum Übereinkommen SEV 108¹¹⁷ hingewiesen.

8.1.10.2 Art. 58 Aufhebung und Änderung anderer Erlasse

Die Aufhebung und Änderung anderer Erlasse wird unter Ziffer 8.2 kommentiert.

¹¹⁶ Abkommen vom 17. Mai 2013 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Union über die Zusammenarbeit bei der Anwendung ihres Wettbewerbsrechts, abgeschlossen am 17. Mai 2013, SR 0.251.268.1. Zu erwähnen ist, dass in diesem Fall die Kompetenz nicht dem Bundesrat übertragen war.

¹¹⁷ BBI 2003 2101, hier 2146–2147

8.1.10.3 Art. 59 Übergangsbestimmung

Der Verantwortliche sowie der Auftragsbearbeiter müssen innert zwei Jahren nach Inkrafttreten des Gesetzes in der Lage sein, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16) und die in den Artikeln 18 und 19 Buchstabe a vorgesehenen Massnahmen für Datenbearbeitungen, welche im Zeitpunkt des Inkrafttretens bereits im Gange waren, zu treffen.

8.2 Erläuterungen zu den Änderungen anderer Bundesgesetze

Die Aufhebung und Änderung anderer Bundesgesetze ist im Anhang des VE-DSG geregelt.¹¹⁸ Diese Änderungen erfolgen aufgrund des VE-DSG.

8.2.1 Aufhebung des Bundesgesetzes über den 19. Juni 1992 über den Datenschutz

Da es sich beim VE-DSG um eine Totalrevision des Datenschutzgesetzes handelt, muss das aktuelle Datenschutzgesetz aufgehoben werden.

8.2.2 Änderung der Terminologie in Bundesgesetzen

Aufgrund der Aufhebung des Begriffs «Datensammlung» im VE-DSG müssen die Bundesgesetze, in denen dieser verwendet wird, ebenfalls angepasst werden. Mit dem VE-DSG wird ferner der Begriff «Inhaber der Datensammlung» ersetzt.

Gemäss dem VE-DSG soll anstelle des Begriffs «Persönlichkeitsprofile» der Begriff «Profiling» verwendet werden. Letzterer Begriff ist treffender und bezieht sich auf eine Tätigkeit (siehe die Erläuterungen zu Artikel 3 Buchstabe f VE-DSG). Aus Gründen der Kohärenz muss der Begriff «Persönlichkeitsprofil» auch in einem grossen Teil der bereichsspezifischen Datenschutznormen ersetzt werden. In den meisten Gesetzen genügt es, den Verweis auf das Persönlichkeitsprofil einfach zu streichen. Dies hat keine praktischen Auswirkungen, denn gemäss dem VE ist nur eine formellgesetzliche Grundlage erforderlich, wenn Daten ausgewertet werden, um wesentliche persönliche Merkmale wie die Arbeitsleistung, die wirtschaftliche Lage, die Gesundheit, die Intimsphäre oder die Mobilität zu analysieren oder Entwicklungen vorherzusagen, d.h. wenn ein Profiling erfolgt. Die Einführung des Begriffs des Profilings ist folglich ausschliesslich in jenen Fällen gerechtfertigt, in denen die betreffende Behörde derartige Analysen oder Vorhersagen erstellt. In Bezug auf die Bearbeitung besonders schützenswerter Daten hingegen ändert sich die Gesetzesgrundlage in den bereichsspezifischen Datenschutznormen nicht. In einigen bereichsspezifischen Datenschutznormen muss der Begriff «Persönlichkeitsprofil» demgegenüber – wie im Folgenden erläutert – mit den nötigen Anpassungen durch den neuen Begriff «Profiling» im Sinne von Artikel 3 Buchstabe f VE-DSG ersetzt werden.

8.2.3 Ausländergesetz vom 16. Dezember 2015¹¹⁹

Art. 101

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Vgl. die Erläuterungen unter Ziffer 8.2.1.

Art. 111d Abs. 2 Bst. a und b

Nach Buchstabe a des geltenden Artikels muss die betroffene Person ohne jeden Zweifel einwilligen; handelt es sich um besonders schützenswerte Daten, so muss die Einwilligung ausdrücklich sein. Der Begriff der «Einwilligung» der betroffenen Person muss im Bundesrecht einheitlich definiert werden. Dementsprechend ist Buchstabe a unter Verweis auf Artikel 4 Absatz 6 VE-DSG anzupassen. Buchstabe b wird geändert, um der neuen Vorschrift nach Artikel 6 Absatz 1 Buchstabe d VE-DSG Rechnung zu tragen.

¹¹⁸ Einzelne Bundesgesetze sind ihrerseits Gegenstand von Revisionen. Es handelt sich dabei um das Bundesgesetz vom 29. September 1952 über den Erwerb und Verlust des Schweizer Bürgerrechts (SR 141.0, BBI 2014 5133), das Bundesgesetz vom 4. Oktober 1991 über die Eidgenössischen Technischen Hochschulen (SR 414.110, BBI 2016 3369) und das Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung (SR 510.10, BBI 2016 2047). Art. 27 und 27d BPG werden geändert durch den Entwurf zum Bundesgesetz über die Anstalt zur Verwaltung der Ausgleichsfonds von AHV, IV und EO (Ausgleichsfondsgesetz, BBI 2016 353).

¹¹⁹ SR 142.20

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 20 Absatz 2 Buchstabe f VE-DSG festgehalten ist.

8.2.4 Asylgesetz vom 26. Juni 1998¹²⁰

Art. 96 Abs. 1, Art. 99a Abs. 2 Bst. a, Art. 100 Abs. 2 und Art. 102 Abs. 1 und 2

Der Begriff «Persönlichkeitsprofil» wird gestrichen. Vgl. die Erläuterungen unter Ziffer 8.2.1.

Art. 99 Abs. 6 erster Satz

Der Begriff des "Inhabers der Datensammlung" wird durch den "Verantwortlichen" ersetzt. Vgl. den Kommentar zu Ziff. 8.2.1.

Art. 102c Einleitungssatz, Abs. 2 Bst. a und b

Siehe die Erläuterungen zu Artikel 111 d Abs. 2 Bst. a und b VE-AuG.

Art. 102e zweiter Satz

Siehe die Erläuterungen zu Artikel 111 f zweiter Satz VE-AuG.

8.2.5 Öffentlichkeitsgesetz vom 17. Dezember 2004¹²¹

Art. 7 Abs. 2 und 3

Nach Artikel 7 Absatz 2 wird der Zugang zu amtlichen Dokumenten einschränkt, wenn durch seine Gewährung die Privatsphäre Dritter beeinträchtigt werden kann, ausser das öffentliche Interesse am Zugang würde ausnahmsweise überwiegen.

Aufgrund der Änderungen von Artikel 11 Absatz 1, Artikel 12 Absatz 3 und Artikel 15 Absatz 2 BGÖ ist es nötig, die Systematik von Artikel 7 Absatz 2 BGÖ anzupassen. Der VE sieht daher die Einschränkung des Zugangs in Artikel 7 Absatz 2 VE-BGÖ vor, die Ausnahme dazu hingegen in Absatz 3. Im Übrigen bleiben die Bestimmungen im Verhältnis zum aktuellen Recht unverändert.

Art. 11 Abs. 1

Artikel 11 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 VE-DSG ist es erforderlich, juristischen Personen das Recht, angehört zu werden, zu garantieren, wenn die Behörde in Betracht zieht, nach Artikel 7 Absatz 3 VE-BGÖ Zugang zu gewähren. Gemäss den Anpassungen in Absatz 1 muss die Behörde künftig Dritte konsultieren, wenn sie den Zugang zu einem Dokument erwägt, das Personendaten enthält, die diese Dritten betreffen, oder wenn sie beabsichtigt, Artikel 7 Absatz 3 VE-BGÖ anzuwenden.

Art. 12 Abs. 3

Aufgrund der Anpassungen von Artikel 7 Absatz 3 und Artikel 11 Absatz 1 VE-BGÖ ist es nötig, Artikel 12 Absatz 3 zu ändern, wonach der Zugang zu einem Dokument, das Personendaten enthält, oder der Zugang aufgrund von Artikel 7 Absatz 3 VE-BGÖ bis zur Klärung der Rechtslage aufgeschoben werden muss.

¹²⁰ SR 142.31

¹²¹ SR 152.3

Art. 15 Abs. 2 Bst. c (neu)

Aus den bereits erwähnten Motiven ist es erforderlich, Artikel 15 Absatz 2 um einen neuen Buchstaben c zu ergänzen, wonach die Behörde eine Verfügung erlassen muss, wenn sie entgegen der Empfehlung des Beauftragten gemäss Artikel 7 Absatz 3 VE-BGÖ den Zugang zu einem amtlichen Dokument gewährt.

8.2.6 Verwaltungsverfahrensgesetz vom 20. Dezember 1968¹²²

Art. 71a

Mit Absatz 1 wird ein vom Bundesgericht entwickelter Grundsatz¹²³ ins Gesetz aufgenommen, wonach datenschutzrechtliche Fragen in einem Verfahren, das andere Rechtsansprüche als spezifische Ansprüche nach dem DSG zum Gegenstand hat, im Hauptverfahren beurteilt werden müssen und den entsprechenden Rechtsmitteln unterliegen.

Aus dem Grundsatz nach Absatz 1 geht hervor, dass der Beauftragte nicht für die Aufsicht über die Datenbearbeitung in einem hängigen Beschwerde- oder Revisionsverfahren zuständig ist (Abs. 2).

8.2.7 Zivilgesetzbuch

Aufgrund der Aufhebung der Ausnahme nach Artikel 2 Absatz 2 Buchstabe d DSG betreffend die öffentlichen Register des Privatrechtsverkehrs müssen im Zivilgesetzbuch einige Bestimmungen zum Zivilstandswesen angepasst werden. Damit soll einerseits dem Grundsatz von Artikel 9 ZGB – wonach öffentliche Register für die durch sie bezeugten Tatsachen vollen Beweis erbringen, solange nicht die Unrichtigkeit ihres Inhaltes nachgewiesen ist – und andererseits dem öffentlichen Interesse am Führen solcher Register Rechnung getragen werden (siehe Erwägung 73 der Verordnung [EU] 2016/679).

Art. 45a Abs. 3 Ziff. 3 und Abs. 4

In Artikel 45a Absatz 3 Ziffer 3 VE-ZGB¹²⁴ wird der Bundesrat beauftragt, unter Mitwirkung der Kantone die Aufsicht über die zentrale Datenbank «Infostar» zu regeln. Es geht insbesondere darum, Artikel 83 ZStV anzupassen. Dies kann beispielsweise in Anlehnung an Artikel 55 Absatz 1 der N-SIS-Verordnung vom 8. März 2013¹²⁵ 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 Infostar dürfen der Beauftragte und die kantonalen Datenschutzbehörden nicht in die Kompetenz der Gerichte zur Änderung streitiger Daten (Art. 42 ZGB) eingreifen.

Gestützt auf Artikel 45a Absatz 4 VE-ZGB kann der Bundesrat die Ansprüche der betroffenen Personen ausserdem ganz oder teilweise abweichend von Artikel 34 Absätze 1 bis 3 VE-DSG regeln. Dabei handelt es sich um eine fakultative Delegation der Rechtsetzungskompetenz. Der Bundesrat kann sich auf diese Kompetenz stützen, wenn er zum Schluss kommt, dass angesichts des Zwecks des zentralen Registers und unter Berücksichtigung der Anforderungen des neuen Übereinkommens SEV 108 – sofern die Schweiz das Protokoll zur Änderung dieses Rechtsakts annimmt – besondere Vorschriften erforderlich sind.

¹²² SR 172.021

¹²³ BGE 128 II 311 E. 8.4

¹²⁴ Art. 45a ZGB wird im Moment revidiert (vgl. die Botschaft des Bundesrates vom 16. April 2014 betreffend die Änderungen des Zivilgesetzbuches (Zivilstandsregister und Grundbuch), BBl 2014 3395).

¹²⁵ SR 362.0

8.2.8 Bundesgesetz vom 24. März 2000¹²⁶ über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten

Art. 1 erster Satz und Art. 2 Abs. 2 erster Satz

Zur Beurteilung, ob eine Person in Begleitung von Familienangehörigen im Ausland eingesetzt werden kann, und zur Einschätzung von Risiken in den persönlichen Verhältnissen können die Personaldienste des EDA nach Artikel 3 dieses Gesetzes Daten über die Familienangehörigen bearbeiten. Diese Bestimmungen sind entsprechend umzuformulieren, so dass die Bearbeitung von besonders schützenswerten Personendaten und das Profiling zulässig sind.

8.2.9 Zivilprozessordnung¹²⁷

8.2.9.1 Gerichtsstand

Art. 20 Bst. d

Artikel 20 ZPO regelt neu den Gerichtsstand für sämtliche zivilrechtlichen Begehren nach dem Datenschutzgesetz. Diese sind namentlich das Einsichts- und Löschungsrecht nach Artikel 12 VE-DSG, das Auskunftsrecht nach Artikel 20 VE-DSG und die verschiedenen Klagen nach Artikel 25 VE-DSG.

8.2.9.2 Befreiung von den Gerichtskosten

Die Evaluation des Datenschutzgesetzes hat ergeben, dass die betroffenen Personen ihre Rechte kaum wahrnehmen bzw. auf dem Rechtsweg durchsetzen, insbesondere im privaten Sektor.¹²⁸ Dies liegt gerade im Kostenrisiko für die betroffene Person begründet und verringert die Wirksamkeit des Datenschutzgesetzes erheblich. Zudem fehlt es als Konsequenz davon im Bereich des Datenschutzgesetzes 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 Datenschutzgesetz 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 Fr. 30 000 sowie Streitigkeiten nach dem Mitwirkungsgesetz). Damit wird das Kostenrisiko für betroffene Personen in einem wichtigen Punkt verringert. Aufgrund der bisherigen Fallzahlen ist es indes 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 Prozessführung auch in unentgeltlichen Verfahren Gerichtskosten auferlegt werden können (Art. 115 ZPO).

Art. 99 Abs. 3 Bst. d

Für Verfahren nach dem Datenschutzgesetz 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 25 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

¹²⁶ SR 235.2

¹²⁷ SR 272

¹²⁸ Vgl. S. 90 f. und 219 des Schlussberichts zur Evaluation des Bundesgesetzes über den Datenschutz vom 10. März 2011.

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 Datenschutzgesetz 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 Datenschutzgesetz. 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 unentgeltlicher Rechtsbeistand bestellt.

Art. 114 Bst. f

Die Zivilprozessordnung soll dahingehend ergänzt werden, dass in Verfahren nach dem Datenschutzgesetz im Entscheidungsverfahren 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 Entscheidungsverfahren nach Datenschutzgesetz 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.

8.2.9.3 Verfahrensart

Art. 243 Abs. 2 Bst. d

Ansprüche nach Artikel 12 VE-DSG können wie das Auskunftsrecht im vereinfachten Verfahren geltend gemacht werden. Die Anpassung der Bestimmung ist nötig, weil Artikel 12 ins Gesetz eingefügt wurde.

8.2.10 Bundesgesetz vom 18. Dezember 1987¹²⁹ über das Internationale Privatrecht

Art. 130 Abs. 3

Die Anpassung des Artikels ist erforderlich, weil der VE-DSG den Begriff der Datensammlung nicht mehr verwendet.

Artikel 130 VE-IPRG sieht nun vor, dass Klagen zur Durchsetzung eines Auskunfts- oder Einsichtsrechts im Zusammenhang mit der Bearbeitung von Personendaten bei den Gerichten nach Artikel 129 IPRG oder den schweizerischen Gerichten am Ort, wo der betreffende Bearbeitungsvorgang erfolgt, eingereicht werden. Ein Auskunftsrecht, das sich auf eine bestimmte Tätigkeit bezieht, muss dort geltend gemacht werden, wo diese bestimmte Tätigkeit stattfindet, und nicht an irgendeinem anderen Ort, an dem die Daten sonst noch von jemandem bearbeitet werden.

¹²⁹ SR 291

8.2.11 Strafgesetzbuch

Art. 179^{novies}

Diese Bestimmung sanktioniert das unbefugte Beschaffen von Personendaten, die nicht frei zugänglich sind. Dabei rechtfertigt es sich aufgrund der vielfältigen technischen Entwicklungen, die Bestimmung auf alle Arten von Personendaten auszudehnen, wie dies bereits in Bezug auf die Geheimnisverletzung in Artikel 52 VE-DSG erfolgt ist (vgl. Ziff. 8.1.8.3). Hervorzuheben ist insbesondere, dass gerade für das Profiling nach Artikel 3 Buchstabe f, von dem eine besondere Gefährdung für die betroffenen Personen ausgeht, sowohl Personendaten als auch andere Daten ohne direkten persönlichen Bezug verwendet werden können. Daher ist es sachgerecht, nunmehr alle Arten von Personendaten als geschütztes Rechtsgut von Artikel 179^{novies} zu definieren.

Ebenfalls wird die Wendung «nicht frei zugänglich sind» ersetzt durch «nicht für jedermann zugänglich».

Art. 179^{decies}

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 in einem rechtlichen Kontext 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 Privatbereich¹³⁰. 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 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

¹³⁰ Art. 173 ff. StGB.

Natur sein. Die Absicht, beim Betroffenen einen massiven Ärger auszulösen, kann als Nachteilsabsicht bereits ausreichen¹³¹.

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 Personendaten¹³² 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.

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.

8.2.12 Bundesgesetz vom 22. März 1974¹³³ über das Verwaltungsstrafrecht

Das 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). Mit Blick auf den neuen Wortlaut von Artikel 2 Absatz 2 Buchstabe c VE-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

In dieser Bestimmung wird die Transparenz bei der Beschaffung von Personendaten geregelt. Es handelt sich um eine Sonderbestimmung, die den Artikeln 13 und 14 VE-DSG vorgeht. Sie entspricht der Regelung nach Artikel 95 StPO.

Art. 18b

Siehe sinngemäss die Erläuterungen zu Artikel 349g Absatz 3 VE-StGB (Ziff. 8.3.1.7).

¹³¹ 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.

¹³² Art. 179^{novies} StGB.

¹³³ SR 313.0

Art. 18c

Diese Bestimmung regelt die Bekanntgabe und Verwendung von Daten in einem hängigen Verfahren. Sie entspricht der Regelung nach Artikel 96 StPO.

Art. 18d

Diese Bestimmung regelt die Auskunftsrechte in einem hängigen Verfahren. Es handelt sich um eine Sonderbestimmung, die den Artikeln 20 und 21 VE-DSG vorgeht. Sie entspricht der Regelung nach Artikel 97 StPO.

Art. 18e

In dieser Bestimmung wird die Richtigkeit der Daten geregelt. Sie entspricht der Regelung nach Artikel 98 StPO. Es handelt sich um eine Sonderbestimmung, die den Artikeln 4 Absatz 5 sowie 34 Absatz 2 VE-DSG vorgeht. In Bezug auf Absatz 2 wird auf die Erläuterungen zu Artikel 98 Absatz 2 VE-StPO verwiesen (vgl. Ziff. 8.3.28.2.11).

Art. 18f

Mit Absatz 1 wird ein vom Bundesgericht entwickelter Grundsatz¹³⁴ ins Gesetz aufgenommen, wonach datenschutzrechtliche Fragen in einem Verfahren, das andere Rechtsansprüche als spezifische Ansprüche nach dem DSG zum Gegenstand hat, im Hauptverfahren beurteilt werden müssen und den entsprechenden Rechtsmitteln unterliegen.

Aus dem Grundsatz nach Absatz 1 geht hervor, dass der Beauftragte nicht zuständig ist für die Aufsicht über die Datenbearbeitung durch die Verwaltungsbehörde des Bundes in einem Verwaltungsstrafverfahren, solange der Endentscheid noch nicht rechtskräftig ist (Abs. 2). Diese Präzisierung ist notwendig, weil die Verwaltungsbehörden des Bundes in der Regel nicht unabhängige Gerichtsbehörden im Sinne von Artikel 2 Absatz 2 Buchstabe c VE-DSG sind. Die Überwachung der Einhaltung der Datenschutzvorschriften in einem hängigen Verfahren wird durch die unabhängige Kontrolle durch die gerichtliche Beschwerdeinstanz sichergestellt. Dieses Aufsichtssystem entspricht jenem des Beauftragten.

8.2.13 Militärstrafprozess vom 23. März 1979¹³⁵ (MStP)

Die Militärjustiz ist eine unabhängige Gerichtsbehörde (Art. 1 MStP). Sie fällt unter die Ausnahme nach Artikel 2 Absatz 2 Buchstabe c VE-DSG. Das Militärstrafprozessrecht sieht, anders als die Strafprozessordnung, 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

In dieser Bestimmung wird die Transparenz bei der Beschaffung von Personendaten geregelt. Es handelt sich um eine Sonderbestimmung, die den Artikeln 13 und 14 VE-DSG vorgeht. Sie entspricht der Regelung nach Artikel 95 StPO.

Art. 25b

Siehe sinngemäss die Erläuterungen zu Artikel 349g Absatz 3 VE-StGB (Ziff. 8.3.1.7).

Art. 25c

Diese Bestimmung regelt die Bekanntgabe und Verwendung von Personendaten in einem hängigen Verfahren. Sie entspricht der Regelung nach Artikel 96 StPO.

¹³⁴ BGE 128 II 311 E. 8.4

¹³⁵ SR 321.0

Art. 25d

Diese Bestimmung regelt die Auskunftsrechte in einem hängigen Verfahren. Es handelt sich um eine Sonderbestimmung, die den Artikeln 20 und 21 VE-DSG vorgeht. Sie entspricht der Regelung nach Artikel 97 StPO.

Art. 25e

In dieser Bestimmung wird die Richtigkeit der Daten geregelt. Sie entspricht der Regelung nach Artikel 98 StPO. Es handelt sich um eine Sonderbestimmung, die den Artikeln 4 Absatz 5 sowie 34 Absatz 2 VE-DSG vorgeht. Des Weiteren wird auf die Erläuterungen zu Artikel Artikel 349g Absatz 2 VE-StGB verwiesen (Ziff. 8.3.1.7).

8.2.14 Bundesgesetz vom 13. Juni 2008¹³⁶ über die polizeilichen Informationssysteme des Bundes

Art. 5 Titel, 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 7 VE-DSG geregelt. Artikel 5 Absatz 2 BPI ist daher überflüssig. Dementsprechend muss auch der Sachtitel angepasst werden.

8.2.15 Bundesstatistikgesetz vom 9. Oktober 1992¹³⁷

Art. 14a Abs. 1 erster und zweiter Satz

In Artikel 14a wird die Verknüpfung von Daten geregelt. Dabei kann es sich unter anderem auch um Profiling handeln. So ist Absatz 1 dahingehend zu ergänzen, dass das Bundesamt zur Erfüllung seiner statistischen Aufgaben zum Profiling befugt ist. Nach Absatz 1 zweiter Satz sind die verknüpften Daten nach Abschluss der statistischen Auswertungsarbeiten zu löschen, wenn besonders schützenswerte Daten verknüpft werden oder sich aus der Verknüpfung Persönlichkeitsprofile ergeben. Diese Bestimmung ist so anzupassen, dass die Daten nach Abschluss der statistischen Auswertungsarbeiten zu löschen sind.

8.2.16 Militärgesetz vom 3. Februar 1995

Art. 31 Abs. 2

Aufgrund der Art der Aufgaben des Nachrichtendienstes der Armee muss diese Bestimmung umformuliert werden, so dass die Kompetenz zum Profiling vorliegt.

Art. 99 Abs. 2

Aufgrund der Art der Aufgaben des Nachrichtendienstes der Armee muss diese Bestimmung umformuliert werden, so dass die Kompetenz zum Profiling vorliegt.

Art. 100 Abs. 2

Aufgrund der Art der Aufgaben des Dienstes für militärische Sicherheit muss diese Bestimmung umformuliert werden, so dass die Kompetenz zum Profiling vorliegt.

¹³⁶ SR 361

¹³⁷ SR 431.01

8.2.17 Bundesgesetz vom 3. Oktober 2008¹³⁸ über die militärischen Informationssysteme

Art. 1 Abs. 1 Einleitungssatz und Art. 11 Abs. 2 Einleitungssatz

Aufgrund der Art der Aufgaben der Armee und der Militärverwaltung müssen diese Bestimmungen umformuliert werden, so dass das Profiling möglich ist. Ebenfalls muss definiert werden, nach welchem Zeitablauf Daten zum Profiling gelöscht werden.

8.2.18 Waffengesetz vom 20. Juni 1997¹³⁹

Art. 32e Abs. 2 Bst. a und b

Siehe die Erläuterungen zu Artikel 111d Absatz 2 Buchstaben a und VE-AuG.

Art. 32g zweiter Satz

Siehe die Erläuterungen zu Artikel 111f zweiter Satz VE-AuG.

8.2.19 Bundesgesetz vom 4. Oktober 2002¹⁴⁰ über den Bevölkerungsschutz und den Zivilschutz

Art. 72 Abs. 1 und 1^{bis}

Nach geltendem Recht ist die zuständige Bundesbehörde befugt, namentlich zur Abklärung des Kaderpotenzials von Schutzdienstpflichtigen und Kursteilnehmenden Persönlichkeitsprofile zu erstellen¹⁴¹. Diese Bestimmungen sind so anzupassen, dass die Behörde zum Profiling im Sinne von Artikel 3 Buchstabe f VE-DSG befugt ist.

8.2.20 Bundesgesetz vom 21. Dezember 1948¹⁴² über die Luftfahrt

Art. 107a Abs. 2 Einleitungssatz, 4 und 5

Nach geltendem Recht ist die zuständige Bundesbehörde befugt, die Befähigung des in der Zivilluftfahrt tätigen Personals zu beurteilen. Daher ist die Bestimmung so umzuformulieren, dass die Zuständigkeit zum Profiling vorliegt.

In Absatz 5 werden hingegen Persönlichkeitsprofile ersatzlos gestrichen. Denn bei Daten, die aus einem Profiling entstanden sind, handelt es sich um Personendaten. Für deren Bekanntgabe besteht eine gesetzliche Grundlage.

8.2.21 Bundesgesetz vom 3. Oktober 1951¹⁴³ über die Betäubungsmittel und die psychotropen Stoffe

Art. 3f Abs. 1

Der Begriff «Persönlichkeitsprofile» wird gestrichen. Siehe die Erläuterungen unter Ziffer 8.2.2.

Art. 18c zweiter Satz

Siehe die Erläuterungen zu Artikel 111f zweiter Satz VE-AuG.

¹³⁸ SR 510.91

¹³⁹ SR 514.54

¹⁴⁰ SR 520.1

¹⁴¹ Art. 72 ist Gegenstand einer Revision, die am 1. Januar 2017 in Kraft treten sollte (siehe FF 2014 6935)

¹⁴² SR 748.0

¹⁴³ SR 812.121

8.3 Kommentare zu den Änderungen der Bundesgesetze, welche die Anforderungen der Richtlinie (EU) 2016/680 umsetzen

Wenn dieselbe Änderung in mehreren Erlassen erfolgt, ist sie nur einmal kommentiert und der Text enthält eine entsprechende Verweisung.

8.3.1 Strafgesetzbuch

Zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680 umfasst die Vorlage einige Datenschutzbestimmungen zum Datenaustausch im Bereich der polizeilichen Zusammenarbeit.

8.3.1.1 Art. 349a

In dieser Bestimmung ist der Grundsatz verankert, wonach sich die Bearbeitung von Daten für die Amtshilfe im Bereich der Polizei, unter Vorbehalt der besonderen Vorschriften nach Artikel 349b ff. VE-StGB, nach den Datenschutzbestimmungen von Bund und Kantonen richtet. Diese Bestimmungen gelten mithin auch für die kantonalen Behörden, ausser die Norm spreche ausdrücklich von Bundesorganen. 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 Gesetzgeber auch Datenschutzbestimmungen erlassen, die für kantonale Behörden gelten, die Bundesrecht anwenden müssen.

8.3.1.2 Art. 349b

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. Zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680 weicht Artikel 349b von Artikel 29 VE-DSG ab. Fehlt eine Rechtsgrundlage, so dürfen die Bundesbehörden Daten ausschliesslich in den Fällen nach Artikel 349b Buchstaben a und b bekannt geben. Diese Bestimmungen entsprechen den Buchstaben c und d von Artikel 29 Absatz 2 VE-DSG. Die zuständigen Bundesbehörden dürfen sich für eine Bekanntgabe hingegen nicht auf Artikel 29 Absatz 3 Buchstaben a, b und e VE-DSG stützen, da diese Bestimmungen nicht mit den Anforderungen der Artikel 8 und 10 der Richtlinie (EU) 2016/680 vereinbar sind.

8.3.1.3 Art. 349c

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 349c entspricht der Lösung des Bundesgesetzgebers in Artikel 6 SlaG. 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.

8.3.1.4 Art.349d

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 349d 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 5 und 6 VE-DSG angelehnt.

Absatz 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.

Absatz 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 Kommission dies in einem Beschluss nach Artikel 36 der Richtlinie (EU) 2016/680 festgehalten hat. Absatz 2 Buchstabe a unterscheidet sich von Artikel 5 Absatz 2 VE-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 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 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. a) oder durch spezifische Garantien (Bst. b) gewährleistet ist. Absatz 2 Buchstabe b entspricht der Voraussetzung nach Artikel 5 Absatz 3 Buchstabe a VE-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, beispielsweise das Übereinkommen SEV 108 und dessen Zusatzprotokoll¹⁴⁴. Absatz 2 Buchstabe c entspricht der Voraussetzung nach Artikel 5 Absatz 3 Buchstabe b VE-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.

Absatz 3

Nach Absatz 3 informiert die zuständige Bundesbehörde 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 sind die Bekanntgaben zu dokumentieren. Anhand dieser Dokumentation ist der Beauftragte in der Lage, die erforderlichen Abklärungen vorzunehmen und allenfalls ein Verbot nach Artikel 43 Absatz 2 VE-DSG zu erlassen.

¹⁴⁴ Siehe die Erwägung 69 der Richtlinie (EU) 2016/680.

Absatz 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.

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 Behörde muss im Rahmen einer 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 die 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. Die zuständige Bundesbehörde muss den Beauftragten über die Bekanntgabe von Daten nach Absatz 4 informieren (Abs. 5).

Absatz 6

Nach Absatz 6 sind die Bestimmungen über die Zusage für die zwischenstaatliche Zusammenarbeit in Strafsachen vorbehalten. Denn das in Absatz 1 verlangte angemessene Datenschutzniveau ist nicht die einzige Voraussetzung für die Zulässigkeit der Bekanntgabe von Daten an einen Drittstaat; darüber hinaus sind auch die Gesetzesbestimmungen im Bereich der zwischenstaatlichen Zusammenarbeit zu beachten. So dürfen Daten einem Drittstaat nur übermittelt werden, wenn die empfangende Behörde für die Verhütung, Feststellung oder Verfolgung einer Straftat zuständig ist und wenn die Bekanntgabe zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Darüber hinaus muss jede weitere Datenbearbeitung durch die empfangende Behörde nach dem Grundsatz der Spezialität erfolgen. Beabsichtigt die Behörde, die Daten an einen anderen Drittstaat weiterzuübermitteln, so muss sie vorgängig die Genehmigung der zuständigen Behörde einholen, welche die ursprüngliche Übermittlung durchgeführt hat.

8.3.1.5 Art. 349e

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 349e Artikel 6b 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 349d 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).

8.3.1.6 Art. 349f

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.¹⁴⁵

Gemäss der Begriffsbestimmung nach Artikel 3 Absatz 8 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. In Artikel 349f wird für den Begriff «Empfänger» der Ausdruck «Dritter» verwendet.

Absatz 1

Nach Absatz 1 ist die Bekanntgabe von Personendaten an in einem Drittstaat niedergelassene Dritte nur dann möglich, wenn vier Voraussetzungen kumulativ erfüllt sind. Die auf Artikel 349f 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.

Die zweite Voraussetzung (Abs. 1 Bst. a) lautet, dass die Bekanntgabe in einem Spezialgesetz oder einem völkerrechtlichen Vertrag vorgesehen sein muss. Denn Artikel 349f an sich bildet keine Rechtsgrundlage für die Bekanntgabe der Personendaten. Es müssen auch die Gesetzesbestimmungen im Bereich der zwischenstaatlichen Zusammenarbeit eingehalten werden.

Nach Absatz 1 Buchstabe b 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 349f 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. c). Die Behörde muss folglich eine Interessenabwägung vornehmen, um festzustellen, ob das gefährdete öffentliche Interesse oder das Interesse der betroffenen Person überwiegt.

Absatz 2

Nach Absatz 2 gibt die zuständige Behörde dem Dritten 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.

¹⁴⁵ Erwägung 73 der Richtlinie (EU) 2016/680.

Absatz 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).

Absatz 4

Absatz 4 schreibt vor, dass die zuständige Behörde auch den Beauftragten unverzüglich über jede Bekanntgabe von Daten gestützt auf Artikel 349f benachrichtigen muss. Anders als im Fall von Artikel 349d 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. 4). Anhand dieser Dokumentation ist der Beauftragte in der Lage, die erforderlichen Abklärungen vorzunehmen und allenfalls ein Verbot nach Artikel 43 Absatz 2 VE-DSG zu erlassen.

8.3.1.7 Art. 349g

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 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. Sie muss vor der Bekanntgabe der Daten über die betroffenen Personen an einen Empfänger so weit wie möglich die erforderlichen Massnahmen treffen, damit die verschiedenen Kategorien betroffener Personen nicht verwechselt werden. 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. Gemäss der Erwägung 30 dieses Rechtsakts liegt die Bestimmung darin begründet, dass die letztere Kategorie Daten enthält, die auf der subjektiven Wahrnehmung natürlicher Personen basieren und nicht immer nachprüfbar sind. 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.¹⁴⁶

¹⁴⁶ Erwägung 30 der Richtlinie (EU) 2016/680.

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.

8.3.1.8 Art. 349h

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 349h wurde die Lösung in Artikel 8 des Bundesgesetzes vom 13. Juni 2008¹⁴⁷ über die polizeilichen Informationssysteme des Bundes (BPI) übernommen und an die Neuerungen dieser Vorlage angepasst (siehe Ziff. 8.3.6).

Nach Absatz 1 kann die betroffene Person in den Fällen nach den Buchstaben a–d 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 349h berufen. Darüber hinaus kann eine Prüfung nur dann verlangt werden, wenn die verantwortliche Bundesbehörde der Aufsicht des Beauftragten untersteht. Dies trifft zum Beispiel auf 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. 44 Abs. 2 VE-DSG). Sie kann somit kein Rechtsmittel gegen allfällige Verwaltungsmassnahmen des Beauftragten (Art. 43 VE-DSG) ergreifen.

8.3.1.9 Art. 349i

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 41 Absatz 1 VE-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. 44 Abs. 2 VE-DSG e contrario). 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 349i 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. 349d VE-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

¹⁴⁷ SR 361

die Erläuterungen zu Art. 349h Abs. 2 VE-StGB). Gegebenenfalls kann der Beauftragte gegenüber der Bundesbehörde vorsorgliche Massnahmen oder Verwaltungsmassnahmen anordnen (Art. 42 und 43 VE-DSG). Der Entscheid und die Rechtsmittelbelehrung dazu müssen der Bundesbehörde sowie der betroffenen Person eröffnet werden.

8.3.1.10 Art. 355a Abs. 1 und 4

Da im VE-DSG der Begriff «Persönlichkeitsprofile» nicht mehr verwendet wird, muss er auch in Absatz 1 gestrichen werden (siehe Erläuterungen unter Ziff. 8.2.28.2.1).

Absatz 4 ist neu. Darin wird präzisiert, dass der Austausch von Personendaten mit Europol dem Austausch mit einer zuständigen Behörde eines Schengen-Staates (Art. 349c) gleichgesetzt wird. Gemäss der Erwägung 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.

8.3.1.11 Art. 355f und Art. 355g

Diese Bestimmungen wurden anlässlich der Übernahme des Rahmenbeschlusses 2008/977 /JAI durch die Schweiz eingeführt.

Artikel 355f 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 im 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 355g kann somit aufgehoben werden.

8.3.2 Strafprozessordnung¹⁴⁸

Art. 95a

Diese Bestimmung setzt die Anforderungen der Artikel 6 und 7 Absatz 1 der Richtlinie (EU) 2016/680 um. Mit Buchstabe a wird auf die Problematik eingegangen, dass betroffene Personen mit Fortschreiten des Verfahrens die Kategorie wechseln können. Die urteilenden Behörden treffen die Unterscheidung zwischen Personendaten, die auf Fakten beruhen, und solchen, die auf persönlichen Einschätzungen basieren, in den Erwägungen des begründeten Urteils. Des Weiteren gelten sinngemäss die Erläuterungen zu Artikel 349g Absatz 3 VE-StGB (Ziff. 8.3.1.78.2.11).

Art. 98 Abs. 2

Artikel 98 regelt den Grundsatz der Richtigkeit der Daten. Es handelt sich um eine Sonderbestimmung, die Artikel 4 Absatz 5 VE-DSG sowie Artikel 34 Absatz 2 VE-DSG vorgeht. In Bezug auf die Änderung von Absatz 2 siehe die Erläuterungen zu Artikel 349g Absatz 2 VE-StGB (Ziff. 8.3.1.7).

8.3.3 Rechtshilfegesetz vom 20. März 1981¹⁴⁹

Mit dieser Vorlage wird im IRSG ein neues Kapitel 1b zum Datenschutz eingefügt, das an die Lösung des Bundesgesetzgebers in Artikel 95 ff. StPO angelehnt ist. Mit diesen Bestimmungen werden zudem bestimmte Anforderungen der Richtlinie (EU) 2016/680 umgesetzt. Es handelt sich dabei um besondere datenschutzrechtliche Bestimmungen, welche den allgemeinen Grundsätzen des VE-DSG vorgehen, solange ein Rechtshilfeverfahren hängig ist.

¹⁴⁸ SR 312.0

¹⁴⁹ SR 351.1

8.3.3.1 Art. 11b

Artikel 11*b* regelt die Informationspflicht der Behörde, wenn sie in einem Rechtshilfeverfahren, das auf Ersuchen eines ausländischen Staates eröffnet wurde, Personendaten bearbeitet. Bei diesem Artikel handelt es sich um eine besondere datenschutzrechtliche Bestimmung, die den Artikeln 13 und 14 VE-DSG vorgeht. Artikel 11*b* gilt auch für kantonale Behörden, die ein Rechtshilfeverfahren unterstützen oder für den Vollzug eines Rechtshilfeersuchens, beispielsweise eines Auslieferungsgesuchs, zuständig sind. Der Bund nutzt hier seine Gesetzgebungskompetenz, da der Bereich der zwischenstaatlichen Zusammenarbeit in Strafsachen im Bundesrecht geregelt ist.

Nach Absatz 1 muss die zuständige Behörde, d.h. die Behörde, die über das ausländische Rechtshilfeersuchen entscheiden muss (Art. 1 Abs. 1 IRSG), die Person, gegen die sich ein solches Ersuchen richtet, über jede Bearbeitung von Daten über sie informieren. Dies gilt für jede strafrechtlich verfolgte oder verurteilte Person, derentwegen der ausländische Staat die Schweiz um Zusammenarbeit ersucht, damit sie die betroffene Person ausliefert, die von ihr begangene strafbare Handlung stellvertretend verfolgt und ahndet oder den ausländischen Strafscheid gegenüber der Person vollstreckt (Art. 1 Abs. 1 Bst. a, c und d IRSG). Die Behörde muss auch die in Artikel 80*b* IRSG definierten Berechtigten in einem Rechtshilfeverfahren zur Unterstützung eines Strafverfahrens im Ausland informieren.

Die Informationspflicht der Behörde gilt jedoch nicht absolut. Diese ist von der Informationspflicht befreit, wenn überwiegende öffentliche oder private Interessen der Information der betroffenen Person entgegenstehen. Die Behörde muss folglich eine Interessenabwägung vornehmen, um festzustellen, ob das gefährdete öffentliche Interesse oder das Interesse der betroffenen Person überwiegt. Kommt die Behörde zum Schluss, dass ein privates oder öffentliches Interesse das Interesse der betroffenen Person an der Information überwiegt, so muss sie auf die Information der betroffenen Person verzichten.

In Absatz 2 werden die Fälle aufgeführt, in denen das öffentliche Interesse überwiegt. Gemäss dieser Bestimmung besteht ein überwiegendes öffentliches Interesse namentlich, wenn durch die Information der betroffenen Person ein Ermittlungs-, Untersuchungs- oder Gerichtsverfahren oder ein Verfahren der zwischenstaatlichen Zusammenarbeit in Strafsachen, zum Beispiel die Festnahme der verfolgten Person zur Auslieferung, gefährdet wird. Die Aufzählung ist nicht abschliessend. Die Behörde kann sich im Einzelfall somit auf andere spezifische Anhaltspunkte stützen.

Ferner gelten die Artikel 52 und 80*b* IRSG.

8.3.3.2 Art. 11c

In dieser Bestimmung werden die Auskunftsrechte in einem hängigen Verfahren geregelt. Sie entspricht Artikel 97 StPO. Es handelt sich um eine Sonderbestimmung, die den Artikeln 20 und 21 VE-DSG vorgeht. Nur die Person, gegen die sich ein Gesuch um internationale Rechtshilfe in Strafsachen richtet, darf im Rahmen ihrer Rechte die Akten einsehen und Personendaten erhalten, die sie betreffen.

Ferner gelten die Artikel 52 und 80*b* IRSG.

8.3.3.3 Art. 11d

Mit dieser Bestimmung wird eine Einschränkung des Auskunftsrechts eingeführt, die für Ersuchen um Festnahme zum Zwecke der Auslieferung gilt. 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 (siehe Ziff. 8.3.6). Artikel 11*d* 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.

Absatz 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.

Absatz 2, 3, 4, 5 und 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 VE 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*d* 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 Privatsphäre und dem öffentlichen Interesse daran, die Strafverfolgung eines ausländischen Staates nicht zu gefährden. 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, 4, 5 und 6 stimmen mit den entsprechenden Vorschriften in Artikel 349*h* VE-StGB überein.

Absatz 7

Absatz 7 schliesslich sieht vor, dass das Bundesamt für Justiz in Abweichung von Artikel 2 der betroffenen Person mit Einverständnis des ersuchenden Staates die Auskünfte geben kann, um die sie ersucht hat.

8.3.3.4 Art. 11e

Diese Bestimmung regelt die Gleichbehandlung der Schengen-Staaten und der nationalen Behörden auf dem Gebiet des Datenschutzes. Siehe des Weiteren die Erläuterungen zu Artikel 349*c* VE-StGB (Ziff. 8.3.1.3).

8.3.3.5 Art. 11f

Diese Bestimmung regelt die Bekanntgabe von Daten an einen Drittstaat oder ein internationales Organ. Der Wortlaut dieses Artikels entspricht im Wesentlichen Artikel 349*d* VE-StGB. Abweichend von Artikel 349*d* Absatz 3 VE-StGB ist in Artikel 11*f* jedoch nicht vorgesehen, dass die zuständige Behörde den Beauftragten über die Kategorien von Bekanntgaben von Personendaten informieren muss, die nach Artikel 11*f* Absatz 2 Buchstabe c erfolgt sind. Dieser Unterschied ist dadurch gerechtfertigt, dass in Artikel 11*i* Absatz 2 die Regelung eingefügt werden muss, wonach der Beauftragte nicht für die Aufsicht über die Datenbearbeitung im Rahmen eines hängigen Rechtshilfeverfahrens zuständig ist

(siehe die Erläuterungen zu Artikel 11*i* unten). Des Weiteren wird auf die Erläuterungen zu Artikel 349*d* VE-StGB verwiesen (siehe Ziff. 8.3.1.4).

8.3.3.6 Art. 11g

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*e* VE-StGB. Abweichend von Artikel 349*e* Absatz 1 Buchstabe a VE-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 die Erläuterungen zu Artikel 349*e* VE-StGB (unter Ziff. 8.3.1.5).

8.3.3.7 Art. 11h

In dieser Bestimmung wird die Richtigkeit der Daten geregelt. Es handelt sich um eine Sonderbestimmung, die den Artikeln 4 Absatz 5 sowie 34 Absatz 2 VE-DSG vorgeht. Die Bestimmung entspricht Artikel 349*g* VE-StGB (siehe die Erläuterungen unter Ziff. 8.3.1.7).

8.3.3.8 Art. 11i

Diese Bestimmung regelt die datenschutzrechtlichen Ansprüche der Personen, gegen die sich ein Ersuchen um Zusammenarbeit in Strafsachen in einem hängigen Rechtshilfeverfahren richtet. Sie entspricht der Lösung nach Artikel 18*g* VE-VStrR unter dem Vorbehalt, dass Absatz 2 ausdrücklich die Anwendung der Artikel 20 und 21 VE-DSG betreffend das Auskunftsrecht der betroffenen Person, Art. 30 VE-DSG betreffend den Widerspruch gegen die Bekanntgabe von Daten und Artikel 34 VE-DSG betreffend die Rechtsansprüche im Falle einer widerrechtlichen Datenbearbeitung durch ein Bundesorgan ausschliesst. Siehe des Weiteren die Erläuterungen zu Artikel 18*g* VE-VStrR (siehe Ziff. 8.2.12).

8.3.4 Bundesgesetz vom 3. Oktober 1975 zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen

Zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680 muss im Bundesgesetz vom 3. Oktober 1975¹⁵⁰ zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen ein Verweis auf die Artikel 11*b*–11*d* und 11*g*–11*i* VE-IRSG eingefügt werden (Art. 9*a*). Artikel 11*e* VE-IRSG ist nicht anwendbar, da die darin verankerte Gleichbehandlung im Datenschutzbereich ausschliesslich für die Behörden der Schengen-Staaten und die schweizerischen Strafverfolgungsbehörden gilt, wie in Artikel 7 Absatz 3 des Bundesgesetzes zum Staatsvertrag mit den Vereinigten Staaten von Amerika sind in Artikel 9*a* die Bestimmungen des Staatsvertrags vom 25. Mai 1973¹⁵¹ zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen vorbehalten.

8.3.5 Bundesgesetz vom 7. Oktober 1994¹⁵² 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*i* VE-StPO anzupassen.

¹⁵⁰ SR 351.93

¹⁵¹ SR 0.351.933.6

¹⁵² SR 360

8.3.6 Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes

Art. 7 Abs. 2

In Absatz 2 wird zusätzlich der neue Artikel 8^{bis} vorbehalten.

Art. 8 Abs. 2, 3, 4, 5, 6, und 8

Dieser Artikel muss angepasst werden, da der Beauftragte gemäss dem neuen DSG keine Empfehlungen mehr erlässt, sondern eine Untersuchung im Sinne von Artikel 41 VE-DSG eröffnen und gegebenenfalls Massnahmen nach den Artikeln 42 und 43 anordnen kann.

Absatz 2 wird redaktionell angepasst.

Die zweite Möglichkeit von Absatz 3 erster Satz 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 41 DSG eröffnet hat». Da dem Beauftragten in den Artikeln 42 und 43 VE-DSG Verfügungskompetenzen verliehen werden, ist es nicht mehr erforderlich, dass das Bundesverwaltungsgericht wie gemäss Absatz 3 letzter Satz sowie Absatz 5 des geltenden Gesetzes eingreift; die entsprechenden Stellen können gestrichen werden.

Absatz 4 kann aufgehoben werden. Die Verweisung auf Artikel 41 VE-DSG genügt.

Auf Grundlage der Untersuchung kann der Beauftragte eine Verfügung erlassen (Art. 43 VE-DSG), die fedpol anfechten kann (Abs. 5).

Absatz 6 wird redaktionell angepasst.

Absatz 8 wird dahingehend angepasst, dass der Beauftragte nicht mehr nur empfehlen, sondern anordnen kann, dass fedpol der betroffenen Person die verlangten Auskünfte erteilt, wenn die Voraussetzungen dafür erfüllt sind.

Art. 8a

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. Die Bestimmung entspricht Artikel 11e VE-IRSG. Siehe folglich die entsprechenden Erläuterungen (Ziff. 8.3.3).

8.3.7 Schengen-Informationsaustausch-Gesetz vom 12. Juni 2009

Art. 2 Abs. 3

Die Artikel 6a bis 6c 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 349a bis 349i VE-StPO einzufügen.

9 Auswirkungen

Die Auswirkungen der Vorlage und jene der Übernahme der Richtlinie sind untrennbar miteinander verbunden und werden daher nicht getrennt dargestellt.

9.1 Finanzielle und personelle Auswirkungen auf den Bund

In diesem Stadium der Arbeiten sind die finanziellen Auswirkungen des VE-DSG auf das Bundespersonal und insbesondere auf die Ressourcen des Beauftragten schwer abzuschätzen.

Wie aus den Antworten auf die Interpellationen Derder 15.4253 «Die Daten schützen, damit sie besser genutzt werden können. Eine dringende Notwendigkeit» und Aebischer 16.3011

«Nicht nur das Datenschutzgesetz, sondern auch die Ressourcen anpassen» hervorgeht, möchte der Bundesrat erst im Rahmen seiner Botschaft prüfen, welche Ressourcen dem Beauftragten zur Verfügung stehen müssen. Er möchte damit zu einem Zeitpunkt auf diese Frage eingehen, in dem die neuen Aufgaben des Beauftragten definitiv feststehen. Wenn der Vorentwurf in dieser Form beibehalten wird, dürfte der finanzielle Bedarf des Beauftragten indes erheblich steigen, dies aufgrund der Aufgaben nach Artikel 5, 8, 16 und 17 und der Verfügungskompetenz (Art. 41 ff. VE-DSG). Mit Blick auf die zunehmende Digitalisierung der Wirtschaft und der Verwaltung ist darüber hinaus anzunehmen, dass die Anzahl öffentlicher und privater Projekte sowie der Umfang von Gesetzgebungsprojekten, zu denen der Beauftragte Stellung nehmen muss, zunehmen werden. Daraus wird sich der Bedarf nach zusätzlichen Ressourcen ergeben. Hingegen hat der Beauftragte bereits heute im Rahmen der Schengener und Dubliner Zusammenarbeit die Bearbeitung persönlicher Daten durch Bundesorgane zu kontrollieren. Nach eigenen Angaben führt der Beauftragte derzeit drei bis vier Kontrollen pro Jahr durch. Diese Zahl könnte nun leicht ansteigen. Zwar wird der Beauftragte im Einklang mit der EU-Richtlinie künftig neue Verfügungskompetenzen haben, doch dürften für deren Ausübung keine zusätzlichen Ressourcen erforderlich sein, da er bereits heute Empfehlungen an die Bundesorgane aussprechen und eine Angelegenheit zum Entscheid an die nächsthöhere Instanz weiterziehen kann, wenn seine Empfehlung nicht umgesetzt wird, und den Entscheid der nächsthöheren Instanz anfechten kann. Dennoch ist eine Zunahme der Abklärungsanfragen betroffener Personen und der Kooperationsanfragen von Datenschutzbehörden anderer Schengen-Staaten nicht auszuschliessen. Die Tatsache, dass die betroffenen Personen künftig das Recht haben, beim Beauftragten die Eröffnung einer Untersuchung zu verlangen, könnte zudem zu einem Anstieg der Fälle führen. Diese neuen Aufgaben könnten also die Zuteilung zusätzlicher Ressourcen im Form von maximal einer oder zwei Stellen erforderlich machen.

Die finanziellen Auswirkungen auf die Bundesverwaltung dürften gering sein. Dennoch wird diese Frage parallel zu jener nach den Ressourcen des Beauftragten geprüft werden.

9.2 Auswirkungen auf die Kantone und Gemeinden

Die Annahme des Zusatzprotokolls 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.

9.3 Auswirkungen im Informatikbereich

Der VE 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 seine Bearbeitungen zu dokumentieren. Schliesslich muss er bestimmte Datenschutzverstösse dem Beauftragten und gegebenenfalls auch der betroffenen Person melden.

Die Auswirkungen auf die Bundesorgane sind in verschiedener Hinsicht geringfügiger. So besteht beispielsweise keine Informationspflicht gegenüber der betroffenen Person, wenn die automatisierte Entscheidung gesetzlich vorgesehen ist. Zudem 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). Auswirkungen auf die automatisierten Datenbearbeitungssysteme der Bundesorgane wird allerdings die Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680 haben, der die Schengen-Staaten verpflichtet, bestimmte Bearbeitungsvorgänge in automatisierten Systemen zu protokollieren. Dies macht eine Anpassung der in Artikel 10 VDSG vorgesehenen Protokollpflicht erforderlich, da diese Bestimmung derzeit nur für die Bearbeitung von besonders schützenswerten Personendaten oder von Persönlichkeitsprofilen gilt, deren Schutz nicht durch präventive Massnahmen gewährleistet werden kann. In diesem Zusammenhang wird es einer Übergangsbestimmung bedürfen, was Artikel 63 Absatz 2 der Richtlinie (EU) 2016/680 im Übrigen auch zulässt. Schliesslich hat auch die Pflicht der Bundesorgane, ihre Bearbeitungsaktivitäten dem Beauftragten zu melden, keine praktischen Auswirkungen, da sie im Wesentlichen der in Artikel 11a 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 Bearbeitungsaktivitäten der Bundesorgane gespeichert werden und nicht mehr jene von privaten Personen.

9.4 Auswirkungen auf die Volkswirtschaft

Ziel des VE 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 VE 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 VE 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 Kommission¹⁵³, welcher der Schweiz ein ausreichendes Datenschutzniveau 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 VE 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 Zusatzprotokolls des revidierten Übereinkommens 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 VE indirekt 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 VE 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

¹⁵³ ABI. L 215 vom 25.8.2000, S. 1.

Handel angeht. Die Kosten für die Umsetzung der neuen Pflichten des Verantwortlichen dürften durch diese Vorteile aufgewogen werden.

Die staatlichen Eingriffe werden auf ein absolutes Minimum begrenzt. Die Idee besteht vielmehr darin, das Verantwortungsbewusstsein der Verantwortlichen zu stärken und diese beispielsweise zur Einhaltung der vom Beauftragten oder von anderen Stellen erarbeiteten Empfehlungen der guten Praxis 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 Garantien oder verbindliche unternehmensinterne Datenschutzvorschriften – des Bestehens eines geeigneten Datenschutzniveaus zu versichern.

9.5 Auswirkungen auf Gesundheit und Gesellschaft

Um die mit den neuen Technologien verbundenen gesellschaftlichen Herausforderungen zu bewältigen, sieht der VE unter anderem die Stärkung der Aufsichtsbefugnisse des Beauftragten vor. Dieser kann künftig Untersuchungen eröffnen und gegebenenfalls Verwaltungsmassnahmen ergreifen, wenn eine Datenbearbeitung eine grössere Anzahl von Personen betrifft und demnach ein allgemeines Interesse für die Öffentlichkeit besteht. 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.

9.6 Auswirkungen auf die Gleichstellung von Mann und Frau

Es sind keine Auswirkungen auf die Gleichstellung von Mann und Frau zu erwarten.

9.7 Auswirkungen auf die Umwelt

Es sind keine direkten ökologischen Auswirkungen zu erwarten.

10 Verhältnis zur Legislaturplanung und zu den nationalen Strategien des Bundesrates

10.1 Verhältnis zur Legislaturplanung

Der Gesetzesentwurf ist in der Botschaft vom 27. Januar 2016 über die Legislaturplanung 2015–2019¹⁵⁴ angekündigt worden.

10.2 Verhältnis zu Strategien des Bundesrates

Der Entwurf ist vereinbar mit der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) sowie mit der Strategie «Open Government Data (OGD)». Ferner ist der VE Teil des Massnahmenkatalogs zur Umsetzung der Strategie «Digitale Schweiz» (vgl. Ziff. 1.1.3 oben).

¹⁵⁴ BBI 2016 1105, hier 1219

11 Rechtliche Aspekte

11.1 Verfassungsmässigkeit

11.1.1 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. 7a 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 handelt es sich nicht um einen Vertrag mit beschränkter Tragweite. Folglich ist die Bundesversammlung für die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/679 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 internationale Verträge untersteht.

11.1.2 Zuständigkeit für die Genehmigung E-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 VE steht im Einklang mit dem E-SEV 108. Sobald das Zusatzprotokoll des Übereinkommens SEV 108 zur Unterzeichnung aufgelegt wird, kann der Bundesrat dieses unterzeichnen und dem Parlament zur Genehmigung vorlegen. Aus den in Ziffer 11.1.1 genannten Gründen untersteht auch der Bundesbeschluss über die Genehmigung des Zusatzprotokolls des Übereinkommens SEV 108 durch die Schweiz gemäss Artikel 141 Absatz 1 Buchstabe d Ziffer 3 BV dem Referendum für internationale Verträge.

11.1.3 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 Datenschutzübereinkommens¹⁵⁵ 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, das 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.

Beim Erlass privatrechtlicher Datenschutzbestimmungen kann sich der Bundesgesetzgeber auf die Rechtsetzungskompetenzen in Sachen Zivilrecht (Art. 122 BV), privatwirtschaftlicher Erwerbstätigkeit (Art. 95 BV) und Verbraucherschutz (Art. 97 BV) stützen.

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 achtet 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.

11.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Der VE ist vereinbar mit den internationalen Verpflichtungen der Schweiz. Er erlaubt ihr, das Zusatzprotokoll des Übereinkommens SEV 108 zu ratifizieren, sobald dies möglich ist. Zudem kann die Schweiz auf diese Weise die Verpflichtungen nach dem Schengen-Assoziierungsabkommen mit der Europäischen Union erfüllen.

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.¹⁵⁶

11.3 Erlassform

Zusätzlich zum Bundesbeschluss zur Genehmigung des Notenaustausches betreffend die Übernahme der Richtlinie (EU) 2016/680 enthält der vorliegende Entwurf den Vorentwurf des Bundesgesetzes über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz. Es handelt sich dabei um einen dem fakultativen Gesetzesreferendum unterstehenden Mantelerlass. Der Mantelerlass besteht aus einer Ziffer I, welche die Totalrevision des DSG (im Folgenden «VE-DSG») und im Anhang die dadurch notwendigen Anpassungen weiterer Bundesgesetze beinhaltet. Ziffer II der Mantelerlasses enthält die Änderungen von Bundesgesetzen, die sich aus der Umsetzung der Richtlinie (EU) 2016/680 im Rahmen der Schengen-Verpflichtungen ergeben.

¹⁵⁵ BBI 2003 2101, hier 2151

¹⁵⁶ Erwägung 95.

11.4 Unterstellung unter die Ausgabenbremse

Der VE bringt keine Ausgaben mit sich, welche der Ausgabenbremse (Art. 159 Abs. 3 Bst. b BV) unterstehen.

11.5 Einhaltung der Grundsätze des Subventionsgesetzes

Der VE sieht keine Subventionen vor.

11.6 Delegation von Rechtssetzungsbefugnissen

Der Entwurf sieht insbesondere die Delegation folgender Rechtssetzungsbefugnisse vor:

- Unverändert ist der Bundesrat gemäss Artikel 10 Absatz 2 dafür zuständig, Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens zu erlassen.
- Der Bundesrat erlässt besondere Regeln über die Kontrolle und Verantwortung für den Datenschutz, wenn ein Bundesorgan Daten zusammen mit anderen Organen bearbeitet (Art. 26 VE-DSG).
- Der Bundesrat behält die Kompetenz, unter bestimmten Voraussetzungen die automatisierte Bearbeitung besonders schützenswerter Daten im Rahmen von Pilotversuchen zu bewilligen (Art. 28 VE-DSG).
- Der Bundesrat kann ausserdem die Ansprüche der betroffenen Personen regeln, indem er im Rahmen des Personenstandsrechts besondere Vorschriften erlässt, welche ganz oder teilweise von Artikel 34 VE-DSG abweichen (Art. 45a Abs. 4 VE-ZGB).