Vernehmlassung

Revision Datenschutzgesetz

Amtliche Akten

Beginn: 21.12.2016

Abschluss: 04.04.2017

Vorlage
DSG

Anhang *Vorentwurf*

Bundesgesetz über den Datenschutz

(Datenschutzgesetz, DSG)

vom …

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,

gestützt auf die Artikel 95 Absatz 1, 122 Absatz 1 und 173 Absatz 2 der Bundesverfassung[1],

nach Einsicht in die Botschaft des Bundesrates vom ...[2],

beschliesst:

1. Abschnitt: Zweck, Geltungsbereich und Begriffe

Art. 1 Zweck

Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden.

Art. 2 Geltungsbereich

1 Dieses Gesetz gilt für die Bearbeitung von Daten natürlicher Personen durch:

a. private Personen;

b. Bundesorgane.

2 Es ist nicht anwendbar auf:

a. Personendaten, die durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden;

b. Personendaten, die durch die Eidgenössischen Räte und die parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

SR .....
1 SR **101**
2 BBl xx

c. Personendaten, die durch unabhängige eidgenössische Justizbehörden im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden;

d. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007[3], die in der Schweiz Immunität geniessen, wie das Internationale Komitee vom Roten Kreuz.

[3] Dieses Gesetz ist nicht anwendbar auf Personendaten, die durch die eidgenössischen Gerichte im Rahmen ihrer Rechtsprechungstätigkeit bearbeitet werden. Für die Bearbeitung der übrigen Daten sind sie von der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) ausgenommen.

[4] Die Bundesversammlung und der Bundesrat sind von der Aufsicht durch den Beauftragten ausgenommen.

Art. 3 Begriffe

Die folgenden Ausdrücke bedeuten:

a. *Personendaten:* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;

b. *betroffene Person:* natürliche Person, über die Daten bearbeitet werden;

c. *besonders schützenswerte Personendaten:*

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,

2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,

3. genetische Daten,

4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,

5. Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen,

6. Daten über Massnahmen der sozialen Hilfe;

d. *Bearbeiten:* jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;

e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten;

f. *Profiling:* jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen,

[3] SR **192.12**

insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;

g. *Bundesorgan:* Behörde und Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist;

h. *Verantwortlicher*: Bundesorgan oder private Person, das oder die – alleine oder zusammen mit anderen – über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet;

i. *Auftragsbearbeiter*: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.

2. Abschnitt: Allgemeine Datenschutzbestimmungen

Art. 4 Grundsätze

[1] Personendaten müssen rechtmässig bearbeitet werden.

[2] Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist.

[4] Personendaten dürfen nur so lange in einer Form aufbewahrt werden, welche die Identifizierung der betroffenen Person ermöglicht, als der Zweck der Bearbeitung es bedingt.

[5] Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden. Andernfalls sind die Daten zu vernichten.

[6] Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von besonders schützenswerten Personendaten und das Profiling muss die Einwilligung zudem ausdrücklich erfolgen.

Art. 5 Bekanntgabe ins Ausland

[1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde.

[2] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessen Schutz gewährleistet.

[3] Liegt kein Entscheid des Bundesrates nach Absatz 2 vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn ein geeigneter Schutz gewährleistet ist durch:

a. einen völkerrechtlichen Vertrag;

b. spezifische Garantien, insbesondere durch Vertrag, über die der Beauftragte vorgängig informiert wurde;

c. standardisierte Garantien, insbesondere durch Vertrag:
   1. welche der Beauftragte vorgängig genehmigt hat, oder
   2. welche der Beauftragte ausgestellt oder anerkannt hat;

d. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig genehmigt wurden:
   1. durch den Beauftragten, oder
   2. durch eine ausländische Behörde, die für den Datenschutz zuständig ist und die einem Staat angehört, der einen angemessenen Schutz gewährleistet.

[4] Hat der Beauftragte Einwände gegen die spezifischen Garantien nach Absatz 3 Buchstabe b, muss er den Verantwortlichen oder den Auftragsbearbeiter innert 30 Tagen nach Erhalt der Garantien informieren.

[5] Der Beauftragte teilt dem Verantwortlichen oder dem Auftragsbearbeiter spätestens sechs Monate nach Erhalt der vollständigen Unterlagen mit, ob die standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 1 oder die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 1 genehmigt sind oder nicht.

[6] Der Verantwortliche oder der Auftragsbearbeiter informieren den Beauftragten, wenn sie von den standardisierten Garantien nach Absatz 3 Buchstabe c Ziffer 2 Gebrauch machen. Sie teilen ihm die verbindlichen unternehmensinternen Datenschutzvorschriften nach Absatz 3 Buchstabe d Ziffer 2 mit.

[7] Der Bundesrat erstellt eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.

Art. 6 Bekanntgabe ins Ausland in Ausnahmefällen

[1] In Abweichung von Artikel 5 Absätze 1 bis 3 dürfen ausnahmsweise Personendaten ins Ausland bekannt gegeben werden, wenn:

a. die betroffene Person im Einzelfall eingewilligt hat;

b. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt;

c. die Bekanntgabe im Einzelfall unerlässlich ist für:
   1. die Wahrung eines überwiegenden öffentlichen Interesses, oder
   2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer Verwaltungsbehörde;

d. die Bekanntgabe im Einzelfall notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen

und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen;

e. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat;

f. die Daten aus einem gesetzlich vorgesehenen Register stammen, das zugänglich ist für die Öffentlichkeit oder für Personen mit einem schutzwürdigen Interesse, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind.

2 Der Verantwortliche oder der Auftragsbearbeiter teilt dem Beauftragten mit, wenn er Personendaten nach Absatz 1 Buchstaben b, c und d bekannt gibt.

Art. 7 Auftragsdatenbearbeitung

1 Die Bearbeitung von Personendaten kann durch Vereinbarung oder Gesetz einem Auftragsbearbeiter übertragen werden, wenn:

a. die Daten nur so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

2 Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit und die Rechte der betroffenen Person zu gewährleisten. Der Bundesrat präzisiert die weiteren Pflichten des Auftragsbearbeiters.

3 Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen einem anderen Auftragsbearbeiter übertragen.

4 Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

Art. 8 Empfehlungen der guten Praxis

1 Der Beauftragte erarbeitet Empfehlungen der guten Praxis, welche die Datenschutzvorschriften konkretisieren. Er zieht dazu die interessierten Kreise bei und berücksichtigt die Besonderheiten des jeweiligen Anwendungsbereichs sowie den Schutz von besonders schutzbedürftigen Personen.

2 Der Verantwortliche sowie interessierte Kreise können die Empfehlungen des Beauftragten ergänzen oder eigene Empfehlungen der guten Praxis ausarbeiten. Sie können ihre Empfehlungen dem Beauftragten zur Genehmigung vorlegen. Sind die Empfehlungen mit den Datenschutzvorschriften vereinbar, genehmigt er sie.

3 Er veröffentlicht die von ihm erarbeiteten sowie die von ihm genehmigten Empfehlungen der guten Praxis.

Art. 9 Einhaltung der Empfehlungen der guten Praxis

1 Befolgt der Verantwortliche die Empfehlungen der guten Praxis, hält er diejenigen Datenschutzvorschriften ein, welche die Empfehlungen konkretisieren.

[2] Die Datenschutzvorschriften können auch auf andere Weise eingehalten werden, als in Empfehlungen der guten Praxis vorgesehen.

Art. 10 Zertifizierung

[1] Der Verantwortliche und der Auftragsbearbeiter können ihre Datenbearbeitungsvorgänge von einer anerkannten, unabhängigen Zertifizierungsstelle beurteilen lassen.

[2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.

Art. 11 Sicherheit von Personendaten

[1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten die Sicherheit der Personendaten. Diese müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust geschützt werden.

[2] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Art. 12 Daten einer verstorbenen Person

[1] Der Verantwortliche muss kostenlos Einsicht in die Daten einer verstorbenen Person gewähren, wenn ein schutzwürdiges Interesse an der Einsicht vorliegt und:

a. die verstorbene Person die Einsicht zu Lebzeiten nicht ausdrücklich untersagt hat; oder

b. keine überwiegenden Interessen der verstorbenen Person oder von Dritten entgegenstehen.

[2] Ein schutzwürdiges Interesse wird bei Personen vermutet, die mit der verstorbenen Person in gerader Linie verwandt sind oder mit ihr bis zum Zeitpunkt des Todes verheiratet waren, in eingetragener Partnerschaft lebten oder mit ihr eine faktische Lebensgemeinschaft führten.

[3] Ein allfälliges Amts- oder Berufsgeheimnis kann nicht geltend gemacht werden.

[4] Jeder Erbe kann verlangen, dass der Verantwortliche Daten des Erblassers kostenlos löscht oder vernichtet, ausser:

a. der Erblasser hat dies zu Lebzeiten ausdrücklich untersagt; oder

b. der Löschung oder Vernichtung stehen überwiegende Interessen des Erblassers oder von Dritten entgegen.

[5] Vorbehalten bleiben spezielle Bestimmungen anderer Bundesgesetze.

3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters

Art. 13 Informationspflicht bei der Beschaffung von Personendaten

[1] Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden.

[2] Er teilt der betroffenen Person spätestens bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann, und eine transparente Datenbearbeitung gewährleistet ist, insbesondere:

a. die Identität und die Kontaktdaten des Verantwortlichen;

b. die bearbeiteten Personendaten oder die Kategorien der bearbeiteten Personendaten;

c. den Zweck der Bearbeitung.

[3] Werden Personendaten Dritten bekanntgegeben, so teilt er der betroffenen Person zudem die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger mit.

[4] Wird die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen, so teilt der Verantwortliche der betroffenen Person die Identität und Kontaktdaten des Auftragsbearbeiters sowie die Daten oder Kategorien von Daten, die er bearbeitet, mit.

[5] Werden die Personendaten nicht bei der betroffenen Person beschafft, so muss die betroffene Person spätestens bei der Speicherung der Daten informiert werden; werden die Daten nicht gespeichert, so muss die betroffene Person bei der ersten Bekanntgabe an Dritte informiert werden.

Art. 14 Ausnahmen von der Informationspflicht und Einschränkungen

[1] Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt.

[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht, wenn:

a. die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist; oder

b. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

[3] Der Verantwortliche kann die Übermittlung der Informationen einschränken, aufschieben oder darauf verzichten, wenn:

a. ein Gesetz im formellen Sinn dies vorsieht; oder

b. dies aufgrund überwiegender Interessen Dritter erforderlich ist.

[4] Darüber hinaus ist es möglich, die Übermittlung von Informationen einzuschränken, aufzuschieben oder darauf zu verzichten:

a. wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern und er die Personendaten nicht Dritten bekannt gibt;

b. wenn es sich beim Verantwortlichen um ein Bundesorgan handelt, falls eine der folgenden Voraussetzungen erfüllt ist:

   1. es ist wegen überwiegender öffentlicher Interessen, insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft, erforderlich; oder

   2. die Übermittlung der Information stellt den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage.

[5] Sobald der Grund für den Verzicht, die Einschränkung oder das Aufschieben der Information wegfällt, muss der Verantwortliche die Informationen mitteilen, ausser dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.

Art. 15 Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung

[1] Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.

[2] Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.

[3] Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.

Art. 16 Datenschutz-Folgenabschätzung

[1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche oder der Auftragsbearbeiter vorgängig eine Datenschutz-Folgenabschätzung durchführen.

[2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person zu verringern.

[3] Der Verantwortliche oder der Auftragsbearbeiter benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen.

[4] Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen oder dem Auftragsbearbeiter innerhalb von drei Monaten nach Erhalt aller erforderlichen Informationen mit.

Art. 17 Meldung von Verletzungen des Datenschutzes

[1] Der Verantwortliche meldet dem Beauftragten unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.

[2] Der Verantwortliche informiert ausserdem die betroffene Person, wenn es zum Schutz der betroffenen Person erforderlich ist oder der Beauftragte es verlangt.

[3] Aus den in Artikel 14 Absätze 3 und 4 erwähnten Gründen kann die für die Bearbeitung verantwortliche Person die Meldung an die betroffene Person einschränken, aufschieben oder darauf verzichten.

[4] Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung.

Art. 18 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

[1] Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen.

[2] Sie sind darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.

Art. 19 Weitere Pflichten

Der Verantwortliche und der Auftragsbearbeiter sind weiter zu Folgendem verpflichtet:

a. Sie dokumentieren ihre Datenbearbeitung;

b. Sie informieren die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Verletzungen des Datenschutzes sowie über Einschränkungen der Bearbeitung nach Artikel 25 Absatz 2 oder 34 Absatz 2 , es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.

4. Abschnitt: Rechte der betroffenen Person

Art. 20 Auskunftsrecht

[1] Jede Person kann vom Verantwortlichen kostenlos Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.

[2] Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente

Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt:

a. die Identität und die Kontaktdaten des Verantwortlichen;

b. die bearbeiteten Personendaten;

c. der Zweck der Bearbeitung;

d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e. das Vorliegen einer automatisierten Einzelentscheidung;

f. die verfügbaren Angaben über die Herkunft der Personendaten;

g. gegebenenfalls die Informationen nach Artikel 13 Absatz 3 und 4.

3 Wird aufgrund einer Datenbearbeitung eine Entscheidung gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.

4 Personendaten über die Gesundheit können der betroffenen Person durch einen von ihr bezeichneten Arzt mitgeteilt werden.

5 Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat.

6 Niemand kann im Voraus auf das Auskunftsrecht verzichten.

Art. 21 Einschränkung des Auskunftsrechts

1 Der Verantwortliche kann die Auskunft unter den Voraussetzungen von Artikel 14 Absätze 3 und 4 verweigern, einschränken oder aufschieben.

2 Der Verantwortliche muss angeben, weshalb er die Übermittlung der Information verweigert, einschränkt oder aufschiebt. Handelt es sich dabei um ein Bundesorgan, so kann es von der Begründung absehen, sofern dadurch die in Artikel 14 Absatz 4 Buchstabe b genannten Interessen gefährdet sein könnten.

Art. 22 Einschränkung des Auskunftsrechts für Medienschaffende

1 Werden Personendaten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet, kann der Verantwortliche aus einem der folgenden Gründe die Auskunft verweigern, einschränken oder aufschieben:

a. Die Daten geben Aufschluss über die Informationsquellen;

b. Es müsste dafür Einsicht in Entwürfe für Publikationen gewährt werden;

c. Die freie Meinungsbildung des Publikums würde gefährdet.

[2] Medienschaffende können die Auskunft zudem verweigern, einschränken oder aufschieben, wenn ihnen die Personendaten ausschliesslich als persönliche Arbeitsinstrumente dienen.

5. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch private Personen

Art. 23 Persönlichkeitsverletzungen

[1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen.

[2] Eine Persönlichkeitsverletzung liegt insbesondere vor:

a. wenn Personendaten entgegen den Grundsätzen nach den Artikeln 4-6 und 11 bearbeitet werden;

b. wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden;

c. wenn Dritten besonders schützenswerte Personendaten bekannt gegeben werden;

d. durch Profiling ohne ausdrückliche Einwilligung der betroffenen Person.

[3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

Art. 24 Rechtfertigungsgründe

[1] Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

[2] Ein überwiegendes Interesse der bearbeitenden Person ist möglicherweise gegeben, wenn dieser insbesondere:

a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet;

b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben;

c. Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person bearbeitet, wenn:

   1. es sich dabei nicht um besonders schützenswerte Personendaten handelt,

   2. Dritten nur Daten bekanntgegeben werden, welche diese für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen,

3. die betroffene Person volljährig ist;

d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet;

e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet, soweit:

1. die Daten anonymisiert werden, sobald der Zweck der Bearbeitung es erlaubt,

2. Dritten besonders schützenswerte Personendaten so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind,

3. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind;

f. Personendaten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.

Art. 25 Rechtsansprüche

[1] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g* - 28*l* des Zivilgesetzbuchs[4]. Die klagende Partei kann insbesondere verlangen, dass:

a. die Datenbearbeitung verboten wird;

b. die Bekanntgabe von Personendaten an Dritte untersagt wird;

c. Personendaten berichtigt, gelöscht oder vernichtet werden.

[2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die klagende Partei verlangen, dass bei den Daten ein Bestreitungsvermerk angebracht wird. Sie kann darüber hinaus verlangen, dass die Bearbeitung der bestrittenen Daten eingeschränkt wird.

[3] Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.

6. Abschnitt: Besondere Bestimmungen für die Datenbearbeitung durch Bundesorgane

Art. 26 Verantwortliches Organ und Kontrolle

[1] Für den Datenschutz ist das Bundesorgan verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt.

[4] SR **210**

[2] Bearbeiten Bundesorgane Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten, so regelt der Bundesrat die Kontrolle und die Verantwortung für den Datenschutz.

Art. 27 Rechtsgrundlagen

[1] Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht.

[2] Für die Bearbeitung besonders schützenswerter Personendaten, das Profiling oder den Erlass einer automatisierten Einzelentscheidung nach Artikel 15 Absatz 1 ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Eine Grundlage in einem Gesetz im materiellen Sinn ist ausreichend, wenn die folgenden Voraussetzungen erfüllt sind:

a. Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn klar festgelegte Aufgabe unentbehrlich; und

b. Die Bearbeitung birgt für die Persönlichkeit und die Grundrechte der betroffenen Person keine besonderen Risiken.

[3] In Abweichung von den Absätzen 1 und 2 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten ohne gesetzliche Grundlage bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Der Bundesrat bewilligt die Bearbeitung, sofern die Rechte der betroffenen Person nicht gefährdet sind;

b. Die betroffene Person hat in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt;

c. Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen.

Art. 28 Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen

[1] Der Bundesrat kann vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder das Profiling bewilligen, wenn:

a. die Aufgaben, aufgrund deren die Bearbeitung erforderlich ist, in einem bereits in Kraft stehenden Gesetz im formellen Sinn geregelt sind;

b. ausreichende Massnahmen getroffen werden, um eine Verletzung der Grundrechte der betroffenen Person zu verhindern; und

c. eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, zwingend erforderlich ist.

[2] Er holt vorgängig die Stellungnahme des Beauftragten ein.

[3] Das zuständige Bundesorgan legt dem Bundesrat spätestens innerhalb von zwei Jahren nach Aufnahme des Pilotversuchs einen Evaluationsbericht vor. Es schlägt darin die Fortführung oder die Einstellung der Bearbeitung vor.

[4] Die automatisierte Datenbearbeitung oder das Profiling müssen in jedem Fall abgebrochen werden, wenn innerhalb von fünf Jahren nach Aufnahme des Pilotversuchs kein Gesetz im formellen Sinn in Kraft getreten ist, das die erforderliche Rechtsgrundlage umfasst.

Art. 29 Bekanntgabe von Personendaten

[1] Bundesorgane dürfen Personendaten bekannt geben, wenn eine Rechtsgrundlage im Sinne von Artikel 27 Absätze 1 und 2 dies vorsieht.

[2] In Abweichung von Absatz 1 dürfen Bundesorgane im Einzelfall ausnahmsweise Personendaten bekannt geben, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Die Bekanntgabe der Daten ist für den Verantwortlichen oder für die Empfängerin oder den Empfänger zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich;

b. Die betroffene Person hat in die Bekanntgabe eingewilligt;

c. Die Bekanntgabe der Daten ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen;

d. Die betroffene Person hat ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt;

e. Der Empfänger macht glaubhaft, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren; der betroffenen Person ist vorher Gelegenheit zur Stellungnahme zu geben, es sei denn, dies ist unmöglich oder nur mit einem unverhältnismässigen Aufwand zu erreichen.

[3] Darüber hinaus dürfen Bundesorgane im Rahmen der behördlichen Information der Öffentlichkeit von Amtes wegen oder gestützt auf das Öffentlichkeitsgesetz vom 17. Dezember 2004[5] auch Personendaten bekannt geben, wenn:

a. die betreffenden Daten im Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe stehen; und

b. an der Bekanntgabe ein überwiegendes öffentliches Interesse besteht.

[4] Name, Vorname, Adresse und Geburtsdatum einer Person dürfen Bundesorgane auf Anfrage auch bekannt geben, wenn die Voraussetzungen von Absatz 1 oder 2 nicht erfüllt sind.

[5] SR **152.3**

[5] Sie dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste allgemein zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie Daten gestützt auf Absatz 3 bekannt geben. Besteht kein öffentliches Interesse mehr daran, die Daten allgemein zugänglich zu machen, so werden die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst gelöscht.

[6] Sie lehnen die Bekanntgabe ab, schränken sie ein oder verbinden sie mit Auflagen, wenn:

a. wesentliche öffentliche Interessen oder offensichtlich schutzwürdige Interessen der betroffenen Person es verlangen; oder

b. gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen.

Art. 30 Widerspruch gegen die Bekanntgabe von Personendaten

[1] Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen.

[2] Das Bundesorgan weist das Begehren ab, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. es besteht eine Rechtspflicht zur Bekanntgabe;

b. die Erfüllung seiner Aufgabe wäre sonst gefährdet.

[3] Artikel 29 Absatz 3 bleibt vorbehalten.

Art. 31 Angebot von Unterlagen an das Bundesarchiv

[1] In Übereinstimmung mit dem Archivierungsgesetz vom 26. Juni 1998[6] bieten die Bundesorgane dem Bundesarchiv alle Personendaten an, die sie nicht mehr ständig benötigen.

[2] Sie vernichten die vom Bundesarchiv als nicht archivwürdig bezeichneten Personendaten, ausser wenn diese:

a. anonymisiert sind;

b. zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.

Art. 32 Datenbearbeitung für Forschung, Planung und Statistik

[1] Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik bearbeiten, wenn:

[6] SR **152.1**

a. die Daten anonymisiert werden, sobald es der Zweck der Bearbeitung erlaubt;

b. das Bundesorgan privaten Personen besonders schützenswerte Personendaten so bekannt gibt, dass die betroffenen Personen nicht bestimmbar sind;

c. die Empfängerin oder der Empfänger die Daten nur mit Zustimmung des Bundesorgans weitergibt; und

d. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

[2] Die Artikel 4 Absatz 3, 27 Absätze 1 und 2 sowie Artikel 29 Absatz 1 sind nicht anwendbar.

Art. 33 Privatrechtliche Tätigkeit von Bundesorganen

[1] Handelt ein Bundesorgan privatrechtlich, so gelten die Bestimmungen für die Datenbearbeitung durch private Personen.

[2] Die Aufsicht richtet sich nach den Bestimmungen für Bundesorgane.

Art. 34 Ansprüche und Verfahren

[1] Wer ein schutzwürdiges Interesse hat, kann vom verantwortlichen Bundesorgan verlangen, dass es:

a. die widerrechtliche Bearbeitung der betreffenden Personendaten unterlässt;

b. die Folgen einer widerrechtlichen Bearbeitung beseitigt;

c. die Widerrechtlichkeit der Bearbeitung feststellt.

[2] Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so muss das Bundesorgan bei den Daten einen Bestreitungsvermerk anbringen und deren Bearbeitung einschränken.

[3] Die Gesuchstellerin oder der Gesuchsteller kann insbesondere verlangen, dass das Bundesorgan:

a. die betreffenden Personendaten berichtigt, löscht oder vernichtet;

b. seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, das Verbot der Bearbeitung, den Widerspruch gegen die Bekanntgabe nach Artikel 30 oder den Bestreitungsvermerk Dritten mitteilt oder veröffentlicht.

[4] Die Berichtigung, Löschung oder Vernichtung von Personendaten kann nicht verlangt werden in Bezug auf die Bestände öffentlich zugänglicher Bibliotheken, Bildungseinrichtungen, Museen, Archiven oder anderer öffentlicher Gedächtnisinstitutionen. Wenn die Gesuchstellerin oder der Gesuchsteller ein überwiegendes Interesse nachweisen kann, kann sie oder er jedoch verlangen, dass die Institution den Zugang zu den umstrittenen Daten beschränkt.

[5] Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 18. Dezember 1968[7]. Die Ausnahmen nach den Artikeln 2 und 3 des Verwaltungsverfahrensgesetzes gelten nicht.

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

Ist ein Verfahren betreffend den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, im Sinne des Öffentlichkeitsgesetzes[8] hängig, so kann die betroffene Person im Rahmen dieses Verfahrens diejenigen Rechte geltend machen, die ihr nach Artikel 34 bezogen auf diejenigen Dokumente zustehen, die Gegenstand des Zugangsverfahrens sind.

Art. 36 Register

[1] Die verantwortlichen Bundesorgane melden dem Beauftragten ihre Datenbearbeitungstätigkeiten.

[2] Der Beauftragte führt ein Register der Datenbearbeitungstätigkeiten. Das Register ist öffentlich.

[3] Datenbearbeitungstätigkeiten müssen vor Beginn der Tätigkeit gemeldet werden.

7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte

Art. 37 Ernennung und Stellung

[1] Die oder der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt. Die Wahl ist durch die Bundesversammlung zu genehmigen.

[2] Das Arbeitsverhältnis der oder des Beauftragten richtet sich, soweit dieses Gesetz nichts anderes vorsieht, nach dem Bundespersonalgesetz vom 24. März 2000 (BPG)[9].

[3] Die oder der Beauftragte übt ihre bzw. seine Funktion unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder zu erhalten. Sie oder er ist administrativ der Bundeskanzlei zugeordnet.

[4] Sie oder er verfügt über ein ständiges Sekretariat und ein eigenes Budget. Sie oder er stellt sein Personal an.

[5] Die oder der Beauftragte unterstehen nicht dem Beurteilungssystem nach Artikel 4 Absatz 3 BPG.

[7] SR **172.021**
[8] SR **152.3**
[9] SR **172.220.1**

Art. 38 Wiederwahl und Beendigung der Amtsdauer

[1] Die oder der Beauftragte kann zwei Mal wiedergewählt werden.

[2] Verfügt der Bundesrat nicht spätestens sechs Monate vor Ablauf der Amtsdauer aus sachlich hinreichenden Gründen die Nichtwiederwahl, so ist der oder die Beauftragte für eine neue Amtsdauer wiedergewählt.

[3] Die oder der Beauftragte kann den Bundesrat unter Einhaltung einer Frist von sechs Monaten um Entlassung auf ein Monatsende ersuchen.

[4] Der Bundesrat kann die Beauftragte oder den Beauftragten vor Ablauf der Amtsdauer des Amtes entheben, wenn diese oder dieser:

a. vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat; oder

b. die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.

Art. 39 Nebenbeschäftigung

[1] Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, der Verwaltung, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig sein.

[2] Der Bundesrat kann der oder dem Beauftragten gestatten, eine Nebenbeschäftigung nach Absatz 1 auszuüben, wenn dadurch die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.

Art. 40 Aufsicht

[1] Der Beauftragte überwacht die Einhaltung der Datenschutzvorschriften des Bundes.

[2] Bundesverwaltungsbehörden, die nach einem anderen Bundesgesetz Private oder Organisationen ausserhalb der Bundesverwaltung beaufsichtigen, laden den Beauftragten zur Stellungnahme ein, bevor sie eine Verfügung treffen, die Fragen des Datenschutzes berührt.

[3] Führt der Beauftragte gegen die gleiche Partei ein eigenes Verfahren, so haben die beiden Behörden ihre Verfahren zu koordinieren.

Art. 41 Untersuchung

[1] Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.

[2] Das Bundesorgan oder die private Person erteilt dem Beauftragten die von ihm verlangten Auskünfte und stellen ihm alle für die Untersuchung notwendigen Unter-

lagen zur Verfügung. Das Auskunftsverweigerungsrecht richtet sich nach den Artikeln 16 und 17 des Verwaltungsverfahrensgesetzes[10].

3 Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte vergeblich versucht, Auskünfte und Unterlagen einzuholen, so kann der Beauftragte im Rahmen einer Untersuchung:

a. ohne Vorankündigung Räumlichkeiten inspizieren;

b. Zugang zu allen notwendigen Daten und Informationen verlangen.

4 Ausserhalb eines Untersuchungsverfahrens darf der Beauftragte überprüfen, ob private Personen oder Bundesorgane die Datenschutzvorschriften einhalten und sie beraten.

5 Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung.

Art. 42 Vorsorgliche Massnahmen

1 Der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete rechtliche Interessen zu schützen oder Beweismittel zu sichern.

2 Für die Vollstreckung vorsorglicher Massnahmen kann der Beauftragte andere Bundesbehörden sowie die kantonalen und kommunalen Polizeibehörden beiziehen.

Art. 43 Verwaltungsmassnahmen

1 Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden.

2 Der Beauftragte kann zudem die Bekanntgabe ins Ausland aufschieben oder untersagen, wenn sie gegen die Voraussetzungen nach Artikel 5 oder 6 oder gegen spezifische Bestimmungen betreffend die Bekanntgabe von Personendaten ins Ausland in anderen Bundesgesetzen, verstösst.

Art. 44 Verfahren

1 Das Untersuchungsverfahren sowie Verfügungen nach den Artikeln 42 und 43 richten sich nach dem Verwaltungsverfahrensgesetz[11].

2 Partei sind lediglich das Bundesorgan oder die private Person, gegen das oder die eine Untersuchung eröffnet wurde.

3 Beschwerden gegen vorsorgliche Massnahmen nach Artikel 42 kommt keine aufschiebende Wirkung zu.

10 SR **172.021**
11 SR **172.021**

[4] Der Beauftragte kann Beschwerdeentscheide des Bundesverwaltungsgerichts anfechten.

Art. 45 Anzeigepflicht

Erfährt der Beauftragte im Rahmen der Ausübung seiner Funktion von Straftaten, die von Amtes wegen verfolgt werden, so teilt er dies den Strafverfolgungsbehörden mit.

Art. 46 Amtshilfe zwischen schweizerischen Behörden

[1] Bundesbehörden und kantonale Behörden geben dem Beauftragten die Informationen und Personendaten bekannt, welche für den Vollzug dieses Gesetzes erforderlich sind.

[2] Der Beauftragte gibt den folgenden Behörden die Informationen und Personendaten bekannt, die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind:

a. den für den Datenschutz zuständigen kantonalen Behörden;

b. den zuständigen Strafverfolgungsbehörden, falls es um die Anzeige einer Straftat gemäss Artikel 45 geht;

c. den Bundesbehörden sowie den kantonalen und kommunalen Polizeibehörden für den Vollzug der Massnahmen gemäss Artikel 41 Absatz 3, 42 und 43.

Art. 47 Amtshilfe zwischen schweizerischen und ausländischen Behörden

[1] Der Beauftragte kann von ausländischen Behörden, die für den Datenschutz zuständig sind, die Bekanntgabe von Informationen und Personendaten ersuchen, die für die Erfüllung seiner gesetzlichen Aufgaben erforderlich sind. Dazu darf er insbesondere folgende Angaben zur Verfügung stellen:

a. die Identität des Verantwortlichen, des Auftragsbearbeiters oder anderer beteiligter Dritter;

b. Kategorien von betroffenen Personen;

c. die Identität der betroffenen Personen, falls:
   1. die betroffenen Personen eingewilligt haben, oder
   2. die Mitteilung der Identität der betroffenen Personen unumgänglich ist, um die gesetzlichen Aufgaben des Beauftragten oder der ausländischen Behörde zu erfüllen;

d. bearbeitete Personendaten oder Kategorien von bearbeiteten Personendaten;

e. den Zweck der Datenbearbeitung;

f. Empfängerinnen und Empfänger oder Kategorien von Empfängerinnen und Empfängern;

g. technische und organisatorische Massnahmen.

[2] Der Beauftragte kann der ausländischen Behörde Amtshilfe gewähren und ihr die Informationen gemäss Absatz 1 zur Verfügung stellen, wenn sie folgende Voraussetzungen erfüllt:

a. Sie verpflichtet sich, die zur Verfügung gestellten Informationen und Personendaten, nicht für andere Zwecke zu verwenden, als im Amtshilfegesuch angegeben;

b. Sie verpflichtet sich, ähnlichen Amtshilfegesuchen der Schweiz Folge zu leisten;

c. Sie verpflichtet sich zur Wahrung des Amts- und Berufsgeheimnisses;

d. Sie verpflichtet sich, die erhaltenen Informationen und Personendaten nur mit ausdrücklicher Genehmigung des Beauftragten an Dritte zu übermitteln;

e. Sie verpflichtet sich, die Auflagen und Nutzungsbeschränkungen des Beauftragten einzuhalten.

Art. 48 Information

[1] Der Beauftragte erstattet der Bundesversammlung periodisch sowie bei Bedarf Bericht. Er übermittelt den Bericht gleichzeitig dem Bundesrat. Die periodischen Berichte werden veröffentlicht.

[2] In Fällen von allgemeinem Interesse informiert er die Öffentlichkeit über seine Feststellungen und Verfügungen.

Art. 49 Weitere Aufgaben

Der Beauftragte nimmt darüber hinaus insbesondere folgende Aufgaben wahr:

a. Er informiert und berät die Organe des Bundes und der Kantone sowie private Personen bei Fragen des Datenschutzes.

b. Er arbeitet mit schweizerischen und ausländischen Behörden, die für den Datenschutz zuständig sind, zusammen.

c. Er sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz.

d. Er erteilt der betroffenen Person auf Anfrage Auskunft darüber, wie sie ihre Rechte ausüben kann.

e. Er nimmt Stellung zu Erlassentwürfen und Massnahmen des Bundes, welche die Datenbearbeitung betreffen.

f. Er nimmt die ihm durch das Öffentlichkeitsgesetz[12] übertragenen Aufgaben wahr.

[12] SR **152.3**

8. Abschnitt: Strafbestimmungen

Art. 50 Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten

[1] Mit Busse bis zu 500 000 Franken werden private Personen auf Antrag bestraft:

a. die ihre Pflichten nach den Artikeln 13, 15 und 20 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen;

b. die es vorsätzlich unterlassen:

1. die betroffene Person nach Artikel 13 Absätze 1 und 5, 15 und 17 Absatz 2 die betroffene Person zu informieren; oder

2. der betroffenen Person die Angaben nach Artikel 13 Absätze 2, 3 und 4 zu liefern.

c. die es vorsätzlich unterlassen, dem Beauftragten die Ergebnisse ihrer Datenschutz-Folgenabschätzung mitzuteilen (Art. 16 Abs. 3).

[2] Mit Busse bis zu 500 000 Franken werden private Personen bestraft, wer vorsätzlich:

a. die es unterlassen, den Beauftragten entsprechend Artikel 5 Absatz 3 Buchstabe b und Absatz 6 zu informieren;

b. die es unterlassen, dem Beauftragten die standardisierten Garantien oder die verbindlichen unternehmensinternen Datenschutzvorschriften zur Genehmigung zu unterbreiten (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d Ziff. 1);

c. dem Beauftragten bei der Untersuchung (Art. 41 Abs. 2) falsche Auskünfte erteilen oder die Mitwirkung verweigern;

e. es unterlassen, dem Beauftragten Verletzungen des Datenschutzes nach Artikel 17 Absatz 1 zu melden;

f. einer Verfügung des Beauftragten nicht Folge leistet.

[3] Mit Busse bis zu 500 000 Franken werden private Personen auf Antrag bestraft, die es vorsätzlich unterlassen:

a. die Empfänger, denen Personendaten übermittelt wurden, nach Artikel 19 Buchstabe b zu informieren;

b. den Verantwortlichen über eine unbefugte Datenbearbeitung nach Artikel 17 Absatz 4 zu informieren.

[4] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.

Art. 51 Verletzung der Sorgfaltspflichten

[1] Mit Busse bis zu 500'000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich:

a. unter Verstoss gegen Artikel 5 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 6 erfüllt sind, Personendaten ins Ausland übermitteln;

b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 7 Absätze 1 und 2 erfüllt sind;

c. es unterlassen, die notwendigen Massnahmen zu treffen, um Daten gegen eine unbefugte Datenbearbeitung oder Verlust zu schützen (Art. 11);

d. es unterlassen, eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 16);

e. es unterlassen, die Vorkehren nach Artikel 18 zu treffen;

f. ihre Datenbearbeitung nicht nach Artikel 19 Buchstabe a dokumentiert.

[2] Wer fahrlässig handelt, wird mit einer Busse von höchstens 250 000 Franken bestraft.

Art. 52 Verletzung der beruflichen Schweigepflicht

[1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird auf Antrag bestraft, wer vorsätzlich geheime Personendaten bekannt gibt:

a. von denen er im Rahmen seiner beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat;

b. welche er selbst zu kommerziellen Zwecken bearbeitet hat.

[2] Gleich wird bestraft, wer vorsätzlich geheime Personendaten bekannt gibt, von denen er bei der Tätigkeit für einen Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat.

[3] Das Bekanntgeben geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

Art. 53 Übertretungen in Geschäftsbetrieben

Von der Ermittlung der strafbaren Personen kann Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt werden, wenn die Busse 100 000 Franken nicht überschreitet und die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974[13] über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären.

Art. 54 Anwendbares Recht und Verfahren

Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen.

Art. 55 Verfolgungsverjährung für Übertretungen

Bei Übertretungen verjährt die Strafverfolgung in fünf Jahren, nachdem die Tat begangen wurde.

[13] SR **313.0**

9. Abschnitt: Abschluss von Staatsverträgen

Art. 56

Der Bundesrat kann Staatsverträge abschliessen betreffend:

a. die internationale Zusammenarbeit zwischen Datenschutzbehörden;

b. die gegenseitige Anerkennung eines angemessenen Schutzes für die Bekanntgabe von Personendaten ins Ausland.

10. Abschnitt: Schlussbestimmungen

Art. 57 Vollzug durch die Kantone

[1] Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, unterstehen den Artikeln 1-22, 26, 27, 29 bis 32, 34 Absätze 1-3 und 36 dieses Gesetzes, soweit sie nicht kantonalen Datenschutzvorschriften unterstehen, die einen angemessenen Schutz der Daten gewährleisten.

[2] Die Kantone bestimmen ein Organ, das die Einhaltung der Datenschutzvorschriften überwacht. Die Artikel 41-43, 48 und 49 gelten sinngemäss.

Art. 58 Aufhebung und Änderung anderer Erlasse

Die Aufhebung und Änderungen anderer Erlasse werden im Anhang geregelt.

Art. 59 Übergangsbestimmung

Zwei Jahre nach Inkrafttreten dieses Gesetzes müssen die für Verantwortlichen sowie der Auftragsbearbeiter in der Lage sein:

a. eine Datenschutz-Folgenabschätzung nach Artikel 16 vornehmen;

b. für Datenbearbeitungen, die im Zeitpunkt des Inkrafttretens bereits durchgeführt wurden, die Massnahmen nach den Artikeln 18 und 19 Buchstabe a zu treffen.

Art. 60 Referendum und Inkrafttreten

[1] Dieses Gesetz untersteht dem fakultativen Referendum.

[2] Der Bundesrat bestimmt das Inkrafttreten.

Anhang
(Art. 58)

Aufhebung und Änderung anderer Erlasse

I

Das Bundesgesetz vom 19. Juni 1992[14] über den Datenschutz wird aufgehoben.

II

Die nachstehenden Bundesgesetze werden wie folgt geändert:

1. Bürgerrechtsgesetz vom 29. September 1952[15]

Art. 49a Abs. 1

[1] Das Bundesamt kann zur Erfüllung seiner Aufgaben nach diesem Gesetz Personendaten bearbeiten, einschliesslich besonders schützenswerter Personendaten über religiöse Ansichten, politische Tätigkeiten, die Gesundheit, Massnahmen der sozialen Hilfe und verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen. Dazu kann es eine Datenbank oder Akten führen.

2. Ausländergesetz vom 16. Dezember 2005[16]

Art. 101 Bearbeitung von Personendaten

Das SEM, die zuständigen Ausländerbehörden der Kantone und, in seinem Zuständigkeitsbereich, das Bundesverwaltungsgericht können Personendaten, einschliesslich besonders schützenswerter Personendaten, von Ausländerinnen und Ausländern sowie von an Verfahren nach diesem Gesetz beteiligten Dritten bearbeiten oder bearbeiten lassen, soweit sie diese Daten zur Erfüllung ihrer gesetzlichen Aufgaben benötigen.

[14] SR **235.1**
[15] SR **141.0**
[16] SR **142.20**

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

2 In Abweichung von Absatz 1 dürfen einem Drittstaat in folgenden Fällen Personendaten bekannt gegeben werden:

a. die betroffene Person hat ihre Einwilligung nach Artikel 4 Absatz 6 des Datenschutzgesetzes vom ... (DSG)[17] erteilt;

b. die Bekanntgabe ist erforderlich, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen;

Art. 111f zweiter Satz

Aufgehoben

3. Asylgesetz vom 26. Juni 1998[18]

Art. 96 Abs. 1 und 6

1 Das SEM, die Beschwerdebehörden sowie die mit Aufgaben nach diesem Gesetz beauftragten privaten Organisationen können Personendaten, einschliesslich besonders schützenswerter Personendaten nach Artikel 3 Buchstabe c des Datenschutzgesetzes vom … (DSG)[19] einer asylsuchenden oder schutzbedürftigen Person und ihrer Angehörigen bearbeiten oder bearbeiten lassen, soweit sie diese zur Erfüllung ihrer gesetzlichen Aufgaben benötigen.

Art. 99 Abs. 6 erster Satz

6 Ohne die Zustimmung des Verantwortlichen dürfen einem Drittstaat keine Personendaten bekanntgegeben werden, die nach Absatz 4 übermittelt wurden.

Art. 99a Abs. 2 Bst. a

2 MIDES dient:

a. der Bearbeitung von Personendaten von Asylsuchenden und Schutzbedürftigen, einschliesslich besonders schützenswerter Personendaten nach Artikel 3 Buchstabe c DSG[20]; und

[17] SR ...
[18] SR **142.31**
[19] SR ...
[20] SR ...

Art. 100 Abs. 2

2 Diese Informationssysteme können besonders schützenswerte Personendaten enthalten, soweit dies zur Erfüllung der gesetzlichen Aufgabe notwendig ist.

Art. 102 Abs. 1 dritter Satz und Abs. 2

1 … Sofern es erforderlich ist, können auch in den Texten enthaltene Personendaten, namentlich Personalien, sowie besonders schützenswerte Personendaten gespeichert werden.

2 Auf Datenbanken und Akten, die besonders schützenswerte Personendaten enthalten, haben nur Mitarbeiterinnen und Mitarbeiter des SEM und des Bundesverwaltungsgerichts Zugriff.

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

2 Gewährleistet ein Drittstaat keinen angemessenen Schutz der Daten, so können ihm in besonderen Fällen Personendaten bekannt gegeben werden, wenn:

a. die betroffene Person ihre Einwilligung nach Artikel 4 Absatz 6 des Datenschutzgesetzes vom … (DSG)[21] erteilt hat;

b. die Bekanntgabe erforderlich ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen;

Art. 102e zweiter Satz

Aufgehoben

4. Bundesgesetz vom 20. Juni 2003 über das Informationssystem für den Ausländer- und den Asylbereich[22]

Art. 4 Abs. 2

2 Im Informationssystem können besonders schützenswerte Personendaten nach Artikel 3 Buchstabe c des Datenschutzgesetzes vom … (DSG)[23] bearbeitet werden, soweit dies zur Erfüllung der Aufgaben nach Artikel 3 unerlässlich ist.

21 SR ...
22 SR **142.51**
23 SR ...

5. Öffentlichkeitsgesetz vom 17. Dezember 2004[24]

Art. 7 Abs. 2 und 3

[2] Der Zugang zu amtlichen Dokumenten wird eingeschränkt, aufgeschoben oder verweigert, wenn durch seine Gewährung die Privatsphäre Dritter beeinträchtigt werden kann.

[3] In Abweichung von Absatz 2 kann die Behörde ausnahmsweise den Zugang zu amtlichen Dokumenten gewähren, wenn ein überwiegendes öffentliches Interesse am Zugang besteht.

Art. 11 Abs. 1

[1] Zieht die Behörde in Erwägung, den Zugang zu Dokumenten zu gewähren, die Personendaten von Dritten enthalten, oder Artikel 7 Absatz 3 anzuwenden, gibt sie den betroffenen Dritten die Gelegenheit zur Stellungnahmen innert zehn Tagen.

Art. 12 Abs. 3

[3] Die Behörde schiebt den Zugang zu amtlichen Dokumenten, die Personendaten enthalten, oder den Zugang nach Artikel 7 Absatz 3 bis zur Klärung der Rechtslage auf.

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

[2] Im Übrigen erlässt die Behörde eine Verfügung, wenn sie in Abweichung von der Empfehlung:

c. nach Artikel 7 Absatz 3 den Zugang zu einem amtlichen Dokument gewähren will.

6. Verwaltungsverfahrensgesetz vom 20. Dezember 1968[25]

Vor dem Titel des Vierten Abschnitts einfügen

Art. 71a

O. Schutz von Personendaten

[1] Die datenschutzrechtlichen Ansprüche werden im hängigen Beschwerdeverfahren beurteilt und unterliegen den entsprechenden Rechtsmitteln.

[2] Die Datenbearbeitung durch die Beschwerdeinstanz im Rahmen eines Beschwerde- oder Revisionsverfahrens ist von der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten ausgenommen.

[24] SR **152.3**
[25] SR **172.021**

7. Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997[26]

Art. 57h Abs. 1 zweiter Satz

[1] … Dieses System kann besonders schützenswerte Personendaten enthalten, die sich aus dem Schriftverkehr oder aus der Art des Geschäftes ergeben. ….

Art. 57j Abs. 2

[2] ... Die Datenbearbeitung nach diesem Abschnitt kann auch besonders schützenswerte Personendaten umfassen.

Art. 57l Bst. b Ziff. 4

Die Bundesorgane dürfen Personendaten, die bei der Nutzung der elektronischen Infrastruktur anfallen, zu folgenden Zwecken aufzeichnen:

b. Daten über die Nutzung der elektronischen Infrastruktur:

4. zum Nachvollzug des Zugriffs auf die elektronische Infrastruktur,

8. Bundespersonalgesetz vom 24. März 2000[27]

Art. 27 Abs. 2, Einleitungssatz und Bst. b

[2] Die Ausführungsbestimmungen regeln im Rahmen des Datenschutzgesetzes vom …[28]:

b. die Voraussetzungen und die Zuständigkeit für die Bearbeitung besonders schützenswerter Personendaten nach Artikel 3 Buchstabe c des Datenschutzgesetzes vom … (DSG); die Bearbeitung dieser Daten ist nur zulässig, sofern sie für die Personalentwicklung notwendig ist und die betroffene Person ihr schriftlich zugestimmt hat;

Art. 27d Abs. 2 und Abs. 4 Einleitungssatz

[2] Die PSB kann die folgenden für die Erfüllung ihrer Aufgaben notwendigen besonders schützenswerten Personendaten der Klientinnen und Klienten bearbeiten:

[4] Die PSB kann den folgenden Personen und Stellen die in Absatz 2 genannten besonders schützenswerten Personendaten zugänglich machen, sofern sie diese für die Erfüllung ihrer Aufgaben benötigen:

[26] SR **172.010**
[27] SR **172.220.1**
[28] SR ...

9. Zivilgesetzbuch[29]

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

[3] Der Bundesrat regelt im Rahmen des Gesetzes und unter Mitwirkung der Kantone:

3. die zur Sicherstellung des Datenschutzes und der Datensicherheit erforderlichen organisatorischen und technischen Massnahmen sowie die Aufsicht über die Einhaltung der Datenschutzvorschriften,

[4] Der Bundesrat kann die Ansprüche der betroffenen Personen ganz oder teilweise abweichend von Artikel 34 Absätze 1-3 des Datenschutzgesetzes vom …[30] regeln, wenn der Zweck der zentralen Datenbank dies erfordert.

10. Bundesgesetz vom 24. März 2000 über die Bearbeitung von Personendaten im Eidgenössischen Departement für auswärtige Angelegenheiten[31]

Art. 1 zweiter Satz

[1]… Die Bearbeitung von besonders schützenswerten Personendaten und das Profiling sind zulässig.

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

[1] Zur Planung und Durchführung der Einsätze für die Friedensförderung, die Stärkung der Menschenrechte und die humanitäre Hilfe können die zuständigen Stellen des Departements über die an solchen Einsätzen beteiligten Personen eine Datenbank oder Akten führen.

[2] Die Bearbeitung von besonders schützenswerten Personendaten und das Profiling sind für diesen Zweck zulässig.

Art. 5 Abs. 1 Einleitungssatz

[1] Zur Erfüllung der völkerrechtlichen Verpflichtungen der Schweiz führen das Staatssekretariat und die ständige Mission der Schweiz bei den internationalen Organisationen in Genf Datenbanken und Akten über:

Art. 6 Bst. a

Der Bundesrat erlässt Ausführungsbestimmungen über:

a. Organisation und Betrieb der Datenbanken und die Aktenführung;

[29] SR **210**
[30] SR ...
[31] SR **235.2**

11. Zivilprozessordnung[32]

Art. 20 Bst. d

Für die folgenden Klagen und Begehren ist das Gericht am Wohnsitz oder Sitz einer der Parteien zuständig:

d. Klagen und Begehren nach dem Datenschutzgesetz vom …[33],

Art. 99 Abs. 3 Bst. d

[3] Keine Sicherheit ist zu leisten:

d. im Verfahren wegen einer Streitigkeit nach dem Datenschutzgesetz vom …[34].

Art. 113 Abs. 2 Bst. g

[2] Keine Gerichtskosten werden gesprochen in Streitigkeiten:

g. nach dem Datenschutzgesetz vom …[35].

Art. 114 Bst. f

Im Entscheidverfahren werden keine Gerichtskosten gesprochen bei Streitigkeiten:

f. nach dem Datenschutzgesetz vom …[36].

Art. 243 Abs. 2 Bst. d

[2] Es gilt ohne Rücksicht auf den Streitwert für Streitigkeiten:

d. zur Durchsetzung der Ansprüche nach den Artikeln 12 und 20 des Datenschutzgesetzes vom …[37];

12. Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht[38]

Art. 130 Abs. 3

Klagen zur Durchsetzung eines Auskunfts- oder Einsichtsrechts im Zusammenhang mit der Bearbeitung von Personendaten können bei den in Artikel 129 genannten

[32] SR **272**
[33] SR ...
[34] SR ...
[35] SR ...
[36] SR ...
[37] SR ...
[38] SR **291**

Gerichten oder bei den schweizerischen Gerichten am Ort, wo der betreffende Vorgang stattfindet, eingereicht werden.

13. Strafgesetzbuch[39]

*Art. 179^novies^*

Wer unbefugt Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Vor dem 4. Titel einfügen

*Art. 179^decies^*

Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils

Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.

14. Bundesgesetz vom 22. März 1974 über das Verwaltungsstrafrecht[40]

Gliederungstitel nach Art. 18

Dritter Abschnitt: Schutz von Personendaten

Nach dem Gliederungstitel des 3. Abschnitts die Artikel 18a–18g einfügen

Art. 18a

A. Schutz von Personendaten

I. Beschaffung von Personendaten

[1] Personendaten sind bei der betroffenen Person oder für diese erkennbar zu beschaffen, wenn dadurch das Verfahren nicht gefährdet oder unverhältnismässig aufwendig wird.

[2] Erfolgte die Beschaffung von Personendaten ohne Wissen der betroffenen Person, so ist diese umgehend darüber zu informieren. Die Information kann zum Schutze überwiegender öffentlicher oder privater Interessen unterlassen oder aufgeschoben werden.

39 SR **311.0**
40 SR **313.0**

Art. 18b

II. Bearbeitung von Personendaten

Bei der Bearbeitung von Personendaten sieht die Verwaltungsbehörde des Bundes angemessene Massnahmen vor, damit so weit wie möglich unterschieden werden zwischen:

a. verschiedenen Kategorien betroffener Personen;

b. auf Fakten und auf persönlichen Einschätzungen beruhenden Personendaten.

Art. 18c

III. Bekanntgabe und Verwendung von Personendaten bei hängigem Strafverfahren

Die Verwaltungsbehörde des Bundes darf Personendaten aus einem hängigen Verwaltungsstrafverfahren zur Verwendung in einem anderen hängigen Verfahren bekannt geben, wenn anzunehmen ist, dass die Personendaten wesentliche Aufschlüsse zum Sachverhalt geben können.

Art. 18d

IV. Auskunftsrechte bei hängigem Verfahren

Solange ein Verfahren hängig ist, haben die Parteien und die anderen Verfahrensbeteiligten nach Massgabe des ihnen zustehenden Akteneinsichtsrechts das Recht auf Auskunft über die sie betreffenden Personendaten.

Art. 18e

V. Richtigkeit der Personendaten

[1] Die Verwaltungsbehörde des Bundes berichtigt unverzüglich unrichtige Personendaten.

[2] Sie benachrichtigt die Behörde, die ihr die Personendaten übermittelt oder bereitgestellt oder der sie diese bekannt gegeben hat, unverzüglich über die Berichtigung.

Art. 18f Ansprüche und Verfahren

VI. Ansprüche und Verfahren

[1] Die datenschutzrechtlichen Ansprüche werden im hängigen Verwaltungsstrafverfahren beurteilt und unterliegen den entsprechenden Rechtsmitteln.

[2] Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte ist für die Aufsicht über die Datenbearbeitung durch die Verwaltungsbehörde des Bundes in diesem Verfahren nicht zuständig, bis der Endentscheid nicht in Rechtskraft erwachsen ist.

15. Militärstrafprozess vom 23. März 1979[41]

Gliederungstitel nach Art. 25

Sechstes Kapitel: Schutz von Personendaten

Nach dem Gliederungstitel des 6. Kapitels die Artikel 25a–25e einfügen

Art. 25a Beschaffung von Personendaten

[1] Personendaten sind bei der betroffenen Person oder für diese erkennbar zu beschaffen, wenn dadurch das Verfahren nicht gefährdet oder unverhältnismässig aufwendig wird.

[2] Erfolgte die Beschaffung von Personendaten ohne Wissen der betroffenen Person, so ist diese umgehend darüber zu informieren. Die Information kann zum Schutze überwiegender öffentlicher oder privater Interessen unterlassen oder aufgeschoben werden.

Art. 25b Bearbeitung von Personendaten

Bei der Bearbeitung von Personendaten sieht die militärische Strafbehörde angemessene Massnahmen vor, damit so weit wie möglich unterschieden werden kann zwischen:

a. verschiedenen Kategorien betroffener Personen;

b. auf Fakten und auf persönlichen Einschätzungen beruhenden Personendaten.

Art. 25c Bekanntgabe und Verwendung von Personendaten bei hängigem Strafverfahren

Die militärische Strafbehörde darf aus einem hängigen militärischen Strafverfahren Personendaten zwecks Verwendung in einem anderen hängigen Verfahren bekannt geben, wenn anzunehmen ist, dass die Personendaten wesentliche Aufschlüsse zum Sachverhalt geben können.

Art. 25d Auskunftsrechte bei hängigem Verfahren

Solange ein Verfahren hängig ist, haben die Parteien und die anderen Verfahrensbeteiligten nach Massgabe des ihnen zustehenden Akteneinsichtsrechts das Recht auf Auskunft über die sie betreffenden Personendaten.

Art. 25e Richtigkeit der Personendaten

[1] Die militärische Strafbehörde berichtigt unverzüglich unrichtige Personendaten.

[41] SR **322.1**

[2] Sie benachrichtigt die Behörde, die ihr diese Personendaten übermittelt oder bereitgestellt oder der sie diese bekannt gegeben hat, unverzüglich über die Berichtigung.

16. Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes [42]

Art. 3 Abs. 2

[2] Im Rahmen dieses Gesetzes sind die Polizeibehörden des Bundes zur Bearbeitung besonders schützenswerter Personendaten sowie zum Profiling befugt und dürfen den kanonalen Polizei- und Strafverfolgungsbehörden sowie anderen schweizerischen oder ausländischen Behörden solche Daten bekannt geben. Personendaten dürfen bearbeitet werden, soweit und solange es zur Erfüllung der gesetzlichen Aufgaben notwendig ist.

Art. 5 Sachüberschrift Abs. 2

Datenbearbeitung zur internen Kontrolle

Aufgehoben

17. ETH-Gesetz vom 4. Oktober 1991[43]

Art. 36a Abs. 1 erster Satz

[1] Der ETH-Rat, die ETH und die Forschungsanstalten betreiben je ein Personalinformationssystem, in welchem auch besonders schützenswerte Personendaten bearbeitet werden können.

Art. 36b Abs. 1 und 5 zweiter Satz

[1] Jede ETH betreibt für die Verwaltung der Daten der Studienanwärter, Studierenden, Doktoranden und Hörer ein Informationssystem, in dem auch besonders schützenswerte Personendaten bearbeitet werden können.

[5] ... Die Bekanntgabe besonders schützenswerter Personendaten durch ein Abrufverfahren ist nur an die für die Studienadministration zuständigen Stellen innerhalb jeder ETH gestattet.

[42] SR **361**
[43] SR **414.110**

18. Sportförderungsgesetz vom 17. Juni 2011[44]

Art. 21 Abs. 3 Einleitungssatz

3 Die Dopingkontrollstellen nach Absatz 2 sind berechtigt, die im Zusammenhang mit ihrer Kontrolltätigkeit erhobenen Personendaten, einschliesslich besonders schützenswerter Personendaten, zu bearbeiten und an die zuständige Stelle weiterzuleiten für:

Art. 25 Abs. 1 Einleitungssatz

1 Die nach Artikel 19 für Massnahmen gegen Doping zuständige Stelle ist berechtigt, Personendaten, einschliesslich besonders schützenswerter Personendaten, zum Zweck der Dopingbekämpfung mit anerkannten ausländischen oder internationalen Dopingbekämpfungsstellen auszutauschen, wenn ein solcher Datenaustausch notwendig ist:

19. Bundesgesetz vom 17. Juni 2011 über die Informationssysteme des Bundes im Bereich Sport[45]

Art. 1 Einleitungssatz

Dieses Gesetz regelt die Bearbeitung von besonders schützenswerten Personendaten (Daten) in Informationssystemen des Bundesamtes für Sport (BASPO) durch:

20. Bundesstatistikgesetz vom 9. Oktober 1992[46]

Art. 4 Abs. 4

2 Bei Erhebungen im Rahmen dieses Gesetzes gibt der Bund den Zweck, die Rechtsgrundlage für die Bearbeitung, die Kategorien der an der Datenbank Beteiligten und die Datenempfänger bekannt.

Art. 7 Abs. 2 erster Satz

2 Er kann dabei die Übernahme von Daten aus ihren Datenbanken anordnen, sofern die Rechtsgrundlage der Datenbank die Verwendung für statistische Zwecke nicht ausdrücklich ausschliesst.

44 SR **415.0**
45 SR **415.1**
46 SR **431.01**

Art. 10 Abs. 4

4 Die Verwaltungseinheiten sowie, nach Massgabe ihrer Unterstellung nach Artikel 2 Absatz 3, die übrigen Organisationen liefern dem Bundesamt zur Erfüllung seiner Aufgaben die Ergebnisse und Grundlagen ihrer Statistiktätigkeit und, falls erforderlich, Daten aus ihren Datenbanken, Akten und Erhebungen.

Art. 12 Abs. 2

2 Das Bundesamt wirkt auf eine Koordination mit den kantonalen Statistiken hin, insbesondere um die Erhebungsprogramme aufeinander abzustimmen und Register oder andere Bearbeitungssysteme im Hinblick auf die statistische Bearbeitung zu harmonisieren.

Art. 14a Abs. 1 erster und zweiter Satz

1 Zur Erfüllung seiner statistischen Aufgaben ist das Bundesamt zur Verknüpfung von Daten und zum Profiling befugt, wenn die Daten anonymisiert werden. Die Daten sind nach Abschluss der statistischen Auswertungsarbeiten zu löschen. ...

21. Bundesgesetz vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer[47]

Art. 3 Abs. 1 Bst. d

1 In diesem Gesetz gelten als:

d. Verwaltungseinheiten von Bund, Kantonen und Gemeinden, öffentlich-rechtliche Anstalten sowie mit öffentlich-rechtlichen Aufgaben betraute private Einrichtungen, die Datenbanken und Akten über UID-Einheiten aufgrund von deren wirtschaftlicher Tätigkeit führen;

Art. 5 Abs. 1 Bst. b

1 Die UID-Stellen müssen die UID:

b. in ihren Datenbanken und Akten führen

22. Nationalbibliotheksgesetz vom 18. Dezember 1992[48]

Art. 2 Abs. 2

2 Sie verzeichnet öffentlich zugängliche Datenbanken oder andere Sammlungen, die einen Bezug zur Schweiz aufweisen.

47 SR **431.03**
48 SR **432.21**

Art. 7 Sachüberschrift und Einleitungssatz

Verzeichnung von Datenbanken

Die Nationalbibliothek verzeichnet die öffentlich zugänglichen Datenbanken oder andere Sammlungen, die:

23. Tierschutzgesetz vom 16. Dezember 2005[49]

Art. 20c Abs. 1 zweiter Satz

1 Die folgenden Personen dürfen im Rahmen ihrer gesetzlichen Aufgaben Personendaten, einschliesslich besonders schützenswerter Personendaten, bearbeiten und im Abrufverfahren auf diese Daten zugreifen:

24. Militärgesetz vom 3. Februar 1995[50]

Art. 31 Abs. 2

2 Der Bund unterhält die entsprechenden Dienste. Diese dürfen Personendaten, einschliesslich besonders schützenswerter Personendaten, bearbeiten, soweit und solange es ihre Aufgaben erfordern.

Art. 99 Abs. 2 erster Satz und 3 Bst. d

2 Er ist zur Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Personendaten, und zum Profiling befugt, gegebenenfalls ohne Wissen der betroffenen Personen, soweit und solange es seine Aufgaben erfordern. ...

3 Der Bundesrat regelt:

d. die Ausnahmen von den Vorschriften über die Registrierung von Datenbearbeitungstätigkeiten, wenn diese die Informationsbeschaffung gefährden würde

Art. 100 Abs. 2 erster Satz und 3 Bst. d

2 Er ist zur Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Personendaten, und zum Profiling befugt, soweit und solange es seine Aufgaben erfordern. ...

3 Der Bundesrat regelt:

49 SR **455**
50 SR **510.10**

d. für den Fall des Assistenz- oder des Aktivdienstes die Ausnahmen von den Vorschriften über die Registrierung der Datenbearbeitungstätigkeiten, wenn diese die Informationsbeschaffung gefährden würde;

Art. 146

Die Bearbeitung von besonders schützenswerten Personendaten sowie das Profiling in Informationssystemen und beim Einsatz von Überwachungsmitteln der Armee und der Militärverwaltung wird im Bundesgesetz vom 3. Oktober 2008 über die militärischen Informationssysteme[51] geregelt.

25. Bundesgesetz vom 3. Oktober 2008 über die militärischen Informationssysteme[52]

Art. 1 Abs. 1 Einleitungssatz

1 Dieses Gesetz regelt die Bearbeitung von besonders schützenswerten Personendaten und das Profiling in Informationssystemen und beim Einsatz von Überwachungsmitteln der Armee und der Militärverwaltung durch:

Art. 11 Abs. 2

2 Daten zum Profiling werden spätestens gelöscht:

a. bei der Entlassung aus der Militärdienstpflicht; oder

b. fünf Jahre nach Beendigung der Anstellung bei der Gruppe Verteidigung.

26. Kriegsmaterialgesetz vom 13. Dezember 1996[53]

Art. 30 Abs. 2 zweiter Satz

2 ... Soweit und solange es ihre Aufgaben erfordern, ist sie zur Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Personendaten, und zum Profiling befugt.

51 SR **510.91**
52 SR **510.91**
53 SR **514.51**

27. Waffengesetz vom 20. Juni 1997[54]

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

[2] Gewährleistet ein Drittstaat keinen angemessenen Schutz der Daten, so können ihm in besonderen Fällen Personendaten bekannt gegeben werden, wenn:

a. die betroffene Person ihre Einwilligung nach Artikel 4 Absatz 6 des Datenschutzgesetzes vom … (DSG)[55] erteilt hat;

b. wenn die Bekanntgabe erforderlich ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es nicht möglich ist, innert angemessener Frist die Einwilligung der betroffenen Person einzuholen oder wenn ...

Art. 32g zweiter Satz

Aufgehoben

28. Bevölkerungs- und Zivilschutzgesetz vom 4. Oktober 2002[56]

Art. 72 Abs. 1 und 1bis

[1] Das BABS bearbeitet zur Erfüllung seiner Aufgaben nach diesem Gesetz Personendaten von Schutzdienstpflichtigen im Zentralen Zivilschutz-Informationssystem. Es ist dabei befugt:

a. zur Bearbeitung von Daten über die Gesundheit;

b. für Entscheide über die Zuteilung der Grundfunktion oder zur Abklärung des Kaderpotenzials zum Profiling im Sinne von Artikel 3 Buchstabe f des Datenschutzgesetzes vom …[57].

[1bis] Es bearbeitet die Personendaten von Kursteilnehmenden zur Durchführung der Ausbildungen im Veranstaltungsadministratorsystem. Es ist dabei befugt:

a. zur Bearbeitung von Daten über die Gesundheit;

b. zum Profiling für die Beurteilung der Eignung für eine Kader- oder Spezialistenfunktion.

[54] SR **514.54**
[55] SR ...
[56] SR **520.10**
[57] SR ...

29. Finanzhaushaltsgesetz vom 7. Oktober 2005[58]

Art. 60c Abs. 1 Einleitungssatz und Absatz 3

1 Die SKB bearbeitet in Papierform und in einem Informationssystem die Daten, einschliesslich besonders schützenswerter Personendaten, ihrer Kundinnen und Kunden, die sie zur Erfüllung ihrer Aufgabe benötigt, namentlich um:

3 Die Angestellten der SKB können für die Erfüllung ihrer Aufgaben Personendaten, einschliesslich besonders schützenswerter Personendaten, an ihre direkten Vorgesetzten weitergeben, auch wenn diese nicht Angestellte der SKB sind.

30. Finanzkontrollgesetz vom 28. Juni 1967[59]

Art. 10 Abs. 3

3 Die Verwaltungseinheiten des Bundes räumen der Eidgenössischen Finanzkontrolle das Recht ein, im Abrufverfahren auf die für die Wahrnehmung der Finanzaufsicht erforderlichen Daten zuzugreifen. Bei Bedarf erstreckt sich das Zugriffsrecht auch auf besonders schützenswerte Personendaten. Die Eidgenössische Finanzkontrolle darf die ihr derart zur Kenntnis gebrachten Personendaten nur bis zum Abschluss des Revisionsverfahrens speichern. Die Zugriffe auf die verschiedenen Systeme und die damit verfolgten Zwecke müssen protokolliert werden.

31. Zollgesetz vom 18. März 2005[60]

Art. 110 Abs. 1

1 Die EZV darf Personendaten, einschliesslich besonders schützenswerter Personendaten, bearbeiten, sofern dies für den Vollzug der von ihr anzuwendenden Erlasse notwendig ist.

Art. 110a Abs. 3 Bst. b

3 Im Informationssystem dürfen folgende besonders schützenswerten Personendaten bearbeitet werden:

b. Angaben zur Religionszugehörigkeit, falls dies ausnahmsweise für die Strafverfolgung erforderlich ist;

58 SR **611.0**
59 SR **614.0**
60 SR **631.0**

Art. 112 Abs. 2 Einleitungssatz und Abs. 4 Bst. b

2 Es dürfen namentlich folgende Daten und Datenverbindungen, einschliesslich besonders schützenswerter Personendaten, bekannt gegeben werden:

4 Die EZV darf die folgenden Daten den nachfolgend genannten Behörden im Abrufverfahren zugänglich machen, sofern die Daten für den Vollzug der von diesen Behörden anzuwendenden Erlasse notwendig sind:

b. *aufgehoben*

Art. 113 Bekanntgabe an ausländische Behörden

Die EZV darf Behörden anderer Staaten sowie supranationaler und internationaler Organisationen (ausländische Behörden) Daten, einschliesslich besonders schützenswerter Personendaten, im Einzelfall oder im Abrufverfahren nur bekannt geben, sofern ein völkerrechtlicher Vertrag dies vorsieht.

Art. 114 Abs. 2

2 Die inländischen Behörden geben der Zollverwaltung Daten, einschliesslich besonders schützenswerter Personendaten, bekannt, sofern dies für den Vollzug der von der Zollverwaltung anzuwendenden Erlasse notwendig ist.

32. Bundesgesetz vom 12. Juni 2009 über die Mehrwertsteuer[61]

Art. 76 Abs. 1 zweiter Satz

1 ... Sie führt die dazu notwendigen Datenbanken und Akten sowie die Mittel zur Bearbeitung und Aufbewahrung.

33. Kernenergiegesetz vom 21. März 2003[62]

Art. 24 Abs. 2

2 Im Rahmen dieser Prüfung können Daten über die Gesundheit und psychische Eignung sowie sicherheitsrelevante Daten über die Lebensführung der betroffenen Person bearbeitet werden; es kann darüber eine Datenbank oder Akten führen.

61 SR **614.20**
62 SR **732.1**

34. Strassenverkehrsgesetz vom 19. Dezember 1958[63]

Art. 76b Abs. 3 zweiter Satz

3 ... Sie sind zur Erfüllung der ihnen übertragenen Aufgaben befugt, die dafür benötigten Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen.

35. Luftfahrtgesetz vom 21. Dezember 1948[64]

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

2 Die Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Daten, und das Profiling sind zulässig betreffend:

4 Die Erbringer der zivilen und der militärischen Flugsicherungsdienste können zur Untersuchung von Flugunfällen und schweren Vorfällen bei Flugverkehrsstellen Hintergrundgespräche und -geräusche aufzeichnen. Der Bundesrat regelt die Verantwortung für die Datenbeschaffung, das Auswertungsverfahren, die Datenempfänger, die Aufbewahrungsdauer und die technischen und organisatorischen Schutzmassnahmen.

5 Die Daten bearbeitenden Stellen können zum Vollzug ihrer gesetzlichen Aufgaben den mit entsprechenden Aufgaben betrauten in- und ausländischen Behörden sowie internationalen Organisationen Personendaten, einschliesslich besonders schützenswerter Daten, bekannt geben, wenn diese Behörden und Organisationen einen angemessenen Schutz der Daten gewährleisten.

36. Postgesetz vom 17. Dezember 2010[65]

Art. 26 Abs. 1

1 Die PostCom sowie weitere mit dem Vollzug dieses Gesetzes betraute Behörden übermitteln anderen Behörden des Bundes und der Kantone diejenigen Daten, die diese zur Erfüllung ihrer gesetzlichen Aufgaben benötigen. Dazu gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten.

63 SR **741.01**
64 SR **748.0**
65 SR **783.0**

Art. 28 Bearbeitung von Personendaten

Die PostCom sowie die Schlichtungsstelle dürfen zur Erfüllung ihrer gesetzlichen Aufgaben Personendaten, einschliesslich besonders schützenswerter Personendaten betreffend strafrechtliche Verfolgungen und Sanktionen, bearbeiten.

37. Fernmeldegesetz vom 30. April 1997[66]

Art. 13a Abs. 1 erster Satz

1 Die Kommission und das Bundesamt können Personendaten, einschliesslich Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, bearbeiten, sofern dies für die Erfüllung der ihnen durch die Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. ...

Art. 13b Abs. 1 zweiter Satz, 2 Einleitungssatz und 4 erster Satz

1 … Zu diesen Daten gehören auch die in Verwaltungs- oder Verwaltungsstrafverfahren beschafften besonders schützenswerten Personendaten.

2 Unter Vorbehalt anders lautender internationaler Vereinbarungen dürfen die Kommission und das Bundesamt ausländischen Aufsichtsbehörden im Fernmeldebereich Daten, einschliesslich in Verwaltungs- oder Verwaltungsstrafverfahren beschaffter besonders schützenswerter Personendaten, nur übermitteln, sofern diese Behörden:

4 Schweizerische Behörden geben der Kommission und dem Bundesamt kostenlos diejenigen Daten weiter, die für die Durchsetzung der Fernmeldegesetzgebung von Bedeutung sein können, einschliesslich besonders schützenswerter Personendaten. ...

38. Betäubungsmittelgesetz vom 3. Oktober 1951[67]

Art. 3f Abs. 1

1 Die für den Vollzug dieses Gesetzes zuständigen Behörden und Institutionen sind berechtigt, Personendaten, einschliesslich besonders schützenswerter Personendaten, zur Überprüfung der Voraussetzungen und des Verlaufs der Behandlung von betäubungsmittelabhängigen Personen zu bearbeiten.

Art. 18c zweiter Satz

Aufgehoben

66 SR **784.10**
67 SR **812.121**

39. Arbeitsvermittlungsgesetz vom 6. Oktober 1989[68]

Art. 33a Abs. 1 Einleitungssatz

1 Die mit der Durchführung sowie mit der Kontrolle oder Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, Personendaten zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:

Art. 35 Abs. 2, 3bis und 5 Bst. d

2 In diesem Informationssystem dürfen Personendaten, einschliesslich besonders schützenswerter Personendaten nach Artikel 33*a* Absatz 2, bearbeitet werden.

3bis Soweit es für den Vollzug dieses Gesetzes und des Arbeitslosenversicherungsgesetzes vom 25. Juni 1982 (AVIG)[69] notwendig ist, dürfen Personendaten, einschliesslich besonders schützenswerter Daten, zwischen den Informationssystemen der öffentlichen Arbeitsvermittlung und den Informationssystemen der Arbeitslosenversicherung (Art. 83 Abs. 1 Bst. i AVIG) ausgetauscht werden.

5 Der Bundesrat regelt:

d. den Zugriff auf die Daten, namentlich, welche Benutzer des Informationssystems befugt sind, besonders schützenswerte Personendaten zu bearbeiten;

40. Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung[70]

Art. 49a Einleitungssatz

Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:

68 SR **823.11**
69 SR **837.0**
70 SR **831.10**

41. Bundesgesetz vom 25. Juni 1982 über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge[71]

Art. 85a Einleitungssatz

Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:

42. Bundesgesetz vom 18. März 1994 über die Krankenversicherung[72]

Art. 84 Einleitungssatz

Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes oder des KVAG[73] betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz oder nach dem KVAG übertragenen Aufgaben zu erfüllen, namentlich um:

43. Bundesgesetz vom 20. März 1981 über die Unfallversicherung[74]

Art. 96 Einleitungssatz

Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:

44. Bundesgesetz vom 19. Juni 1992 über die Militärversicherung[75]

Art. 94a Einleitungssatz

Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die

71 SR **831.40**
72 SR **832.10**
73 SR **832.12**
74 SR **832.20**
75 SR **833.1**

sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:

45. Arbeitslosenversicherungsgesetz vom 25. Juni 1982[76]

Art. 96b Einleitungssatz

Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten, zu bearbeiten oder bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:

Art. 96c Abs. 2 Einleitungssatz, Abs. 2bis

2 Sie dürfen diejenigen Personendaten, einschliesslich besonders schützenswerter Daten, abrufen, die sie benötigen, um die folgenden ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen:

2bis Soweit es für den Vollzug dieses Gesetzes und des Arbeitsvermittlungsgesetzes vom 6. Oktober 1989 (AVG)[77] notwendig ist, dürfen Personendaten, einschliesslich besonders schützenswerter Daten, zwischen den Informationssystemen der Arbeitslosenversicherung (Art. 83 Abs. 1 Bst. i) und den Informationssystemen der öffentlichen Arbeitsvermittlung (Art. 35 AVG) ausgetauscht werden.

46. Tierseuchengesetz vom 1. Juli 1966[78]

Art. 54a Abs. 3

3 Im Rahmen ihrer gesetzlichen Aufgaben dürfen die Vollzugsbehörden besonders schützenswerte Personendaten und Betriebsprofile bearbeiten.

47. Jagdgesetz vom 20. Juni 1986[79]

Art. 22 Abs. 3 erster und zweiter Satz

3 Es darf diese Daten in einer Datenbank oder in Akten aufbewahren. Nach Ablauf des Entzugs der Jagdberechtigung löscht es die Daten und vernichtet die entsprechenden kantonalen Verfügungen. ...

76 SR **837.0**
77 SR **823.11**
78 SR **916.40**
79 SR **955.0**

48. Geldwäschereigesetz vom 10. Oktober 1997[80]

Art. 29 Abs. 2 zweiter Satz

2 …. Dazu gehören namentlich Finanzinformationen sowie andere, in Straf-, Verwaltungsstraf- und Verwaltungsverfahren beschaffte besonders schützenswerte Personendaten, einschliesslich solcher aus hängigen Verfahren.

Art. 34 Sachüberschrift und Abs. 1 und 2

Datenbanken und Akten im Zusammenhang mit der Meldepflicht

1 Die Finanzintermediäre führen separate Datenbanken und Akten, die alle im Zusammenhang mit der Meldung stehenden Unterlagen enthalten.

2 Sie dürfen die Daten dieser Datenbanken und Akten nur an die FINMA, die Eidgenössische Spielbankenkommission, Selbstregulierungsorganisationen, die Meldestelle und Strafverfolgungsbehörden weitergeben.

49. Finanzmarktaufsichtsgesetz vom 22. Juni 2007[81]

Art. 23 Abs. 1 erster Satz

1 Die FINMA bearbeitet im Rahmen der Aufsicht nach diesem Gesetz und den Finanzmarktgesetzen Personendaten, einschliesslich besonders schützenswerter Personendaten. …

50. Bundesgesetz vom 19. März 1976 über die internationale Entwicklungszusammenarbeit und humanitäre Hilfe[82]

Art. 13a Abs. 1 Bst. g

Aufgehoben

51. Bundesgesetz vom 24. März 2006 über die Zusammenarbeit mit den Staaten Osteuropas[83]

Art. 16 Abs. 1 Bst. g

Aufgehoben

80 SR **955.0**
81 SR **956.1**
82 SR **974.0**
83 SR **974.1**

Vorlage Änderung weiterer Erlasse

Vorentwurf

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

vom …

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
nach Einsicht in die Botschaft des Bundesrates vom …,
beschliesst:

I

Das nachstehende Gesetz wird erlassen:

das Bundesgesetz über den Datenschutz, in der Fassung gemäss Anhang.

II

Die nachstehenden Bundesgesetze werden wie folgt geändert:

1. Strafgesetzbuch[1]

Art. 349a

1. Schutz von Personendaten

a. Anwendbares Recht

Soweit dieses Gesetz nichts anderes vorsieht, richtet sich die Bearbeitung von Personendaten nach den Bestimmungen von Bund und Kantonen zum Schutz von Personendaten.

SR .....
1 SR **311.0**

Art. 349b

b. Rechtsgrundlage

Die zuständigen Bundesbehörden dürfen Personendaten nur bekannt geben, wenn dafür eine Rechtsgrundlage im Sinne von Artikel 29 Absatz 1 des Datenschutzgesetzes vom …[2] (DSG) besteht oder wenn:

a. die Bekanntgabe von Personendaten notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen;

b. die betroffene Person ihre Personendaten allgemein zugänglich gemacht und die Bekanntgabe nicht ausdrücklich untersagt hat.

Art. 349c

c. Gleichbehandlung

[1] Für die Bekanntgabe von Personendaten an die zuständigen Behörden von Staaten, die mit der Schweiz über eines der Schengen-Assoziierungsabkommen verbunden sind (Schengen-Staaten), dürfen nicht strengere Regeln gelten als für die Bekanntgabe von Personendaten an schweizerische Strafbehörden.

[2] Spezialgesetze, die strengere Regeln für die Bekanntgabe von Personendaten an die zuständigen ausländischen Behörden vorsehen, finden auf die Bekanntgabe an die zuständigen Behörden der anderen Schengen-Staaten keine Anwendung.

Art. 349d

d. Bekanntgabe von Personendaten an einen Drittstaat oder an ein internationales Organ

[1] Personendaten dürfen der zuständigen Behörde eines Staates, der nicht über eines der Schengen-Assoziierungsabkommen mit der Schweiz verbunden ist (Drittstaat), oder einem internationalen Organ nicht bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein angemessener Schutz der Daten fehlt.

[2] Ein angemessener Schutz wird gewährleistet durch:

a. die Gesetzgebung des Drittstaats, sofern die Europäische Kommission dies in einem Beschluss nach Artikel 36 der Richtlinie (EU) 2016/680[3] festgehalten hat;

b. einen völkerrechtlichen Vertrag;

2 SR….

3 Richtlinie (EU) 2016/680 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; ABl. L 119 vom 4.5.2016, S. 89.

c. spezifische Garantien.

[3] Die zuständige Bundesbehörde informiert den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) über die Kategorien von Bekanntgaben von Personendaten, die nach Absatz 2 Buchstabe c erfolgen. Jede Bekanntgabe wird dokumentiert.

[4] In Abweichung von Absatz 1 können Personendaten der zuständigen Behörde eines Drittstaates oder eines internationalen Organs bekannt gegeben werden, wenn die Bekanntgabe im Einzelfall notwendig ist:

a. zum Schutz des Lebens oder der körperlichen Unversehrtheit der betroffenen Person oder eines Dritten;

b. zur Abwehr einer unmittelbar drohenden ernsthaften Gefahr für die öffentliche Sicherheit eines Schengen- oder Drittstaats;

c. zur Verhütung, Feststellung oder Verfolgung einer Straftat, sofern keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen;

d. zur Ausübung oder Durchsetzung von Rechtsansprüchen gegenüber einer für die Verhütung, Feststellung oder Verfolgung einer Straftat zuständigen Behörde, sofern keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen.

[5] Die zuständige Bundesbehörde informiert den Beauftragten über die Bekanntgabe von Daten nach Absatz 4.

[6] Darüber hinaus gelten die Bestimmungen über die Zusage für die zwischenstaatliche Zusammenarbeit in Strafsachen gegenüber einem Drittstaat oder einem internationalen Organ.

Art. 349e

e. Bekanntgabe von Personendaten aus einem Schengen-Staat an einen Drittstaat oder an ein internationales Organ

[1] Personendaten, die von einem Schengen-Staat übermittelt oder zur Verfügung gestellt wurden, können der zuständigen Behörde eines Drittstaates oder einem internationalen Organ bekannt gegeben werden, wenn:

a. die Bekanntgabe zur Verhütung, Feststellung oder Verfolgung einer Straftat erforderlich ist;

b. der Schengen-Staat, der die Personendaten übermittelt oder zur Verfügung gestellt hat, der Bekanntgabe vorgängig zugestimmt hat;

c. die Voraussetzungen nach Artikel 349*d* erfüllt sind.

[2] Abweichend von Absatz 1 Buchstabe b dürfen Personendaten im Einzelfall bekannt gegeben werden, wenn:

a. die vorgängige Zustimmung des Schengen-Staates nicht rechtzeitig eingeholt werden kann; und

b. 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.

[3] Die zuständige Behörde informiert den Schengen-Staat unverzüglich über die Bekanntgabe von Personendaten nach Absatz 2.

Art. 349f

f. Bekanntgabe von Personendaten an in einem Drittstaat niedergelassene Dritte

[1] Ist es namentlich in Notfällen nicht möglich, der zuständigen Behörde eines Drittstaates Personendaten auf dem üblichen Weg der polizeilichen Zusammenarbeit bekannt zu geben, so kann die zuständige Behörde sie ausnahmsweise einem in diesem Staat niedergelassenen Dritten bekannt geben, sofern die folgenden Voraussetzungen erfüllt sind:

a. Die Spezialgesetzgebung oder ein völkerrechtlicher Vertrag sieht die Bekanntgabe vor.

b. Die Bekanntgabe ist für die Erfüllung einer gesetzlichen Aufgabe der Behörde, die die Daten bekannt gibt, unentbehrlich.

c. Der Bekanntgabe stehen keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegen.

[2] Die zuständige Behörde weist den Dritten, dem sie die Personendaten bekannt gibt, darauf hin, dass er sie nicht für andere Zwecke verwenden darf, als für die von der Behörde festgelegten.

[3] Sie benachrichtigt die zuständige Behörde des Drittstaats unverzüglich über jede Bekanntgabe von Personendaten, sofern diese Information als zweckmässig erachtet wird.

[4] Die zuständige Bundesbehörde informiert den Beauftragten unverzüglich über jede Bekanntgabe von Personendaten, die nach Absatz 1 erfolgt, informiert.

[5] Jede Bekanntgabe von Personendaten wird dokumentiert. Der Bundesrat regelt die Einzelheiten.

Art. 349g

g. Richtigkeit der Personendaten

[1] Die Behörde berichtigt unverzüglich unrichtige Personendaten.

[2] Sie benachrichtigt die Behörde, die ihr diese Daten übermittelt oder zur Verfügung gestellt oder der sie diese bekannt gegeben hat, unverzüglich über die Berichtigung.

[3] Sie informiert den Datenempfänger über die Aktualität und die Zuverlässigkeit der von ihr bekannt gegebenen Personendaten.

[4] Sie gibt dem Datenempfänger ausserdem alle weiteren Informationen bekannt, anhand welcher so weit wie möglich unterschieden werden können:

a. die verschiedenen Kategorien betroffener Personen;

b. Personendaten, die auf Fakten beruhen, und solchen, die auf persönlichen Einschätzungen beruhen.

[5] Die Pflicht zur Information des Datenempfängers entfällt, wenn die Informationen nach den Absätzen 3 und 4 aus den Personendaten selbst oder aus den Umständen ersichtlich sind.

Art. 349h

h. Prüfung der Rechtmässigkeit der Datenbearbeitung

[1] Die betroffene Person kann vom Beauftragten verlangen, dass er prüft, ob allfällige Daten über sie rechtmässig bearbeitet werden, wenn:

a. ihr Recht auf Information über den Austausch von Daten über sie eingeschränkt oder aufgeschoben wird (Art. 13 und 14 DSG[4]);

b. ihr Auskunftsrecht verweigert, eingeschränkt oder aufgeschoben wird (Art. 20 und 21 DSG);

c. ihr Recht, die Einschränkung des Austauschs von Daten über sie zu verlangen, teilweise oder ganz verweigert wird (Art. 34 Abs. 2 DSG);

d. ihr Recht, die Berichtigung, die Vernichtung oder Löschung von Daten über sie zu verlangen, teilweise oder ganz verweigert wird (Art. 34 Abs. 3 DSG).

[2] Der Prüfung unterzogen werden kann ausschliesslich eine Bundesbehörde, die der Aufsicht des Beauftragten untersteht.

[3] Der Beauftragte führt die Prüfung durch; er teilt der betroffenen Person mit, dass entweder keine Daten über sie unrechtmässig bearbeitet werden oder dass er einen Fehler bei der Bearbeitung der Personendaten festgestellt und eine Untersuchung nach Artikel 41 DSG eröffnet hat.

[4] Stellt der Beauftragte Fehler bei der Datenbearbeitung fest, so ordnet er an, dass die zuständige Bundesbehörde die Fehler behebt.

[5] Die Mitteilung nach Absatz 3 lautet stets gleich und wird nicht begründet. Sie kann nicht angefochten werden.

Art. 349i

i. Untersuchung

[1] Macht die betroffene Person glaubhaft, dass ein Austausch von Personendaten über sie gegen die Vorschriften zum Schutz von Personendaten verstossen könnte, kann sie vom Beauftragten eine Untersuchung nach Artikel 41 DSG[5] verlangen.

4 SR…
5 SR …

[2] Eine Untersuchung kann ausschliesslich gegen eine Bundesbehörde, die der Aufsicht des Beauftragten untersteht, eröffnet werden.

[3] Partei sind die betroffene Person und die Bundesbehörde, gegen die eine Untersuchung eröffnet wurde.

[4] Ferner gelten die Artikel 42 und 43 DSG.

Art. 355a Abs. 1 und 4

[1] Das fedpol und der Nachrichtendienst des Bundes (NDB) können dem Europäischen Polizeiamt (Europol) Personendaten, einschliesslich besonders schützenswerter Personendaten, weitergeben.

[4] Der Austausch von Personendaten mit Europol wird dem Austausch mit einer zuständigen Behörde eines Schengen-Staates gleichgesetzt (Art. 349*c*).

Art. 355f

Aufgehoben

Art. 355g

Aufgehoben

Art. 365 Abs. 1 erster Satz

[1] Das Bundesamt für Justiz führt unter Mitwirkung anderer Bundesbehörden und der Kantone (Art. 367 Abs. 1) ein automatisiertes Strafregister über Verurteilungen und Gesuche um Strafregisterauszug im Rahmen von hängigen Strafverfahren, welches besonders schützenswerte Personendaten enthält. …

2. Strafprozessordnung[6]

Art. 95a Bearbeitung von Personendaten

Bei der Bearbeitung von Personendaten sehen die Strafbehörden angemessene Massnahmen vor, damit so weit wie möglich unterschieden werden können:

a. die verschiedenen Kategorien betroffener Personen;

b. die auf Fakten und die auf persönlichen Einschätzungen beruhenden Personendaten.

6 SR **312.0**

Art. 98 Abs. 2

[2] Sie benachrichtigen die Behörde, die ihnen diese Daten übermittelt oder zur Verfügung gestellt oder der sie diese bekannt gegeben hat, unverzüglich über die Berichtigung.

3. Rechtshilfegesetz vom 20. März 1981[7]

Gliederungstitel nach Artikel 11a

1b. Kapitel: Schutz von Personendaten

Nach dem Gliederungstitel des 1b. Kapitels die Artikel 11b–11i einfügen

Art. 11b Informationspflicht bei Datenbearbeitung

[1] Wird auf Ersuchen eines anderen Staates ein Rechtshilfeverfahren eröffnet, so informiert die zuständige Behörde die Person, gegen die sich das Ersuchen um Zusammenarbeit in Strafsachen (Art. 1 Abs. 1) richtet, über jede Bearbeitung von sie betreffenden Personendaten, soweit keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen.

[2] Ein überwiegendes öffentliches Interesse besteht namentlich, wenn durch die Information der betroffenen Person ein Ermittlungs-, Untersuchungs- oder Gerichtsverfahren oder ein Verfahren der zwischenstaatlichen Zusammenarbeit in Strafsachen gefährdet wird.

Art. 11c Auskunftsrechte bei hängigem Verfahren

Solange ein Rechtshilfeverfahren hängig ist, kann die Person, gegen die sich ein Ersuchen um Zusammenarbeit in Strafsachen richtet, nach Massgabe des ihr zustehenden Akteneinsichtsrechts die sie betreffenden Personendaten einsehen.

Art. 11d Einschränkung des Auskunftsrechts bei Ersuchen um Festnahme zum Zwecke der Auslieferung

[1] Das jeder Person zustehende Recht, Auskunft darüber zu verlangen, ob die Schweiz von einem ausländischen Staat ein Ersuchen um Festnahme zum Zwecke ihrer Auslieferung erhalten hat, wird beim Bundesamt geltend gemacht. Wird das entsprechende Gesuch um Auskunft an eine andere Behörde gerichtet, so leitet es diese unverzüglich an das Bundesamt weiter.

[2] Verlangt eine Person beim Bundesamt Auskunft darüber, ob es ein Ersuchen eines ausländischen Staates um Festnahme zum Zwecke ihrer Auslieferung erhalten hat, so teilt dieses ihr mit, dass keine Daten über sie unrechtmässig bearbeitet werden

7 SR **351.1**

und dass sie vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (der Beauftragte) verlangen kann, zu prüfen, ob allfällige Daten über sie rechtmässig bearbeitet werden.

3 Der Beauftragte führt die Prüfung durch; er teilt der betroffenen Person mit, dass entweder keine Daten über sie unrechtmässig bearbeitet werden oder dass er einen Fehler bei der Bearbeitung der Personendaten festgestellt und eine Untersuchung nach Artikel 41 des Datenschutzgesetzes vom …[8] (DSG) eröffnet hat.

4 Im Fall von Fehlern bei der Datenbearbeitung ordnet der Beauftragte an, dass das Bundesamt diese behebt.

5 Die Mitteilungen nach den Absätzen 2 und 3 lauten stets gleich und werden nicht begründet.

6 Die Mitteilung nach Absatz 3 kann nicht mit einem Rechtsmittel angefochten werden.

7 Das Bundesamt ist in Abweichung von Absatz 2 ermächtigt, der betroffenen Person die verlangten Auskünfte zu erteilen, wenn der ersuchende Staat vorgängig zustimmt.

Art. 11e Gleichbehandlung

1 Für die Bekanntgabe von Personendaten an die zuständigen Behörden von Staaten, die mit der Schweiz über eines der Schengen-Assoziierungsabkommen verbunden sind (Schengen-Staaten), dürfen nicht strengere Regeln gelten als für die Bekanntgabe von Personendaten an schweizerische Strafbehörden.

2 Spezialgesetze, die strengere Regeln für die Bekanntgabe von Personendaten an die zuständigen ausländischen Behörden vorsehen, finden auf die Bekanntgabe an die zuständigen Behörden der anderen Schengen-Staaten keine Anwendung.

Art. 11f Bekanntgabe von Personendaten an einen Drittstaat oder an ein internationales Organ

1 Personendaten dürfen der zuständigen Behörde eines Staates, der nicht über eines der Schengen-Assoziierungsabkommen mit der Schweiz verbunden ist (Drittstaat), oder einem internationalen Organ nicht bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein angemessener Schutz der Daten fehlt.

2 Ein angemessener Schutz wird gewährleistet durch:

a. die Gesetzgebung des Drittstaats, sofern die Europäische Kommission dies in einem Beschluss nach Artikel 36 der Richtlinie (EU) 2016/680[9] festgehalten hat;

8 SR…

9 Richtlinie (EU) 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der

b. einen völkerrechtlichen Vertrag;

c. spezifische Garantien.

3 In Abweichung von Absatz 1 können Personendaten einem Drittstaat oder einem internationalen Organ bekannt gegeben werden, wenn die Bekanntgabe im Einzelfall notwendig ist:

a. zum Schutz des Lebens oder der körperlichen Unversehrtheit der betroffenen Person oder eines Dritten;

b. zur Abwehr einer unmittelbar drohenden ernsthaften Gefahr für die öffentliche Sicherheit eines Schengen-Staates oder eines Drittstaates;

c. zur Verhütung, Feststellung oder Verfolgung einer Straftat oder zur Vollstreckung eines Strafentscheides, sofern der Bekanntgabe keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen;

d. zur Ausübung oder Durchsetzung von Rechtsansprüchen gegenüber einer für die Verhütung, Feststellung oder Verfolgung einer Straftat oder die Vollstreckung eines Strafentscheids zuständigen Behörde, sofern der Bekanntgabe keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen.

4 Darüber hinaus gelten die Bestimmungen über die Zusage für die zwischenstaatliche Zusammenarbeit in Strafsachen gegenüber einem Drittstaat oder einem internationalen Organ.

Art. 11g Bekanntgabe von Personendaten aus einem Schengen-Staat an einen Drittstaat oder ein internationales Organ

1 Personendaten, die von einem Schengen-Staat übermittelt oder zur Verfügung gestellt wurden, können der zuständigen Behörde eines Drittstaates oder einem internationalen Organ bekannt gegeben werden, wenn:

a. die Bekanntgabe zur Verhütung, Feststellung oder Verfolgung einer Straftat oder zur Vollstreckung eines Strafentscheids erforderlich ist;

b. der Schengen-Staat, der die Personendaten übermittelt oder zur Verfügung gestellt hat, der Bekanntgabe vorgängig zugestimmt hat;

c. die Voraussetzungen nach Artikel 11*f* erfüllt sind.

2 Abweichend von Absatz 1 Buchstabe b dürfen Personendaten im Einzelfall bekannt gegeben werden, wenn:

a. die vorgängige Zustimmung des Schengen-Staates nicht rechtzeitig eingeholt werden kann; und

b. die Bekanntgabe zur Abwehr einer unmittelbar drohenden ernsthaften Gefahr für die öffentliche Sicherheit eines Schengen-Staates oder eines Dritt-

Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr; ABl. L 119 vom 4.5.2016, S. 89.

staates oder zur Wahrung der wesentlichen Interessen eines Schengen-Staates unerlässlich ist.

3 Der Schengen-Staat wird unverzüglich über die auf Absatz 2 gestützte Bekanntgabe von Personendaten informiert.

Art. 11h Richtigkeit der Personendaten

1 Die Behörde berichtigt unverzüglich unrichtige Personendaten.

2 Sie benachrichtigt die Behörde, die ihr diese Daten übermittelt oder zur Verfügung gestellt oder der sie diese bekannt gegeben hat, unverzüglich über die Berichtigung.

3 Sie meldet dem Datenempfänger die Aktualität und die Zuverlässigkeit der von ihr bekannt gegebenen Personendaten.

4 Die Behörde gibt dem Datenempfänger ausserdem alle weiteren Informationen bekannt, anhand welcher so weit wie möglich unterschieden werden können:

a. die verschiedenen Kategorien betroffener Personen;

b. die auf Fakten und die auf persönlichen Einschätzungen beruhenden Personendaten.

5 Die Pflicht zur Information des Datenempfängers entfällt, wenn die Informationen nach den Absätzen 3 und 4 aus den Personendaten selbst oder aus den Umständen ersichtlich sind.

Art. 11i Ansprüche und Verfahren

1 Die datenschutzrechtlichen Ansprüche werden im hängigen Rechtshilfeverfahren beurteilt und unterliegen denselben Rechtsmitteln.

2 Die Artikel 20, 21, 30 und 34 DSG[10] gelten nicht, solange der Endentscheid betreffend das Rechtshilfeverfahren nicht rechtskräftig ist.

3 Datenbearbeitungen, die eine Behörde im Rahmen des Rechtshilfeverfahrens durchführt, sind von der Aufsicht durch den Beauftragten ausgenommen, bis der Endentscheid rechtskräftig ist.

10 SR …

4. Bundesgesetz vom 3. Oktober 1975[11] zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen

Art. 9a Schutz von Personendaten

Soweit der Vertrag nichts anderes bestimmt, richtet sich die Bearbeitung von Personendaten nach den Artikeln 11*b*–11*c* und 11*f*–11*i* des Rechtshilfegesetzes vom 20. März 1981[12].

5. Bundesgesetz vom 7. Oktober 1994[13] über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten

Art. 13 Abs. 2

Die Bekanntgabe von Personendaten im Rahmen der Polizeizusammenarbeit mit ausländischen Strafverfolgungsbehörden wird in Art. 349*a* bis 349*i* des Strafgesetzbuches[14] geregelt.

6. Bundesgesetz vom 13. Juni 2008[15] über die polizeilichen Informationssysteme des Bundes

Art. 7 Abs. 2

2 Fedpol erteilt die Auskünfte nach Rücksprache mit der Behörde, welche die Daten eingetragen hat oder hat eintragen lassen; die Artikel 8 und 8a bleiben vorbehalten.

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

2 Fedpol teilt der gesuchstellenden Personen den Aufschub der Auskunft mit und weist sie darauf hin, dass sie das Recht hat, vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragten) zu verlangen, dass er prüfe, ob allfällige Daten über sie rechtmässig bearbeitet werden und ob überwiegende Geheimhaltungsinteressen den Aufschub rechtfertigen.

3 Der Beauftragte führt die Prüfung durch; er teilt der betroffenen Person mit, dass entweder keine Daten über sie unrechtmässig bearbeitet werden oder dass er einen

11 SR **351.93**
12 SR **351.1**
13 SR **360**
14 SR **311.0**
15 SR **361**

Fehler bei der Bearbeitung der Personendaten festgestellt und eine Untersuchung nach Artikel 41 des Datenschutzgesetzes vom …[16] (DSG) eröffnet hat.

[4] *Aufgehoben*

[5] Im Fall von Fehlern bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft verpflichtet der Beauftragte fedpol mit einer Verfügung zu deren Behebung.

[6] Die Mitteilung nach Absatz 3 lautet stets gleich und wird nicht begründet. Sie kann nicht mit einem Rechtsmittel angefochten werden.

[8] Legt eine Person glaubhaft dar, dass ihr bei einem Aufschub der Auskunft ein erheblicher, nicht wieder gut zu machender Schaden erwächst, so kann der Beauftragte anordnen, dass fedpol ausnahmsweise sofort Auskunft erteilt, wenn und soweit damit keine Gefährdung der inneren oder der äusseren Sicherheit verbunden ist.

Vor dem Titel des zweiten Abschnitts einfügen

Art. 8a Einschränkung des Auskunftsrechts bei Ausschreibungen zur Festnahme zum Zweck der Auslieferung

[1] Verlangt eine Person bei fedpol Auskunft darüber, ob sie in einem polizeilichen Informationssystem zur Festnahme zum Zweck der Auslieferung ausgeschrieben ist, so teilt fedpol der betroffenen Person mit, dass keine Daten über sie unrechtmässig bearbeitet werden und dass sie vom Beauftragten verlangen kann, zu prüfen, ob allfällige Daten über sie rechtmässig bearbeitet werden.

[2] Der Beauftragte führt die Prüfung durch; er teilt der betroffenen Person mit, dass entweder keine Daten über sie unrechtmässig bearbeitet werden oder dass er einen Fehler bei der Bearbeitung der Personendaten festgestellt und eine Untersuchung nach Artikel 41 DSG[17] eröffnet hat.

[3] Im Fall von Fehlern bei der Datenbearbeitung ordnet der Beauftragte an, dass fedpol diese behebt.

[4] Die Mitteilungen nach den Absätzen 1 und 2 lauten stets gleich und werden nicht begründet.

[5] Die Mitteilung nach Absatz 2 kann nicht mit einem Rechtsmittel angefochten werden.

16 SR **...**
17 SR …

7. Schengen-Informationsaustausch-Gesetz vom 12. Juni 2009[18]

Art. 2 Abs. 3

3 Die Bearbeitung von Personendaten wird in Art. 349*a* bis 349*i* des Strafgesetzbuches[19] geregelt..

Art. 6a

Aufgehoben

Art. 6b

Aufgehoben

Art. 6c

Aufgehoben

III

1 Dieses Gesetz untersteht dem fakultativen Referendum.

2 Der Bundesrat bestimmt das Inkrafttreten.

18 SR **362.2**
19 SR **311**

Vorlage Bundesbeschluss Genehmigung Notenaustausch CH-EU

Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der EU betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung

(Weiterentwicklung des Schengen-Besitzstands)

vom …

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf die Artikel 54 Absatz 1 und 166 Absatz 2 der Bundesverfassung[1],
nach Einsicht in die Botschaft des Bundesrates vom…[2],

beschliesst:

Art. 1

[1] Der Notenaustausch vom 1. September 2016[3] zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung wird genehmigt.

[2] Der Bundesrat wird ermächtigt, die Europäische Union nach Artikel 7 Absatz 2 Buchstabe b des Abkommens vom 26. Oktober 2004[4] 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 über die Erfüllung der verfassungsrechtlichen Voraussetzungen in Bezug auf den Notenaustausch nach Absatz 1 zu informieren.

1 SR **101**
2 BBl…
3 SR …, AS …
4 SR **0.362.31**

Art. 2

Dieser Beschluss untersteht dem fakultativen Referendum (Art. 141 Abs. 1 Bst. d Ziff. 3 BV).

Notenaustausch

Notenaustausch vom 1. September 2016

zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung

(Weiterentwicklung des Schengen-Besitzstands)

In Kraft getreten am …

Übersetzung[1]

Mission der Schweiz
bei der Europäischen Union

Brüssel, den 1. September 2016

Generalsekretariat des Rates
der Europäischen Union
Generaldirektion D
Justiz und Inneres
Brüssel

Die Mission der Schweiz bei der Europäischen Union entbietet dem Generalsekretariat des Rates der Europäischen Union ihre Empfehlung und beehrt sich, mit Bezug auf die Notifikation des Rates vom 1. August 2016, die erstellt worden ist gestützt auf Artikel 7 Absatz 2 Buchstabe a erster Satz des Abkommens 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: Assoziierungsabkommen)[2], das am 26. Oktober 2004 in Luxemburg unterzeichnet worden ist, den Empfang dieser Notifikation zu bestätigen. Letztere hat folgenden Inhalt:

« In Übereinstimmung mit Artikel 7 Absatz 2 Buchstabe a erster Satz in Verbindung mit Artikel 14 Absatz 1 des Abkommens, welches die Schweiz an den Schengen-Besitzstand assoziiert, wird der Schweiz hiermit die Verabschiedung des folgenden Rechtsakts notifiziert:

SR **…**

1 Übersetzung des englischen Originaltextes.
2 AS **2008** 481

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/JI des Rates

Ratsdokument: 5418/1/16 REV 1 DATAPROTECT 1 JAI 37 DAPIX 8 FREMP 3 COMIX 36 CODEC 51 PARLNAT 82

Datum der Annahme : 8. April 2016»[3]

Gemäss Artikel 7 Absatz 2 Buchstabe a und b des Assoziierungsabkommens und unter Vorbehalt der Erfüllung der verfassungsrechtlichen Voraussetzungen der Schweiz informiert die Mission der Schweiz bei der Europäischen Union das Generalsekretariat des Rates der Europäischen Union, dass die Schweiz den Inhalt des Rechtsakts, welcher der Notifikation des Rates beigelegt und Teil dieser Antwortnote ist, akzeptiert und in ihre innerstaatliche Rechtsordnung umsetzen wird.

Gemäss Artikel 7 Absatz 2 Buchstabe b des Assoziierungsabkommens wird die Schweiz das Generalsekretariat des Rates der Europäischen Union unverzüglich über die Erfüllung ihrer verfassungsrechtlichen Voraussetzungen informieren.

Gemäss Artikel 7 Absatz 3 des Assoziierungsabkommens begründen die Notifikation des Rates vom 1. August 2016 und diese Antwortnote Rechte und Pflichten zwischen der Schweiz und der Europäischen Union und bilden somit ein Abkommen zwischen der Schweiz und der Europäischen Union.

Dieses Abkommen wird zum Zeitpunkt der Notifikation durch die Schweiz über die Erfüllung ihrer verfassungsrechtlichen Voraussetzungen in Kraft treten. Gekündigt werden kann das Abkommen unter den Bedingungen, die in den Artikeln 7 und 17 des Assoziierungsabkommens aufgeführt sind.

Mit Inkrafttreten dieses Abkommens wird der Notenaustausch vom 14. Januar 2009 2008[4] zwischen der Schweiz und der Europäischen Union betreffend die Übernahme des Rahmenbeschlusses 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, beendigt.

Eine Kopie dieser Note wird der Europäischen Kommission, Generalsekretariat, SG.A.3, Brüssel, übermittelt.

3 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/JI des Rates, Fassung gemäss ABl. L 119 vom 4.5.2016, S. 89.

4 AS **2010** 3419

Die Mission der Schweiz bei der Europäischen Union benützt die Gelegenheit, um das Generalsekretariat des Rates der Europäischen Union ihrer ausgezeichneten Hochachtung zu versichern.

Erläuternder Bericht

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte 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

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 des 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 technoloischen 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 Legislaturprogamm 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 betroffeen 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 miteinbeziehn 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 Verwaltungssanktionen 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 1992[1] 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 10*a* ist die Bearbeitung von Daten durch Dritte geregelt. Gemäss Artikel 11*a* 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 18*a* sind Bundesorgane verpflichtet, die betroffene Person über die Beschaffung von Personendaten zu informieren; vorbehalten sind einige Ausnahmen (Art. 18*b*). Grundsätzlich dürfen Bundesorgane Personendaten nur 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 26*a* regelt das DSG die Wahl, die Stellung, die Wiederwahl und die Beendigung der Amtsdauer der oder des Beauftragten. In den Artikeln 27–33 sind die Aufgaben und Zuständigkeiten des Beauftragten festgelegt. Dieser überwacht die Einhaltung des Gesetzes durch die Bundesorgane und berät private Personen in Fragen des Datenschutzes. Er kann Abklärungen durchführen und Empfehlungen abgeben. Hält sich eine private Person nicht an eine Empfehlung, kann der Beauftragte die Angelegenheit dem Bundesverwaltungsgericht unterbreiten, und ist berechtigt, gegen diesen Entscheid Beschwerde zu führen (Art. 29 Abs. 4). Befolgt hingegen ein Bundesorgan eine Empfehlung nicht, kann er die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorlegen (Art. 27 Abs. 5). Der Beauftragte kann gegen den Entscheid der vorgesetzten Behörde und gegen den Entscheid der Beschwerdebehörde Beschwerde führen (Art. 27 Abs. 6).

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

Vorbehaltlich von Artikel 37 DSG und Bestimmungen in Spezialgesetzen des Bundes 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 DSG gelten in vielen Bereichen Spezialgesetze, die ebenfalls datenschutzrechtliche Bestimmungen enthalten (bereichsspezifische Datenschutznormen).

1.1.2 Vorarbeiten und Konzept

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

Zur Umsetzung des Auftrags des Bundesrates vom 9. Dezember 2011 bildete das Bundesamt für Justiz (BJ) eine Arbeitsgruppe, um die Arbeiten zur Revision des DSG zu begleiten. Diese Arbeitsgruppe setzte sich aus Vertreterinnen und Vertretern der Bundesverwaltung[4], der Kantone[5], der Wirtschaft[6], der Konsumentenschutzorganisationen[7] sowie aus Expertinnen und Experten zusammen. Die Begleitgruppe präsentierte ihre Überlegungen im Bericht vom 29. Oktober 2014 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 DSG (im Folgenden «VE-DSG») und im Anhang die dadurch notwendigen Anpassungen weiterer Bundesgesetze beinhaltet. Ziffer II der Matelerlasses 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, BBl **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 Aktionsplan[9] 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 2014[12]*:* 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] BBl **2012** 335, hier 350

[16] BBl **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 Menschenrechtskonvention[17], Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte[18]), 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 1995[20] 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/JAI[21] 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 Programms[22] 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) 2016/679[24] 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) 2016/680[25] 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 1981[28] 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 2001[29] 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 substanziellen 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%20modernisée%20juillet%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 Resolution[31] verabschiedet. Sie ruft alle 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 identifizieren[38].

---

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-Richtlinien[39] 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 verstärkt[41]. Die revidierten Datenschutz-Richtlinien sehen neu explizit vor, dass Datenhauptverantwortliche stets für die unter ihrer Kontrolle stehenden Personendaten verantwortlich sind, dies ungeachtet des Standorts der Daten[42]. 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/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.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 angemessen Schutzniveau gehört. An diesem Beschluss hat insbesondere die Schweizer Wirtschaft ein erhebliches Interesse.

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

1.4 Darstellung des 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 gewährleitet 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 Vorkehren sollen für eine datenschutzfreundliche Ausgestaltung von Systemen sorgen. Diese Pflichten werden indessen durch gewisse Erleichterungen ausgeglichen. So soll die im privaten Sektor geltende Verpflichtung, dem Beauftragten die Datensammlungen zu melden, aufgehoben werden, was den Aufwand für die Verantwortlichen reduziert.

Die siebte Leitlinie ist die Stärkung der Kontrolle. So werden einerseits Stellung und Unabhängigkeit des Beauftragten gestärkt. Die Befugnisse des Beauftragten werden künftig mit den Befugnissen der entsprechenden ausländischen Kontrollbehörden vergleichbar sein. Anders als 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 Datenschutzanforderungen 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 13*a* 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 Entscheidfindung 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 2002[44] über die Bundesversammlung (ParlG) festgelegt.

Das BJ und das Staatssekretariat für Wirtschaft (SECO) haben das Unternehmen PwC mit der Durchführung einer RFA[45] 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, solle 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-Assozierungsabkommens).

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

Das Europäische Parlament und der Rat der Europäischen Union haben die Richtlinie (EU) 2016/680 am 27. April 2016 verabschiedet. Der Rechtsakt wurde der Schweiz indessen erst am 1. August 2016 notifiziert. Dadurch war es der Schweiz nicht möglich, dem Generalsekretariat des Rates ihre Antwortnote innert der durch das Assoziierungsabkommen vorgeschriebenen Frist zu übermitteln. Die Schweiz 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 1937[47] (StGB), die Strafprozessordnung vom 5. Oktober 2007[48] (StPO), das Bundesgesetz vom 20. März 1981[49] über internationale Rechtshilfe in Strafsachen (IRSG), das Bundesgesetz vom 3. Oktober 1975[50] zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen, das Schengen-Informationsaustausch-Gesetz vom 12. Juni 2009[51] (SIaG) und das Bundesgesetz vom 7. Oktober 1994[52] 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. 8bis Abs. 2 und 3).

Die Vertragsparteien müssen der betroffenen Person das Recht einräumen, nicht einer Entscheidung unterworfen zu sein, die ausschliesslich auf der Grundlage einer

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 2011[54] 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] BBl **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 Kommission[55] 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 1558/2001[58] 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 fünftägigen 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 ABl. 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 Commissionner» (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 Zulässigkeitserklärungen bei Verstössen gegen den «Privacy Act» abgeben.

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

Gegenwärtig muss jede «Agency»[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 Singapurer Recht zahlreiche Ausnahmen vor, bei denen die Einwilligung nicht notwendig ist oder als gegeben vorausgesetzt werden kann (Art. 13–15 PDPA). Die Datenbearbeitung muss zu einem Zweck durchgeführt werden, welcher der betroffenen Person bekannt ist oder der jeder Person unter den gleichen Umständen als sinnvoll erscheint (Art. 18 PDPA). Die Verantwortlichen müssen für die Richtigkeit der Daten sorgen (Art. 23 PDPA) und sie sind verpflichtet, geeignete Vorsichtsmassnahmen zu ergreifen, um das Abhandenkommen, das Kopieren oder den unerlaubten Zugriff auf in ihrem Besitz befindliche Personendaten zu verhindern (Art. 24 PDPA). Die Verantwortlichen müssen Personendaten vernichten oder anonymisieren, sobald deren Aufbewahrung nicht mehr dem Zweck ihrer Beschaffung entspricht und nicht durch einen rechtlichen oder wirtschaftlichen Grund gerechtfertigt ist (Art. 25 PDPA). Die grenzüberschreitende Bekanntgabe von Personendaten ist nur zulässig, wenn das Empfängerland ein Schutzniveau gewährleistet, das mit jenem von Singapur vergleichbar ist (Art. 26 PDPA).

Anscheinend wurden keine spezifischen Massnahmen zur Förderung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen vorgesehen. Die PDPC könnte 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 Gesetzesebene das in Artikel 13 Absatz 2 BV festgehaltene Recht auf informationelle Selbstbestimmung im Zusammenhang mit Personendaten, d. h. das

Recht der betroffenen Person, grundsätzlich selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen.[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. 2Geltungsbereich

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 1992[67] 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 2004[70] 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 BBl **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 1988[71] angeführt hat. Schliesslich übernimmt Buchstabe d dieser Bestimmung die Ausnahme betreffend das Internationale Komittee 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 2007[72], 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 einfliessenden 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 eidgenössichen 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 2011[75] [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 1986[76]). 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 BBl **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 2007[78]).

- Für die Führung der Betreibungs- und Konkursregister sind die Kantone zuständig (Art. 8 Abs. 1 des Bundesgesetzes vom 11. April 1889[79] 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 eidgenässischen 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/2015/2015-12-110/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 2005[82] 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 bestimmbaren 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 2004[83] 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 Mobiliät 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 DSG) oder die Informationspflicht (Art. 14 DSG) –, während gerade in diesem Zusammenhang mehr Transparenz erforderlich ist. Im Übrigen weist der Bundesrat darauf hin, dass ein Teil der Lehre den Begriff Datensammlung sehr weit auslegt. Dabei besteht das entscheidende Kriterium darin, dass die Zuweisung von Daten zu einer Person keinen unverhältnismässigen Aufwand verursachen darf.[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 DSG 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 zu vereinbaren 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 Privatunternehmen[86].

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 DSG enthalten ist. Auf diese Weise werden die wichtigsten Datenschutzgrundsätze in einer einzigen Bestimmung zusammengefasst, wie dies auch in Artikel 5 E-SEV 108, in Artikel 4 der Richtlinie (EU) 2016/680 und in Artikel 5 der Verordnung (EU) 2016/679) der Fall ist. 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 NBibG[88]). 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 Einwilligung[90] 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 BBl **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 Schutz[91] 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 BBl **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 DSG), eine Verschärfung dar. Sie entspricht der Anforderung von Artikel 12bis 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 Beauftrage 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 DSG. 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 bekanntgegebener 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 beistpielsweise 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 git. 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 DSG) 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 Gesellschaft[93], 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 Vorkehren 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 1998[96] 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 18*a* DSG werden damit in einer Norm zusammengeführt. Dadurch werden Doppelspurigkeiten vermieden und es gilt eine einheitliche Regelung für die Datenbearbeitung durch Bundesorgane und private Verantwortliche. Die Bestimmung entspricht den Anforderungen von Artikel 7bis E-SEV 108 sowie Artikel 13 der Richtlinie (EU) 2016/680. Die Artikel 13 f. der Verordnung (EU) 2016/679 enthalten eine ähnliche Regelung.

Die Informationspflicht verbessert die Transparenz bei der Datenbearbeitung, die ein zentrales Ziel der Revision ist. Denn regelmässig kann die betroffene Person ohne entsprechende Informationen nicht erkennen, dass Daten über sie bearbeitet werden. Zugleich kann die betroffene Person ihre Rechte gemäss dem 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 Dazutun 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 18*b* 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 Vorkehren 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 Dazutun 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 automatischen 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 Dazutun 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 un 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 Identität[97]. 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 Gesetzgebund 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 Datenschutzbeauftragen 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 Vorkehren den Verstoss gegen Datenschutzvorschriften verunmöglichen oder zumindest die Gefahr erheblich verringern. Zugleich sind datenschutzfreundliche Technologien unabdingbar für die praktische Umsetzung der Datenschutzvorschriften. Denn Datenbearbeitung ist in vieler Hinsicht bereits allgegenwärtig und wird tendenziell weiter zunehmen (Ubiquitous Computing). Dies sorgt für kaum überblickbare Datenmengen, die im Einklang mit den Datenschutzregeln bearbeitet werden müssen, wofür technische Vorkehren zentral sind. Insgesamt zielt der technikgestützte Datenschutz nicht auf eine bestimmte Technologie. Vielmehr geht es darum, Systeme zur Datenbearbeitung technisch und organisatorisch so auszugestalten, dass sie insbesondere den Grundsätzen nach Artikel 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 gleichmässigere 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 Sekor ihre Rechte kaum wahrnehmen. Dies wird hauptsächlich auf die Kostenrisiken eines Prozesses zurückgeführt[100], 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 erfolgte[101]. 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 Personendaben zu rechtfertigen mit der Begründung, diese erfolge zur Bearbeitung zu Zwecken der Forschung, Planung oder Statistik.

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

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

Aufgehoben wird hingegen die Bestimmung betreffend das vereinfachte Verfahren für Auskunftsbegehren. Diese Regelung ist mit Einführung der ZPO[106] 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 Einzentscheidung. 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 17*a* DSG sollen nicht die Voraussetzungen abschwächen, unter denen ein Bundesorgan vor Inkrafttreten eines Gesetzes im formellen Sinn im Rahmen eines Pilotversuchs Daten automatisiert bearbeiten kann. Es soll lediglich die Regelungsdichte reduziert werden. Denn seit dem Inkrafttreten dieser Norm haben die Bundesorgane nur selten darauf zurückgegriffen. Gewisse Bestimmungen von Artikel 17*a* DSG können zudem in die künftigen Ausführungsverordnung aufgenommen werden.

Abgesehen davon, dass der Begriff «Persönlichkeitsprofile» durch «Profiling» ersetzt wird, stimmen die Voraussetzungen nach den Absätzen 1 und 2 mit jenen von Artikel 17*a* 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 17*a* Absatz 2 DSG begründet, der die Fälle aufzählt, in denen die praktische Umsetzung einer Datenbearbeitung zwingend eine Testphase erfordern kann. Aus den hiervor aufgeführten Gründen können diese Fälle in einer Ausführungsverordnung geregelt werden.

Die Absätze 3 und 4 bleiben, von 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 1bis 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 3bis 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 DSG. 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 DSG. Sie bleibt materiell unverändert.

8.1.6.9 Art. 34 Ansprüche und Verfahren

Artikel 34 entspricht weitgehend dem heutigen Artikel 25 DSG. 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 DSG. Um die Anforderungen von Artikel 8 Buchstabe e E-SEV 108 und von Artikel 16 der Richtlinie (EU) 2016/680 zu berücksichtigen, wird dieser Anspruch nun ausdrücklich in Artikel 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 DSG, 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, Bildungseinrichtugen, 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 Einzelfallen 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 25bis 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 VDSG 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 12bis Absatz 4 E-SEV 108 und von Artikel 42 Absätze 1 und 2 der Richtlinie (EU) 2016/680, der denselben Wortlaut hat wie Artikel 52 Absätze 1 und 2 der Verordnung (EU) 2016/679.

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 Beauftragen; die Stellvertreterin oder der Stellvertreter sowie das Sekretariat unterstehen dem BPG.

Nach Artikel 26*b* DSG ist lediglich vorgesehen, dass der Bundesrat der oder dem Beauftragten gestatten kann, eine andere Beschäftigung auszuüben, wenn dadurch deren oder dessen Unabhängigkeit und Ansehen nicht beeinträchtigt werden. Artikel 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 einem Entscheid 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 11*a* 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 DSG 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 Amtgeheimnis 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 DSG. 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 12bis 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 Verfügunskompetenz 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 anficht. 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 12bis 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 Aktzeptanz solcher Verfügungen sowie die Wahrung der Verfahrensrechte sicherzustellen, hätte die Organisation des Beauftragten verändert werden müssen, beispielsweise analog zur Schweizerischen Wettwewerbskommission. 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 Auskunfts-, 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 1998[112] (SBG; Art. 56) oder im Bundesgesetz über die Banken und Sparkassen vom 8. November 1934[113] (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 privatePersonen 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 Disziplinarmassnahmen 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 vorgesehenen 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 Datenbeabeitung 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 1974[115] 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 Wettbewerbsrechts[116]. 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 108[117] 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] BBl **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 2015[119]

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,** BBl 2014 5133), das Bundesgesetz vom 4. Oktober 1991 über die Eidgenössischen Technischen Hochschulen (SR 414.110, BBl 2016 3369) und das Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung (SR 510.10, BBl 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, BBl 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 1998[120]

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 2004[121]

Art. 7 Abs. 2 und 3

Nach Artikel 7 Absatz 2 wird der Zugang zu amtlichen Dokumenten eintschränkt, 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 1968[122]

Art. 71a

Mit Absatz 1 wird ein vom Bundesgericht entwickelter Grundsatz[123] 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 45*a* Absatz 3 Ziffer 3 VE-ZGB[124] 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 2013[125] 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 45*a* 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 2000[126] 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 Betimmungen sind entsprechend umzuformulieren, so dass die Bearbeitung von besonders schützenswerten Personendaten und das Profiling zulässig sind.

8.2.9 Zivilprozessordnung[127]

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 Entscheidverfahren keine Gerichtskosten gesprochen werden, wie dies zum Beispiel auch für Streitigkeiten nach dem Gleichstellungs- oder Mitwirkungsgesetz oder für arbeitsrechtliche Streitigkeiten bis zu einem Streitwert bis 30 000 Franken gilt.

Durch diese wichtige Neuregelung werden Entscheidverfahren nach 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 1987[129] 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. 179novies

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 179novies zu definieren.

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

Art. 179decies

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 Privatbereich[130]. 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 ausreichen[131].

Bei der Verwendung einer fremden Identität in Schädigungsabsicht oder zwecks Erlangung eines unrechtmässigen Vorteils stellt sich in der Regel die Frage nach der Anwendung weiterer Strafbestimmungen wie Betrug, Urkundenfälschung oder Delikte gegen die Ehre. In Fällen, in welchen der Unrechtsgehalt der Tat durch den gleichzeitig anwendbaren Tatbestand nicht gänzlich abgedeckt wird, der Aspekt der Persönlichkeitsverletzung durch den Identitätsmissbrauch also noch nicht berücksichtigt wird, ist von echter Konkurrenz auszugehen. Beide Strafbestimmungen finden Anwendung. Nimmt der Täter beispielsweise auf einem sozialen Netzwerk die Identität von B an und verleumdet C, wird neben dem Straftatbestand der Verleumdung auch der neu zu schaffende Tatbestand des Identitätsmissbrauchs angewendet. Nur so wird das gegen B begangene Unrecht geahndet und die bei diesem entstandenen negativen Folgen wie Reputationsverlust, Einleitung eines Verfahrens oder eine aufwändige und nur bedingt erfolgreiche Richtigstellung berücksichtigt. Im Falle des unbefugten Beschaffens von Personendaten[132] 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 1974[133] 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 349*g* 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 Grundsatz[134] 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 1979[135] (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 349*g* Absatz 3 VE-StGB (Ziff. 8.3.1.7).

Art. 25*c*

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 349*g* Absatz 2 VE-StGB verwiesen (Ziff. 8.3.1.7).

8.2.14 Bundesgesetz vom 13. Juni 2008[136] über die polizeilichen Informationssysteme des Bundes

Art. 5 Titel, Abs. 2

Nach Ansicht des Bundesrates kann Artikel 5 Abstz 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 1992[137]

Art. 14a Abs. 1 erster und zweiter Satz

In Artikel 14*a* 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 2008[138] 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 1997[139]

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

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

Art. 32g zweiter Satz

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

8.2.19 Bundesgesetz vom 4. Oktober 2002[140] über den Bevölkerungsschutz und den Zivilschutz

Art. 72 Abs. 1 und 1bis

Nach geltendem Recht ist die zuständige Bundesbehörde befugt, namentlich zur Abklärung des Kaderpotenzials von Schutzdienstpflichtigen und Kursteilnehmenden Persönlichkeitsprofile zu erstellen[141]. 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 1948[142] 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 1951[143] 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 111*f* 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 349*b* 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 349*b* von Artikel 29 VE-DSG ab. Fehlt eine Rechtsgrundlage, so dürfen die Bundesbehörden Daten ausschliesslich in den Fällen nach Artikel 349*b* 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 349*c* entspricht der Lösung des Bundesgesetzgebers in Artikel 6 SIaG. Für die Bekanntgabe von Daten an Behörden eines Schengen-Staates gelten dieselben Datenschutzvorschriften wie für die Bekanntgabe an eine nationale Behörde. Die Verabschiedung neuer gesetzlicher Einschränkungen ist weiterhin möglich, sofern der Gleichbehandlungsgrundsatz eingehalten wird.

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 349*d* 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 Zusatzprotokoll[144]. 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 349*e* Artikel 6*b* SIaG, der aus systematischen Gründen aufgehoben wird.

Die entsprechende Bekanntgabe von Daten ist nur möglich, wenn die drei Voraussetzungen nach Absatz 1 kumulativ erfüllt sind. In Übereinstimmung mit den Grundsätzen der Zweckbindung und der Verhältnismässigkeit muss die Bekanntgabe für die Verhütung, Feststellung oder Verfolgung einer Straftat erforderlich sein und muss die empfangende Behörde dafür zuständig sein (Abs. 1 Einleitungssatz und Bst. a). Der Schengen-Staat, bei dem die Daten beschafft wurden, muss der Bekanntgabe zudem vorgängig zugestimmt haben (Bst. b). Schliesslich muss der Drittstaat oder das internationale Organ ein angemessenes Datenschutzniveau im Sinne von Artikel 349*d* 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 349*f* 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 349*f* 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 349*f* 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 349*f* 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 349*f* benachrichtigen muss. Anders als im Fall von Artikel 349*d* 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 Beahörde 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 349*h* wurde die Lösung in Artikel 8 des Bundesgesetzes vom 13. Juni 2008[147] 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 349*h* 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 349*i* Absatz 1 vom Beauftragten die Eröffnung einer Untersuchung verlangen. Damit das entsprechende Gesuch zulässig ist, muss die betroffene Person glaubhaft machen, dass ein Austausch von Daten über sie gegen die Datenschutzvorschriften verstösst, zum Beispiel in Bezug auf die Anforderungen an die Bekanntgabe von Daten an einen Drittstaat oder ein internationales Organ (Art. 349*d* 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. 349*h* 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. 349*c*) 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 355*f* StGB regelt die Bekanntgabe von Daten aus einem Schengen-Staat an einen Drittstaat oder ein internationales Organ im Bereich der justiziellen Zusammenarbeit im Rahmen der Schengen-Assoziierungsabkommen. Er kann aufgehoben werden. Aus systematischen Gründen wird diese Kategorie von Bekanntgaben 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 355*g* kann somit aufgehoben werden.

8.3.2 Strafprozessordnung[148]

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 349*g* 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 349*g* Absatz 2 VE-StGB (Ziff. 8.3.1.7).

8.3.3 Rechtshilfegesetz vom 20. März 1981[149]

Mit dieser Vorlage wird im IRSG ein neues Kapitel 1*b* 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 Strafentscheid 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 1975[150] zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen ein Verweis auf die Artikel 11b–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 1973[151] zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen vorbehalten.

8.3.5 Bundesgesetz vom 7. Oktober 1994[152] 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 349a bis 349i 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 8bis 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 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 11*a* Absatz 2 DSG vorgesehenen Pflicht entspricht, dem Beauftragten sämtliche Datensammlungen zur Registrierung anzumelden.

In Bezug auf das vom Beauftragten geführte Register der Datensammlungen ergibt sich mit dem Inkrafttreten des neuen Gesetzes die Änderung, dass darin nur noch die 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 Kommission[153], 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] ABl. 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 2015–2019[154] 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] BBl **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 Datenschutzübereinkommens[155] schreibt, enthält die Bundesverfassung keine Bestimmung, die dem Bund ausdrücklich eine Kompetenz im Datenschutzbereich zuweist. Wohl stipuliert Artikel 13 Absatz 2 BV den Anspruch jeder Person auf Schutz vor Missbrauch ihrer persönlichen Daten. Es handelt sich hier aber um ein Grundrecht, dass dem Bund keine neuen Zuständigkeiten überträgt. Gemäss Artikel 35 Absätze 2 und 3 BV sind Personen, die staatliche Aufgaben wahrnehmen, an die Grundrechte gebunden und verpflichtet, zu ihrer Verwirklichung beizutragen, und die Behörden sorgen dafür, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden. Der Entwurf trägt in diesem Sinne zur Verwirklichung von Artikel 13 Absatz 2 BV bei, und zwar sowohl hinsichtlich der Beziehungen zwischen Staat und Privaten als auch zwischen Individuen.

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 Matelerlasses enthält die Änderungen von Bundesgesetzen, die sich aus der Umsetzung der Richtlinie (EU) 2016/680 im Rahmen der Schengen-Verpflichtungen ergeben.

---

[155] BBl **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. 45*a* Abs. 4 VE-ZGB).

Europarat Datenschutz-übereinkommen

September 2016

Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[1]

Präambel

Die Mitgliederstaaten des Europarats, die dieses Übereinkommen unterzeichnen –

in der Erwägung, dass es das Ziel des Europarats ist, eine engere Verbindung zwischen seinen Mitgliedern herbeizuführen, die vor allem auf der Achtung des Vorranges des Rechts sowie der Menschenrechte und Grundfreiheiten beruht;

in der Erwägung, dass es notwendig ist, die menschliche Würde und den Schutz der Menschenrechte und der individuellen Grundfreiheiten zu gewährleisten sowie – angesichts der Diversifizierung, Intensivierung und Internationalisierung der Datenverarbeitung und des Verkehrs personenbezogener Daten – die Selbstbestimmung sicherzustellen, die auf dem individuellen Recht beruht, die Kontrolle über die eigenen personenbezogenen Daten und deren Verarbeitung auszuüben;

unter Hinweis darauf, dass das Recht auf Schutz personenbezogener Daten im Hinblick auf dessen Rolle in der Gesellschaft zu berücksichtigen und mit anderen Menschenrechten und Grundfreiheiten, darunter die freie Meinungsäusserung, in Einklang zu bringen ist;

in der Erwägung, dass dieses Übereinkommen bei der Umsetzung der darin festgeschriebenen Regeln die Berücksichtigung des grundsätzlichen Rechts auf Zugang zu amtlichen Dokumenten erlaubt;

in Anerkennung der Notwendigkeit, die grundlegenden Werte der Achtung der Privatsphäre und des Schutzes personenbezogener Daten weltweit zu fördern und damit zum freien Informationsaustausch zwischen den Völkern beizutragen;

in Anerkennung der Bedeutung einer verstärkten internationalen Zusammenarbeit zwischen den Vertragsparteien des Übereinkommens –

sind wie folgt übereingekommen:

Kapitel I – Allgemeine Bestimmungen

Art. 1 – Gegenstand und Zweck

Zweck dieses Übereinkommens ist es, alle natürlichen Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthalts in Bezug auf die Verarbeitung ihrer personenbezogenen Daten zu schützen und damit zur Achtung ihrer Menschenrechte und Grundfreiheiten, insbesondere ihres Rechts auf Privatsphäre beizutragen.

Art. 2 – Begriffsbestimmungen

In diesem Übereinkommen:

a. bedeutet «personenbezogene Daten» jede Information über eine bestimmte oder bestimmbare natürliche Person («betroffene Person»);

b. umfasst «Datenverarbeitung» jeden Vorgang oder Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, Speichern, Aufbewahren, Verändern, Wiedergewinnen, Bekanntgeben, Bereitstellen, Löschen oder Vernichten der Daten oder das Durchführen logischer und/oder rechnerischer Operationen mit diesen Daten;

c. Wird kein automatisiertes Verfahren angewandt, bezeichnet der Begriff der Datenverarbeitung einen Vorgang oder eine Vorgangsreihe im Zusammenhang mit personenbezogenen Daten in einem strukturierten Datenbestand, die nach spezifischen Kriterien zugänglich oder auffindbar sind;

[1] Konsolidierter Wortlaut der Vorschläge zur Modernisierung des Übereinkommens 108 im Anschluss an die Sitzung des CAHDATA (15./16. Juni 2016). Die Russische Föderation hat spezifisch zu Art. 3 Abs. 1, 9 Abs. 1 und 2 Stellung genommen sowie Einwände zu Art. 12 Abs. 1 des modernisierten Übereinkommensentwurfs vorgebracht (vgl. Kurzbericht des CAHDATA).

d. bedeutet «der für die Verarbeitung Verantwortliche» die natürliche oder juristische Person, die Behörde, die Einrichtung, die Agentur oder jede andere Stelle, die allein oder gemeinsam mit anderen bei der Datenverarbeitung entscheidungsbefugt ist;

e. bedeutet «Empfänger» die natürliche oder juristische Person, die Behörde, die Einrichtung, die Agentur oder jede andere Stelle, der Daten bekanntgegeben oder zugänglich gemacht werden;

f. bedeutet «Auftragsverarbeiter» die natürliche oder juristische Person, die Behörde, die Einrichtung, die Agentur oder jede andere Stelle, die im Auftrag des für die Verarbeitung Verantwortlichen personenbezogene Daten verarbeitet.

Art. 3 – Geltungsbereich

1. Jede Vertragspartei verpflichtet sich, dieses Übereinkommen auf die Datenverarbeitungen in ihrem Zuständigkeitsbereich im öffentlichen und privaten Bereich anzuwenden und damit jedem Menschen das Recht auf Schutz seiner personenbezogenen Daten zu gewährleisten.

1bis. Dieses Übereinkommen findet keine Anwendung auf die Datenverarbeitung, die von einer Person im Rahmen ausschliesslich persönlicher oder familiärer Tätigkeiten ausgeführt wird.

Kapitel II – Grundsätze für den Schutz personenbezogener Daten

Art. 4 – Pflichten der Vertragsparteien

1. Jede Vertragspartei trifft in ihrem innerstaatlichen Recht die erforderlichen Massnahmen, um die Bestimmungen dieses Übereinkommens zu verwirklichen und die wirksame Umsetzung sicherzustellen.

2. Diese Massnahmen sind durch jede Vertragspartei zu treffen und treten zum Zeitpunkt der Ratifizierung dieses Übereinkommens oder des Beitritts dazu in Kraft.

3. Jede Vertragspartei verpflichtet sich:

    a. dem Ausschuss der Vertragsparteien nach Kapitel V zu gestatten, die Wirksamkeit der Massnahmen zu beurteilen, die sie im innerstaatlichen Recht getroffen hat, um die Bestimmungen dieses Übereinkommens zu verwirklichen; und

    b. aktiv an diesem Beurteilungsprozess teilzunehmen.

Art. 5 – Rechtmässigkeit der Datenverarbeitung und Qualität der Daten

1. Die Datenverarbeitung muss in einem angemessenen Verhältnis zum rechtmässig verfolgten Zweck stehen und in jedem Verarbeitungsschritt die sorgfältige Abwägung aller vorhandenen öffentlichen oder privaten Interessen im Lichte der betroffenen Rechte und Freiheiten erkennen lassen.

2. Jede Vertragspartei stellt sicher, dass die Datenverarbeitung ausschliesslich nach vorheriger Aufklärung auf der Grundlage der freien und unzweideutigen Einwilligung der betroffenen Person eigens für diesen Fall oder gestützt auf eine andere gesetzlich vorgesehene, rechtmässige Grundlage erfolgt.

3. Personenbezogene Daten müssen auf rechtmässige Weise verarbeitet werden.

4. Personenbezogene Daten müssen im Rahmen ihrer Verarbeitung:

    a. nach Treu und Glauben und auf transparente Weise verarbeitet werden;

    b. für eindeutige, festgelegte und rechtmässige Zwecke erhoben werden und dürfen nicht so verarbeitet werden, dass es mit diesen Zwecken unvereinbar ist; die Weiterverarbeitung zu archivarischen Zwecken im öffentlichen Interesse, zu Zwecken der wissenschaftlichen oder historischen Forschung oder zu statistischen Zwecken ist mit diesen Zwecken vereinbar, sofern zusätzliche Sicherheiten vorgesehen sind;

    c. den Verarbeitungszwecken entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen;

    d. richtig und wenn nötig auf den neuesten Stand gebracht sein;

e. nicht länger in einer Form aufbewahrt zu werden, welche die Identifikation der betroffenen Person erlaubt, als es die Zwecke, für die sie verarbeitet werden, erfordern.

Art. 6 – Besondere Arten von Daten

1. Die Verarbeitung:

   - genetischer Daten,
   - personenbezogener Daten über Straftaten, -verfahren und -urteile und über damit zusammenhängende Sicherheitsmassnahmen,
   - biometrischer Daten, die ein Individuum eindeutig identifizieren,
   - personenbezogener Daten, die Hinweise über die rassische oder ethnische Herkunft, politische Anschauungen, Gewerkschaftszugehörigkeit, religiöse oder andere Überzeugungen, die Gesundheit oder das Sexualleben erkennen lassen,

   ist nur unter der Bedingung zulässig, dass zusätzlich zum Schutz durch dieses Übereinkommen geeignete Sicherheiten im Gesetz vorgesehen sind.

2. Diese Sicherheiten müssen geeignet sein, die möglichen Risiken für die Interessen, Rechte und Grundfreiheiten der betroffenen Person bei der Verarbeitung sensibler Daten zu verhindern, insbesondere das Risiko einer Diskriminierung.

Art. 7 – Datensicherung

1. Jede Vertragspartei stellt sicher, dass der für die Verarbeitung Verantwortliche und gegebenenfalls der Auftragsverarbeiter geeignete Sicherungsmassnahmen gegen Risiken wie den zufälligen oder unbefugten Zugriff auf personenbezogene Daten oder deren Zerstörung, Verlust, Verwendung, Veränderung oder Bekanntgabe treffen.

2. Jede Vertragspartei stellt sicher, dass der für die Verarbeitung Verantwortliche Verstösse gegen die Datensicherheit, welche die Rechte und Grundfreiheiten der betroffenen Person erheblich zu beeinträchtigen vermögen, ohne übermässige Verzögerung zumindest der zuständigen Aufsichtsbehörde nach Artikel 12bis meldet.

Art. 7bis – Transparenz der Datenverarbeitung

1. Jede Vertragspartei stellt sicher, dass der für die Verarbeitung Verantwortliche der betroffenen Person Auskunft gibt über:

   a. seine Identität sowie seinen gewöhnlichen Aufenthaltsort oder Sitz;
   b. die gesetzliche Grundlage und den Zweck der beabsichtigten Verarbeitung;
   c. die Kategorien personenbezogener Daten;
   d. gegebenenfalls die Empfänger oder Empfängerkategorien der personenbezogenen Daten; und
   e. die Mittel zur Ausübung der Rechte nach Artikel 8;

sowie über alle zusätzlich erforderlichen Informationen, um sicherzustellen, dass die personenbezogenen Daten nach Treu und Glauben und auf transparente Weise verarbeitet werden.

1bis. Absatz 1 ist nicht anwendbar, wenn die betroffene Person bereits informiert ist.

2. Werden die Daten nicht direkt bei der betroffenen Person erhoben, ist der für die Verarbeitung Verantwortliche nicht verpflichtet, diese Auskünfte zu erteilen, sofern die Verarbeitung im Gesetz ausdrücklich vorgesehen ist oder die Auskunftserteilung nicht oder nur unter unverhältnismässigem Aufwand möglich ist.

Art. 8 – Rechte der betroffenen Person

1. Jede Person hat das Recht:

   a. nicht einer Entscheidung unterworfen zu werden, die erhebliche Auswirkungen auf sie hat und die ausschliesslich aufg einer automatischen Datenverarbeitung beruht, ohne dass ihr Standpunkt berücksichtigt wird;

b. auf Antrag in angemessenen Zeitabständen und ohne unzumutbare Verzögerung oder übermässige Kosten folgende Auskünfte zu erhalten: die Bestätigung, ob Daten über sie verarbeitet werden, die Mitteilung der verarbeiteten Daten in verständlicher Form sowie alle verfügbaren Informationen über deren Herkunft, die Dauer ihrer Aufbewahrung und alle sonstigen Angaben, die der für die Verarbeitung Verantwortliche im Sinne der Transparenz der Datenverarbeitung nach Artikel 7bis Absatz 1 zu machen hat;

c. auf Antrag die Logik zu erfahren, die der Datenverarbeitung zugrunde liegt, sofern die Ergebnisse dieser Verarbeitung sie betreffen;

d. jederzeit aus Gründen, die sich aus ihrer Situation ergeben, gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen, es sei denn, der für die Verarbeitung Verantwortliche weist rechtmässige Gründe nach, welche die Verarbeitung rechtfertigen und gegenüber den Interessen oder den Rechten und Grundfreiheiten der betroffenen Person überwiegen;

e. auf Antrag ohne unzumutbare Verzögerung oder übermässige Kosten Daten berichtigen oder gegebenenfalls löschen zu lassen, wenn sie entgegen den Vorschriften dieses Übereinkommens verarbeitet worden sind;

f. über ein Rechtsmittel nach Artikel 10 zu verfügen, sofern ihre Rechte gemäss diesem Übereinkommen verletzt wurden;

g. unabhängig von ihrer Staatsangehörigkeit oder ihrem Aufenthalt bei der Ausübung ihrer Rechte gemäss diesem Übereinkommen die Unterstützung einer Aufsichtsbehörde im Sinne von Artikel 12bis zu erhalten.

2. Absatz 1 Buchstabe a ist nicht anwendbar, wenn die Entscheidung aufgrund des Gesetzes, dem der für die Verarbeitung Verantwortliche unterstellt ist, zulässig ist und dieses Gesetz zudem geeignete Massnahmen zum Schutz der Rechte und Freiheiten sowie der legitimen Interessen der betroffenen Person vorsieht.

Art. 8bis – Zusätzliche Pflichten

1. Jede Vertragspartei stellt sicher, dass die für die Verarbeitung Verantwortlichen sowie gegebenenfalls die Auftragsverarbeiter alle geeigneten Massnahmen treffen, um die Verpflichtungen dieses Übereinkommens einzuhalten und insbesondere gegenüber der zuständigen Aufsichtsbehörde nach Artikel 12bis darlegen zu können, dass die Verarbeitung, für die sie verantwortlich sind, mit den Bestimmungen dieses Übereinkommens in Einklang stehen.

2. Jede Vertragspartei stellt sicher, dass die für die Verarbeitung Verantwortlichen sowie gegebenenfalls die Auftragsverarbeiter vor Beginn jeder Verarbeitung die möglichen Auswirkungen der geplanten Datenverarbeitung auf die Rechte und Grundfreiheiten der betroffenen Person prüfen und die Datenverarbeitung so ausgestalten, dass das Risiko der Verletzung dieser Rechte und Grundfreiheiten vermieden oder auf ein Mindestmass beschränkt wird.

3. Jede Vertragspartei stellt sicher, dass die für die Verarbeitung Verantwortlichen sowie gegebenenfalls die Auftragsverarbeiter technische und organisatorische Massnahmen zur Berücksichtigung der Implikationen treffen, die sich aus dem Recht auf Schutz der personenbezogenen Daten ergeben.

4. Jede Vertragspartei kann mit Blick auf die Risiken für die Interessen, Rechte und Grundfreiheiten der betroffenen Person die Umsetzung der Bestimmungen von Absatz 1-3 im Gesetz zur Verwirklichung dieses Übereinkommens auf Art und Umfang der Daten, auf Art, Tragweite und Zweck der Verarbeitung sowie gegebenenfalls auf die Grösse der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter abstimmen.

Art. 9 – Ausnahmen und Einschränkungen

1. Ausnahmen von den Bestimmungen dieses Kapitels sind nicht zulässig, abgesehen von jenen in Artikel 5 Absatz 4, 7 Absatz 2, 7bis Absatz 1 und 8, sofern eine derartige Ausnahme im Gesetz vorgesehen ist, den Kerngehalt der Rechte und Grundfreiheiten wahrt und in einer demokratischen Gesellschaft eine notwendige und verhältnismässige Massnahme ist:

a. für die Staatssicherheit, die Verteidigung, die öffentliche Sicherheit, für wichtige Wirtschafts- und Finanzinteressen des Staates, für die Unparteilichkeit und Unabhängigkeit der Justiz oder zur

Verhütung, Aufklärung und Bekämpfung von Straftaten und den Strafvollzug sowie für weitere übergeordnete Ziele im Allgemeininteresse;

b. zum Schutz des betroffenen Person oder der Rechte und Freiheiten Dritter, insbesondere der freien Meinungsäusserung.

2. Die Ausübung der Bestimmungen in Artikel 7bis und 8 kann durch Gesetz für die Verarbeitung von Daten eingeschränkt werden, die archivarischen Zwecken im öffentlichen Interesse, Zwecken der wissenschaftlichen oder historischen Forschung oder statistischen Zwecken dienen, wenn keine erkennbare Gefahr besteht, dass die Rechte und Grundfreiheiten der betroffenen Person beeinträchtigt werden.

3. Ausser in den Ausnahmefällen nach Absatz 1, die Verarbeitungstätigkeiten zum Zwecke der Staatssicherheit und der Verteidigung betreffen, kann jede Vertragspartei im Gesetz Ausnahmen von Artikel 12 Absätze 5 und 6 sowie von Artikel 12bis Absatz 2 Buchstaben a, b, c und d vorsehen, allerdings nur soweit dies in einer demokratischen Gesellschaft eine notwendigr und verhältnismässige Massnahme ist.

Dies gilt unbeschadet der Anforderung, dass Verarbeitungstätigkeiten zum Zwecke der Staatssicherheit und der Verteidigung wirksam und unabhängig zu prüfen und zu kontrollieren sind.

Art. 10 – Sanktionen und Rechtsmittel

Jede Vertragspartei verpflichtet sich, geeignete gerichtliche und nicht-gerichtliche Sanktionen und Rechtsmittel für Verletzungen der Vorschriften dieses Übereinkommens festzulegen.

Art. 11 – Weitergehender Schutz

Dieses Kapitel ist nicht so auszulegen, dass es die Möglichkeit einer Vertragspartei begrenzt oder auf andere Weise beeinträchtigt, den betroffenen Personen ein grösseres Mass an Schutz zu gewähren, als in diesem Übereinkommen vorgeschrieben ist.

Kapitel III – Grenzüberschreitender Verkehr personenbezogener Daten

Art. 12 – Grenzüberschreitender Verkehr personenbezogener Daten

1. Eine Vertragspartei darf allein zum Zweck des Schutzes personenbezogener Daten die Weitergabe dieser Daten an einen Empfänger unter der Gerichtsbarkeit einer anderen Vertragspartei nicht verbieten oder von einer besonderen Genehmigung abhängig machen. Dies ist jedoch zulässig, wenn die Vertragspartei einheitliche Schutzbestimmungen einhalten muss, die den Mitgliedsstaaten einer regionalen internationalen Organisation gemeinsam sind.

2. Untersteht der Empfänger der Gerichtsbarkeit eines Staates oder einer internationalen Organisation, die nicht Vertragspartei dieses Übereinkommens ist, so ist die Weitergabe personenbezogener Daten nur möglich, wenn ein angemessenes Schutzniveau auf der Grundlage dieses Übereinkommens gewährleistet ist.

3. Ein angemessenes Datenschutzniveau kann gewährleistet sein durch:

   a. Rechtsvorschriften des betreffenden Staates oder der betreffenden internationalen Organisation, einschliesslich der anwendbaren Staatsverträge oder internationalen Abkommen; oder

   b. Ad-hoc- oder standardisierte, genehmigte Garantien auf der Grundlage rechtsverbindlicher und durchsetzbarer Instrumente, die von den Personen, die an der Weitergabe und -verarbeitung der Daten beteiligt sind, vereinbart und verwirklicht werden.

4. Ungeachtet der vorangehenden Absätze kann jede Vertragspartei vorsehen, dass die Weitergabe personenbezogener Daten zulässig ist, sofern:

   a. die betroffene Person eigens für diesen Fall seine freie und unzweideutige Einwilligung erteilt hat, nach vorheriger Aufklärung über die Risiken, die mit dem Fehlen angemessener Sicherheiten einhergehen; oder

   b. bestimmte Interessen der betroffenen Person dies im Einzelfall erfordern; oder

c. legitime überwiegende Interessen, insbesondere wichtige öffentliche Interessen im Gesetz vorgesehen sind und die Weitergabe in einer demokratischen Gesellschaft eine notwendige und verhältnismässige Massnahme ist;

d. die Weitergabe in einer demokratischen Gesellschaft im Hinblick auf die freie Meinungsäusserung eine notwendige und verhältnismässige Massnahme ist.

5. Jede Vertragspartei stellt sicher, dass die zuständige Aufsichtsbehörde nach Artikel 12bis alle zweckdienlichen Informationen über Datenweitergaben gemäss Absatz 3 Buchstabe b und, auf Antrag, gemäss Absatz 4 Buchstaben b und c erhält.

6. Jede Vertragspartei stellt zudem sicher, dass die Aufsichtsbehörde von der weitergebenden Person den Nachweis über die Wirksamkeit der verwendeten Garantien oder das Vorhandensein legitimer überwiegender Interessen verlangen kann und dass sie zum Schutz der Rechte und Grundfreiheiten der betroffenen Person die Datenweitergabe verbieten, aussetzen oder an Bedingungen knüpfen kann.

Kapitel IIIbis – Aufsichtsbehörden

Art. 12bis – Aufsichtsbehörden

1. Jede Vertragspartei sieht eine oder mehrere Behörden vor, die dafür zuständig sind, die Einhaltung der Bestimmungen dieses Übereinkommens zu gewährleisten.

2. Zu diesem Zweck sind die besagten Behörden:

   a. befugt, Ermittlungen durchzuführen und einzuschreiten;

   b. mit den Aufgaben in Zusammenhang mit der Datenweitergabe nach Artikel 12 betraut, insbesondere der Genehmigung standardisierter Garantien;

   c. befugt, bei Verstössen gegen die Bestimmungen dieses Übereinkommens Entscheidungen zu fällen und insbesondere verwaltungsrechtliche Sanktionen zu verhängen;

   d. befugt, Anliegen vor Gericht zu vertreten bzw. den zuständigen Justizbehörden Verstösse gegen die Bestimmungen dieses Übereinkommens zur Kenntnis zu bringen;

   e. dafür zuständig:

      i. die Öffentlichkeit für die Aufgaben, Befugnisse und Tätigkeiten der Behörde zu sensibilisieren,
      ii. die Öffentlichkeit für die Rechte der betroffenen Personen und die Ausübung dieser Rechte zu sensibilisieren,
      iii. die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter für ihre Verantwortung aufgrund dieses Übereinkommens zu sensibilisieren,

      besondere Aufmerksamkeit gilt dem Recht auf Schutz der Daten von Kindern und anderen schutzbedürftigen Personen.

2bis. Die zuständigen Aufsichtsbehörden werden zu jedem Gesetzes- oder Verwaltungsvorhaben konsultiert, das die Verarbeitung personenbezogener Daten nach sich zieht.

3. Jede zuständige Aufsichtsbehörde behandelt die Anfragen und Beschwerden, die betroffene Personen hinsichtlich ihrer Rechte auf Datenschutz vorbringen, und hält diese über die Ergebnisse auf dem laufenden.

4. Die Aufsichtsbehörden handeln bei der Wahrnehmung ihrer Aufgaben und der Ausübung ihrer Befugnisse unabhängig und unparteilich und dürfen dabei keine Weisungen einholen oder entgegennehmen.

5. Jede Vertragspartei stellt sicher, dass die Aufsichtsbehörden über die erforderlichen Ressourcen zur tatsächlichen Wahrnehmung ihrer Aufgaben und Ausübung ihrer Befugnisse verfügen.

5bis. Jede Aufsichtsbehörde erstellt und veröffentlicht periodisch einen Tätigkeitsbericht.

5ter. Mitglieder und Bedienstete der Aufsichtsbehörden unterliegen der Pflicht zur Geheimhaltung vertraulicher Informationen, zu denen Sie bei der Wahrnehmung ihrer Aufgaben und der Ausübung ihrer Befugnisse Zugang hatten oder haben.

6. Entscheidungen der Aufsichtsbehörden können vor Gericht angefochten werden.

7. In Übereinstimmung mit den Bestimmungen von Kapitel IV arbeiten die Aufsichtsbehörden zusammen, soweit dies für die Wahrnehmung ihrer Aufgaben und die Ausübung ihrer Befugnisse erforderlich ist, wobei sie insbesondere:

   a. einander durch den Austausch von zweckdienlichen und nützlichen Informationen sowie durch gegenseitige Zusammenarbeit Hilfe leisten, unter der Bedingung, dass hinsichtlich des Schutzes personenbezogener Daten sämtliche Regeln und Sicherheiten dieses Übereinkommens eingehalten werden;

   b. ihre Ermittlungen und Interventionen koordinieren oder gemeinsam tätig werden;

   c. Informationen und Unterlagen über ihr Recht und ihre Verwaltungspraxis im Bereich des Datenschutzes zur Verfügung stellen.

7bis. Die Informationen nach Absatz 7 Buchstabe a umfassen nicht personenbezogene Daten, die verarbeitet werden, es sei denn, diese Daten sind für die Zusammenarbeit unerlässlich oder die betroffene Person hat eigens für diesen Fall ihre unzweideutige, freie und aufgeklärte Einwilligung erteilt.

8. Zur Organisation ihrer Zusammenarbeit und zur Wahrnehmung der Aufgaben gemäss den vorangehenden Absätzen bilden die Aufsichtsbehörden der Vertragsparteien ein Netzwerk.

9. Die Aufsichtsbehörden sind nicht zuständig im Falle von Verarbeitungen, die von Organen in Ausübung ihrer Rechtsprechungsbefugnisse ausgeführt werden.

Kapitel IV – Gegenseitige Hilfeleistung

Art. 13 – Zusammenarbeit zwischen den Vertragsparteien

1. Die Vertragsparteien verpflichten sich, einander bei der Durchführung dieses Übereinkommens Hilfe zu leisten.

2. Zu diesem Zweck:

   a. bezeichnet jede Vertragspartei eine oder mehrere Aufsichtsbehörden nach Artikel 12bis und teilt deren amtliche Bezeichnung und Anschrift dem Generalsekretär des Europarats mit;

   b. legt jede Vertragspartei, die mehrere Aufsichtsbehörden bezeichnet hat, die Zuständigkeit jeder Behörde fest und gibt sie in ihrer Mitteilung nach Buchstabe a an.

Art. 14 – Unterstützung von betroffenen Personen

1. Jede Vertragspartei unterstützt die betroffenen Personen unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnsitz bei der Ausübung der Rechte nach Artikel 8.

2. Eine im Hoheitsgebiet einer anderen Vertragspartei wohnende betroffene Person kann ihren Antrag über die bezeichnete Aufsichtsbehörde dieser Vertragspartei stellen.

3. Der Antrag auf Unterstützung muss alle erforderlichen Angaben enthalten, insbesondere über:

   a. den Namen, die Anschrift und alle anderen für die Identifizierung der antragstellenden betroffenen Person erheblichen Einzelheiten;

   b. die Verarbeitung oder den für die Verarbeitung Verantwortlichen, auf die sich der Antrag bezieht;

   c. den Gegenstand des Antrags.

Art. 15 – Sicherheiten bei Hilfeleistung durch bezeichnete Aufsichtsbehörden

1. Hat eine bezeichnete Aufsichtsbehörde einer Vertragspartei von einer bezeichneten Aufsichtsbehörde einer anderen Vertragspartei Auskünfte erhalten, die einem Antrag auf Unterstützung dienen oder Antwort auf ein eigenes Ersuchen geben, so darf sie diese Auskünfte nur zu den Zwecken verwenden, die dem Antrag oder Ersuchen zugrunde liegen.

2. Es ist einer bezeichneten Behörde in keinem Fall erlaubt, im Namen einer betroffenen Person von sich aus und ohne deren ausdrückliche Zustimmung einen Antrag auf Unterstützung zu stellen.

Art. 16 – Ablehnung von Ersuchen und Anträgen

Eine bezeichnete Aufsichtsbehörde, an die nach Artikel 13 ein Ersuchen oder ein Antrag gerichtet wird, kann dieses bzw. diesen nur ablehnen, wenn:

a. es bzw. er mit ihren Befugnissen nicht vereinbar sind;

b. es bzw. er den Bestimmungen dieses Übereinkommens nicht entsprechen;

c. dessen Erfüllung mit der Souveränität, der Sicherheit oder der öffentlichen Ordnung der Vertragspartei, die bezeichnet wurde, oder mit den Rechten und Grundfreiheiten der Personen, die der Gerichtsbarkeit dieser Vertragspartei unterstehen, nicht vereinbar wäre.

Art. 17 – Kosten und Verfahren

1. Für Hilfe, welche die Vertragsparteien einander nach Artikel 13 leisten, oder für Unterstützung, die sie betroffenen Personen nach Artikel 8 und 14 leisten, werden keine Auslagen oder Gebühren ausser für Sachverständige und Dolmetscher erhoben. Diese Auslagen oder Gebühren werden von der Vertragspartei getragen, welche die ersuchende Aufsichtsbehörde bezeichnet hat.

2. Die betroffene Person kann nicht verpflichtet werden, für Schritte, die im Hoheitsgebiet einer anderen Vertragspartei für ihn unternommen werden, höhere Auslagen oder Gebühren zu zahlen, als von Personen erhoben werden können, die im Hoheitsgebiet der betreffenden Vertragspartei wohnen.

3. Die sonstigen Einzelheiten im Zusammenhang mit der Hilfeleistung oder Unterstützung, insbesondere hinsichtlich der Form und der Verfahren sowie der zu verwendenden Sprachen, werden unmittelbar zwischen den beteiligten Vertragsparteien festgelegt.

Kapitel V – Ausschuss der Vertragsparteien

Art. 18 – Zusammensetzung des Ausschusses

1. Nach dem Inkrafttreten dieses Übereinkommens wird ein Ausschuss der Vertragsparteien eingesetzt.

2. Jede Vertragspartei ernennt einen Vertreter und einen Stellvertreter für diesen Ausschuss. Jeder Mitgliedstaat des Europarats, der nicht Vertragspartei des Übereinkommens ist, hat das Recht, sich im Ausschuss durch einen Beobachter vertreten zu lassen.

3. Der Ausschuss der Vertragsparteien kann durch Beschluss einer Zweidrittelmehrheit der Vertreter der Vertragsparteien einen Beobachter einladen, sich in seinen Sitzungen vertreten zu lassen.

4. Jede Vertragspartei, die nicht Mitgliedstaat des Europarats ist, beteiligt sich in dem vom Ministerkomitee im Einvernehmen mit dieser Vertragspartei festgesetzten Ausmass an der Finanzierung der Tätigkeit des Ausschusses.

Art. 19 – Aufgaben des Ausschusses

Der Ausschuss der Vertragsparteien:

a. kann Empfehlungen zur Erleichterung oder Verbesserung der Anwendung des Übereinkommens abgeben;

b. kann in Übereinstimmung mit Artikel 21 Änderungen dieses Übereinkommens vorschlagen;

c. nimmt zu jeder vorgeschlagenen Änderung dieses Übereinkommens Stellung, die ihm nach Artikel 21 Absatz 3 unterbreitet wird;

d. kann zu allen Fragen im Zusammenhang mit der Auslegung oder Anwendung dieses Übereinkommens Stellung nehmen;

e. gibt dem Ministerkomitee vor jedem Neubeitritt zum Übereinkommen eine Stellungnahme über das Schutzniveau für personenbezogene Daten ab, das der Beitrittskandidat gewährleistet, und empfiehlt gegebenenfalls Massnahmen zur Erfüllung der Anforderungen dieses Übereinkommens;

f. kann auf Ersuchen eines Staates oder einer internationalen Organisation prüfen, ob deren Schutzniveau für personenbezogene Daten die Anforderungen dieses Übereinkommens erfüllt, und empfiehlt gegebenenfalls Massnahmen zur Erfüllung dieser Anforderungen;

g. kann Muster für Standardsicherheiten im Sinne von Artikel 12 erarbeiten oder genehmigen;

h. überprüft die Umsetzung dieses Übereinkommens durch die Vertragsparteien und empfiehlt Massnahmen für den Fall, dass sich eine Vertragspartei nicht an dieses Übereinkommen hält.

i. erleichtert gegebenenfalls die gütliche Behebung aller Schwierigkeiten, die sich aus der Anwendung dieses Übereinkommens ergeben könnten.

Art. 20 – Verfahren

1. Der Ausschuss der Vertragsparteien wird vom Generalsekretär des Europarats einberufen. Seine erste Sitzung findet innerhalb von zwölf Monaten nach Inkrafttreten dieses Übereinkommens statt. Danach tritt er mindestens einmal im Jahr sowie immer dann zusammen, wenn ein Drittel der Vertreter der Vertragsparteien dies verlangt.

2. Der Ausschuss der Vertragsparteien ist in einer Sitzung beschlussfähig, wenn die Mehrheit der Vertreter der Vertragsparteien anwesend ist.

[3. .][2]

4. Im Anschluss an jede Sitzung unterbreitet der Ausschuss der Vertragsparteien dem Ministerkomitee des Europarats einen Bericht über seine Arbeit und die Wirksamkeit dieses Übereinkommens.

5. Der Ausschuss der Vertragsparteien gibt sich eine Geschäftsordnung und regelt insbesondere die Verfahren für die Beurteilung nach Artikel 4 Absatz 3 und die Prüfung des Datenschutzniveaus nach Artikel 19 auf der Grundlage objektiver Kriterien.

Kapitel VI – Änderungen

Art. 21 – Änderungen

1. Änderungen dieses Übereinkommens können von einer Vertragspartei, vom Ministerkomitee des Europarats oder vom Ausschuss der Vertragsparteien vorgeschlagen werden.

2. Der Generalsekretär des Europarats teilt jeden Änderungsvorschlag den Vertragsparteien dieses Übereinkommens, den anderen Mitgliedstaaten des Europarats, der Europäischen Union sowie jedem Nichtmitgliedstaat oder jeder internationalen Organisation mit, die nach Artikel 23 eingeladen worden sind, diesem Übereinkommen beizutreten.

3. Darüber hinaus wird jede von einer Vertragspartei oder vom Ministerkomitee vorgeschlagene Änderung dem Ausschuss der Vertragsparteien übermittelt; dieser teilt dem Ministerkomitee seine Stellungnahme zu der vorgeschlagenen Änderung mit.

4. Das Ministerkomitee prüft die vorgeschlagene Änderung und die Stellungnahme des Ausschusses der Vertragsparteien und kann die Änderung genehmigen.

[2] Vgl. Entscheidung der Delegierten (1252. Sitzung vom 30. März 2016, Punkt 10.1), mandat des CAHDATA CM(2016)28-final und das Dokument J(2016)r-rev2.

5. Der Wortlaut einer Änderung, die das Ministerkomitee nach Absatz 4 genehmigt hat, wird den Vertragsparteien zur Annahme zugeleitet.

6. Eine nach Absatz 4 genehmigte Änderung tritt am dreissigsten Tag nach dem Zeitpunkt in Kraft, zu dem alle Vertragsparteien dem Generalsekretär ihre Annahme mitgeteilt haben.

7. Das Ministerkomitee kann nach Beratung mit dem Ausschuss der Vertragsparteien beschliessen, dass eine bestimmte Änderung nach Ablauf von zwei Jahren nach dem Zeitpunkt in Kraft tritt, in dem es zur Annahme aufgelegt wurde, sofern nicht eine der Vertragsparteien dem Generalsekretär des Europarats einen Einwand gegen sein Inkrafttreten notifiziert hat. Wenn ein solcher Einwand notifiziert wurde, tritt die Änderung am ersten Tag des Monats nach dem Tag in Kraft, an dem die Vertragspartei, die den Einwand notifiziert hat, ihre Annahmeurkunde beim Generalsekretär des Europarats hinterlegt hat.

Kapitel VII – Schlussklauseln

Art. 22 – Inkrafttreten

1. Dieses Übereinkommen liegt für die Mitgliedstaaten des Europarats und der Europäischen Union zur Unterzeichnung auf. Es bedarf der Ratifikation, Annahme oder Genehmigung. Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden beim Generalsekretär des Europarats hinterlegt.

2. Dieses Übereinkommen tritt am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem fünf Mitgliedstaaten des Europarats nach Absatz 1 ihre Zustimmung ausgedrückt haben, durch das Übereinkommen gebunden zu sein.

3. Für jede Vertragspartei, die später ihre Zustimmung ausdrückt, durch das Übereinkommen gebunden zu sein, tritt es am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Hinterlegung der Ratifikations-, Annahme- oder Genehmigungsurkunde folgt.

Art. 23 – Beitritt von Nichtmitgliedstaaten oder internationalen Organisationen

1. Nach Inkrafttreten dieses Übereinkommens kann das Ministerkomitee des Europarats nach Konsultation der Vertragsparteien des Übereinkommens und mit deren einhelliger Zustimmung und im Lichte der Stellungnahme des Ausschusses der Vertragsparteien nach Artikel 19 Buchstabe e jeden Nichtmitgliedstaat des Rates oder eine internationale Organisation einladen, dem Übereinkommen beizutreten; die entsprechende Beschlussfassung erfolgt mit der in Artikel 20 Buchstabe d der Satzung vorgesehenen Mehrheit und mit einhelliger Zustimmung der Vertreter der Vertragsstaaten, die Anspruch auf einen Sitz im Ministerkomitee haben.

2. Für jeden Staat oder jede internationale Organisation, die diesem Übereinkommen nach Massgabe von Absatz 1 beitreten, tritt das Übereinkommen am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Hinterlegen der Beitrittsurkunde beim Generalsekretär des Europarats folgt.

Art. 24 – Räumlicher Geltungsbereich

1. Jeder Staat, die Europäische Union oder eine andere internationale Organisation können bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde einzelne oder mehrere Hoheitsgebiete bezeichnen, auf die dieses Übereinkommen Anwendung findet.

2. Jeder Staat, die Europäische Union oder eine andere internationale Organisation können jederzeit danach durch eine an den Generalsekretär des Europarats gerichtete Erklärung die Anwendung dieses Übereinkommens auf jedes weitere in der Erklärung bezeichnete Hoheitsgebiet erstrecken. Das Übereinkommen tritt für dieses Hoheitsgebiet am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Erklärung beim Generalsekretär folgt.

3. Jede nach den Absätzen 1 und 2 abgegebene Erklärung kann in Bezug auf jedes darin bezeichnete Hoheitsgebiet durch eine an den Generalsekretär des Europarats gerichtete Notifikation zurückgenommen werden. Die Zurücknahme wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von sechs Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

Art. 25 – Vorbehalte

Vorbehalte zu diesem Übereinkommen sind nicht zulässig.

Art. 26 – Kündigung

1. Jede Vertragspartei kann dieses Übereinkommen jederzeit durch eine an den Generalsekretär des Europarats gerichtete Notifikation kündigen.

2. Die Kündigung wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von sechs Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

Art. 27 – Notifikationen

Der Generalsekretär des Europarats notifiziert den Mitgliedstaaten des Rates und jedem Staat, der diesem Übereinkommen beigetreten ist:

a. jede Unterzeichnung;

b. jede Hinterlegung einer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde;

c. jeden Zeitpunkt des Inkrafttretens dieses Übereinkommens nach den Artikeln 22, 23 und 24;

d. jede andere Handlung, Notifikation oder Mitteilung im Zusammenhang mit diesem Übereinkommen.

Art. … des Protokolls: Unterzeichnung und Inkrafttreten

1. Dieses Protokoll liegt für alle Vertragsparteien des Übereinkommens zur Unterzeichnung auf. Es bedarf der Ratifikation, Annahme oder Genehmigung. Ratifikations-, Annahme- bzw. Genehmigungsurkunden werden beim Generalsekretär des Europarats hinterlegt.

2. Dieses Protokoll tritt am ersten Tag des Monats in Kraft, der auf eine Frist von [drei] Monaten nach dem Tag folgt, an dem alle Vertragsparteien des Übereinkommens sich gemäss den Bestimmungen von Absatz 1 als an das Protokoll gebunden erklärt haben.

3. Dieses Protokoll jedoch tritt nach Ablauf von [zwei] Jahren nach dem Zeitpunkt in Kraft, zu dem es zur Unterzeichnung aufgelegt wurde, sofern nicht eine der Vertragsparteien dem Generalsekretär des Europarats einen Einwand gegen sein Inkrafttreten notifiziert hat. Das Recht, einen Einwand zu erheben, ist den Staaten vorbehalten, die am Tag der Auflegung dieses Protokolls zur Unterzeichnung Vertragsparteien des Übereinkommens waren.

4. Wenn ein solcher Einwand notifiziert wurde, tritt das Protokoll am ersten Tag des Monats nach Ablauf von [drei] Monaten nach dem Zeitpunkt in Kraft, an dem die Vertragspartei, die den Einwand notifiziert hat, ihre Ratifikations-, Annahme- bzw. Genehmigungsurkunden beim Generalsekretär des Europarats hinterlegt.

5. Bei Inkrafttreten dieses Protokolls werden allfällige auf der Grundlage von Artikel 3 des ursprünglichen Übereinkommens abgegebene Erklärungen der Vertragsparteien hinfällig.

EU-Richtlinie 2016/680 EU Datenschutz

RICHTLINIEN

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/JI des Rates

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16 Absatz 2,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Ausschusses der Regionen ([1]),

gemäß dem ordentlichen Gesetzgebungsverfahren, ([2])

in Erwägung nachstehender Gründe:

(1) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Richtlinie soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts beitragen.

(3) Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass für die Ausübung von Tätigkeiten wie die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung in einem noch nie dagewesenen Umfang personenbezogene Daten verarbeitet werden können.

(4) Der freie Verkehr personenbezogener Daten zwischen den zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit innerhalb der Union und die Übermittlung solcher personenbezogener Daten an Drittländer und internationale Organisationen, sollte erleichtert und dabei gleichzeitig ein hohes Schutzniveau für personenbezogene Daten gewährleistet werden. Angesichts dieser Entwicklungen bedarf es des Aufbaus eines soliden und kohärenteren Rechtsrahmens für den Schutz personenbezogener Daten in der Union, die konsequent durchgesetzt werden.

(5) Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ([3]) gilt für jegliche Verarbeitung personenbezogener Daten in den Mitgliedstaaten sowohl im öffentlichen als auch im privaten Bereich. Ausgenommen ist jedoch die Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit.

([1]) ABl. C 391, 18.12.2012, S. 127.
([2]) Standpunkt des Europäischen Parlamentes vom 12. März 2014 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 8. April 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlamentes vom 14. April 2016.
([3]) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

(6) Für den Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit gilt der Rahmenbeschluss 2008/977/JI des Rates ([1]). Der Anwendungsbereich dieses Rahmenbeschlusses beschränkt sich auf die Verarbeitung personenbezogener Daten, die zwischen Mitgliedstaaten weitergegeben oder bereitgestellt werden.

(7) Für den Zweck der wirksamen justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit ist es entscheidend, ein einheitliches und hohes Schutzniveau für die personenbezogenen Daten natürlicher Personen zu gewährleisten und den Austausch personenbezogener Daten zwischen den zuständigen Behörden der Mitgliedstaaten zu erleichtern. Im Hinblick darauf sollte dafür gesorgt werden, dass die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, in allen Mitgliedstaaten gleichwertig geschützt werden. Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung der Rechte der betroffenen Personen und eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten, und auch gleichwertige Befugnisse der Mitgliedstaaten bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten.

(8) Artikel 16 Absatz 2 AEUV ermächtigt das Europäische Parlament und den Rat, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr personenbezogener Daten zu erlassen.

(9) Auf dieser Grundlage sind in der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([2]) allgemeine Bestimmungen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr personenbezogener Daten in der Union niedergelegt.

(10) In der Erklärung Nr. 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang zur Schlussakte der Regierungskonferenz, die den Vertrag von Lissabon annahm, erkannte die Regierungskonferenz an, dass es sich aufgrund der Besonderheiten dieser Bereiche als erforderlich erweisen könnte, auf Artikel 16 AEUV gestützte spezifische Vorschriften über den Schutz personenbezogener Daten und den freien Verkehr personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit zu erlassen.

(11) Daher sollte diesen Bereichen durch eine Richtlinie Rechnung getragen werden, die spezifische Vorschriften 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, enthält, wobei den Besonderheiten dieser Tätigkeiten Rechnung getragen wird. Diese zuständigen Behörden können nicht nur staatliche Stellen wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden einschließen, sondern auch alle anderen Stellen oder Einrichtungen, denen durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke dieser Richtlinie übertragen wurde. Wenn solche Stellen oder Einrichtungen jedoch personenbezogene Daten zu anderen Zwecken als denen dieser Richtlinie verarbeiten, gilt die Verordnung (EU) 2016/679. Daher gilt die Verordnung (EU) 2016/679 in Fällen, in denen eine Stelle oder Einrichtung personenbezogene Daten zu anderen Zwecken erhebt und diese personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der sie unterliegt, weiterverarbeitet. Zum Beispiel speichern Finanzinstitute zum Zwecke der Ermittlung, Aufdeckung oder Verfolgung von Straftaten bestimmte personenbezogene Daten, die sie verarbeiten, und stellen sie nur den zuständigen nationalen Behörden in bestimmten Fällen und in Einklang mit dem Recht der Mitgliedstaaten zur Verfügung. Eine Stelle oder Einrichtung, die personenbezogene Daten im Rahmen des Anwendungsbereichs dieser Richtlinie für solche Behörden verarbeitet, sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments und durch die für Auftragsverarbeiter nach dieser Richtlinie geltenden Bestimmungen gebunden sein, wobei die Anwendung der Verordnung (EU) 2016/679 in Bezug auf die Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter außerhalb des Anwendungsbereichs dieser Richtlinie durchführt, unberührt bleibt.

(12) Die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden sind hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet, dazu zählen auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht. Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen. Sie umfassen auch die Aufrechterhaltung der öffentlichen Ordnung als Aufgabe, die der Polizei oder anderen Strafverfolgungsbehörden übertragen wurde, soweit dies zum Zweck des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen

([1]) Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60).

([2]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Ersetzung von Richtlinie 95/46/EC (Datenschutz-Grundverordnung) (Siehe Seite 1 dieses Amtsblatts).

Sicherheit und Bedrohungen für durch Rechtsvorschriften geschützte grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist. Die Mitgliedstaaten können die zuständigen Behörden mit anderen Aufgaben betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt, als sie in den Anwendungsbereich des Unionsrechts fällt.

(13) Eine Straftat im Sinne dieser Richtlinie sollte ein eigenständiger Begriff des Unionsrechts in der Auslegung durch den Gerichtshof der Europäischen Union (im Folgenden „Gerichtshof") sein.

(14) Da diese Richtlinie nicht für die Verarbeitung personenbezogener Daten gelten sollte, die im Rahmen einer nicht unter das Unionsrecht fallenden Tätigkeit erfolgt, sollten die nationale Sicherheit betreffende Tätigkeiten, Tätigkeiten von Agenturen oder Stellen, die mit Fragen der nationalen Sicherheit befasst sind, und die Verarbeitung personenbezogener Daten, die von den Mitgliedstaaten bei Tätigkeiten vorgenommen wird, die in den Anwendungsbereich des Titels V Kapitel 2 des Vertrags über die Europäische Union (EUV) fallen, nicht als Tätigkeiten betrachtet werden, die in den Anwendungsbereich dieser Richtlinie fallen.

(15) Um zu gewährleisten, dass natürliche Personen in der Union auf der Grundlage unionsweit durchsetzbarer Rechte das gleiche Maß an Schutz genießen und Unterschiede, die den Austausch personenbezogener Daten zwischen den zuständigen Behörden behindern könnten, beseitigt werden, sollte diese Richtlinie harmonisierte Vorschriften für den Schutz und den freien Verkehr personenbezogener Daten festlegen, die zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, verarbeitet werden. Die Angleichung der Rechtsvorschriften der Mitgliedstaaten sollte nicht zu einer Lockerung des Schutzes personenbezogener Daten in diesen Ländern führen, sondern vielmehr auf ein hohes Schutzniveau in der gesamten Union abstellen. Die Mitgliedstaaten sollten nicht daran gehindert werden, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie.

(16) Diese Richtlinie berührt nicht den Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten. Gemäß der Verordnung (EU) 2016/679 können personenbezogene Daten in amtlichen Dokumenten, die sich im Besitz einer öffentlichen Behörde oder einer öffentlichen oder privaten Einrichtung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe befinden, von der Behörde oder der Einrichtung gemäß dem Unionsrecht oder dem Recht des Mitgliedstaats, dem die öffentliche Behörde oder Einrichtung unterliegt, offengelegt werden, um den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten in Einklang zu bringen.

(17) Der durch diese Richtlinie gewährte Schutz sollte für die Verarbeitung der personenbezogenen Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gelten.

(18) Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen. Er sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten nicht in den Anwendungsbereich der Richtlinie fallen.

(19) Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates [1] gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, sollten an die Grundsätze und Vorschriften gemäß der Verordnung (EU) 2016/679 angepasst werden.

(20) Diese Richtlinie hindert die Mitgliedstaaten nicht daran, in den nationalen Vorschriften für Strafverfahren Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden festzulegen, insbesondere in Bezug auf personenbezogene Daten in einer gerichtlichen Entscheidung oder in Dokumenten betreffend Strafverfahren.

[1] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

(21) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologischen Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann.

(22) Behörden, gegenüber denen personenbezogene Daten aufgrund einer rechtlichen Verpflichtung für die Ausübung ihres offiziellen Auftrags offengelegt werden, wie Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden, die für die Regulierung und Aufsicht von Wertpapiermärkten zuständig sind, sollten nicht als Empfänger gelten, wenn sie personenbezogene Daten erhalten, die für die Durchführung — gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten — eines einzelnen Untersuchungsauftrags im Interesse der Allgemeinheit erforderlich sind. Anträge auf Offenlegung, die von Behörden ausgehen, sollten immer schriftlich erfolgen, mit Gründen versehen sein und gelegentlichen Charakter haben, und sie sollten nicht vollständige Dateisysteme betreffen oder zur Verknüpfung von Dateisystemen führen. Die Verarbeitung personenbezogener Daten durch die genannten Behörden sollte für die Zwecke der Verarbeitung geltenden Datenschutzvorschriften entsprechen.

(23) Genetische Daten sollten als personenbezogene Daten über die ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person definiert werden, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und die aus der Analyse einer biologischen Probe der betreffenden natürlichen Person, insbesondere durch eine Chromosomen-, Desoxyribonukleinsäure (DNS)- oder Ribonukleinsäure (RNS)-Analyse oder der Analyse eines anderen Elements, durch die gleichwertige Informationen erlangt werden können, gewonnen werden. Angesichts der Komplexität und Sensibilität genetischer Informationen besteht ein hohes Missbrauchs- und Wiederverwendungsrisiko für unterschiedliche Zwecke durch den Verantwortlichen. Jede Diskriminierung aufgrund genetischer Merkmale sollte grundsätzlich verboten sein.

(24) Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Vormerkung zur Erbringung und der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ([1]) erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, einschließlich genetischer Daten und biologischer Proben, abgeleitet wurden, sowie Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.

(25) Alle Mitgliedstaaten sind Mitglied der Internationalen Kriminalpolizeilichen Organisation (Interpol). Interpol erhält, speichert und übermittelt für die Erfüllung ihres Auftrags personenbezogene Daten, um die zuständigen Behörden dabei zu unterstützen, internationale Kriminalität zu verhüten und zu bekämpfen. Daher sollte die Zusammenarbeit zwischen der Union und Interpol gestärkt werden, indem ein effizienter Austausch personenbezogener Daten gefördert und zugleich die Achtung der Grundrechte und Grundfreiheiten hinsichtlich der automatischen Verarbeitung personenbezogener Daten gewährleistet wird. Wenn personenbezogene Daten aus der Union an Interpol und die Staaten, die Mitglieder zu Interpol abgestellt haben, übermittelt werden, sollte diese Richtlinie, insbesondere die Bestimmungen über grenzüberschreitende Datenübermittlungen, zur Anwendung kommen. Diese Richtlinie sollte die spezifischen Vorschriften unberührt lassen, die im Gemeinsamen Standpunkt 2005/69/JI des Rates ([2]) und im Beschluss 2007/533/JI des Rates ([3]) festgelegt sind.

(26) Jede Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffenen natürlichen Personen nachvollziehbaren Weise erfolgen, und die Daten dürfen nur für bestimmte, durch Rechtsvorschriften geregelte Zwecke verarbeitet werden. Dies steht an sich der

([1]) Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).

([2]) Gemeinsamer Standpunkt 2005/69/JI des Rates vom 24. Januar 2005 zum Austausch bestimmter Daten mit Interpol (ABl. L 27 vom 29.1.2005, S. 61).

([3]) Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 205 vom 7.8.2007, S. 63).

Durchführung von Maßnahmen wie verdeckten Ermittlungen oder Videoüberwachung durch die Strafverfolgungsbehörden nicht entgegen. Diese Maßnahmen können zwecks Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, getroffen werden, sofern sie durch Rechtsvorschriften geregelt sind und eine erforderliche und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellen, bei der die berechtigten Interessen der betroffenen natürlichen Person gebührend berücksichtigt werden. Der Datenschutzgrundsatz der Verarbeitung nach Treu und Glauben ist ein anderes Konzept als das Recht auf ein faires Verfahren im Sinne des Artikels 47 der Charta und des Artikels 6 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK). Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogene Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt deren Erhebung feststehen. Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sein. Es sollte insbesondere sichergestellt werden, dass nicht übermäßige personenbezogene Daten erhoben werden und sie nicht länger aufbewahrt werden, als dies für den Zweck, zu dem sie verarbeitet werden, erforderlich ist. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Die Mitgliedstaaten sollten geeignete Garantien für den Fall festlegen, dass personenbezogene Daten für die Archivierung im öffentlichen Interesse und die wissenschaftliche, statistische oder historische Verwendung für längere Zeiträume gespeichert werden.

(27) Zur Verhütung, Ermittlung und Verfolgung von Straftaten müssen die zuständigen Behörden personenbezogene Daten, die im Zusammenhang mit der Verhütung, Ermittlung, Aufdeckung oder Verfolgung einer bestimmten Straftat erhoben wurden, auch in einem anderen Kontext verarbeiten können, um sich ein Bild von den kriminellen Handlungen machen und Verbindungen zwischen verschiedenen aufgedeckten Straftaten herstellen zu können.

(28) Um stets eine sichere Verarbeitung zu gewährleisten und Verarbeitungen, die gegen diese Richtlinie verstoßen, zu verhindern, sollten personenbezogene Daten so verarbeitet werden, dass ein Maß an Sicherheit und Vertraulichkeit gegeben ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können, und dass die Verarbeitung den Stand der verfügbaren Technik, die Kosten für ihre Einführung im Verhältnis zu den von der Verarbeitung ausgehenden Risiken und die Art der zu schützenden personenbezogenen Daten berücksichtigt.

(29) Personenbezogene Daten sollten für festgelegte, eindeutige und rechtmäßige Zwecke innerhalb des Anwendungsbereichs dieser Richtlinie erhoben und nicht zu Zwecken verarbeitet werden, die nicht mit den Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zu vereinbaren sind. Werden personenbezogene Daten von demselben oder einem anderen Verantwortlichen für einen anderen in den Anwendungsbereich dieser Richtlinie fallenden Zweck als den, für den sie erhoben wurden, verarbeitet, so sollte diese Verarbeitung erlaubt sein, unter der Bedingung, dass diese Verarbeitung nach den geltenden Rechtsvorschriften zulässig ist und dass sie für diesen anderen Zweck erforderlich und verhältnismäßig ist.

(30) Der Grundsatz der sachlichen Richtigkeit der Daten sollte unter Berücksichtigung von Art und Zweck der jeweiligen Verarbeitung angewandt werden. Aussagen, die personenbezogene Daten enthalten, basieren gerade in Gerichtsverfahren auf der subjektiven Wahrnehmung von natürlichen Personen und sind nicht immer nachprüfbar. Infolgedessen sollte sich der Grundsatz der sachlichen Richtigkeit nicht auf die Richtigkeit einer Aussage beziehen, sondern lediglich auf die Tatsache, dass eine bestimmte Aussage gemacht worden ist.

(31) Bei der Verarbeitung personenbezogener Daten im Rahmen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit geht es naturgemäß um betroffene Personen verschiedener Kategorien. Daher sollte gegebenenfalls und so weit wie möglich klar zwischen den personenbezogenen Daten der einzelnen Kategorien betroffener Personen unterschieden werden wie Verdächtige, verurteilte Straftäter, Opfer und andere Parteien, beispielsweise Zeugen, Personen, die über einschlägige Informationen verfügen, oder Personen, die mit Verdächtigen oder verurteilten Straftätern in Kontakt oder in Verbindung stehen. Dies sollte nicht der Anwendung des Rechts auf die Unschuldsvermutung, wie es in der Charta und in der EMRK gewährleistet ist, in der Auslegung durch die Rechtsprechung des Gerichtshofs bzw. des Europäischen Gerichtshofs für Menschenrechte entgegenstehen.

(32) Die zuständigen Behörden sollten dafür sorgen, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Um den Schutz natürlicher Personen, die Richtigkeit, die Vollständigkeit oder den Aktualitätsgrad sowie die Zuverlässigkeit der übermittelten oder bereitgestellten personenbezogenen Daten zu gewährleisten, sollten die zuständigen Behörden möglichst bei allen Übermittlungen personenbezogener Daten die erforderlichen Informationen beifügen.

(33) Wenn in dieser Richtlinie auf Recht der Mitgliedstaaten, eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, erfordert dies nicht notwendigerweise einen von einem Parlament angenommenen

Gesetzgebungsakt, wobei Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats unberührt bleiben. Recht der Mitgliedstaaten, Rechtsgrundlagen oder Gesetzgebungsmaßnahmen sollten jedoch klar und präzise sein und ihre Anwendung sollte für diejenigen, die ihnen unterliegen, vorhersehbar sein, wie in der Rechtsprechung des Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte gefordert. Im Recht der Mitgliedstaaten, das die Verarbeitung personenbezogener Daten innerhalb des Anwendungsbereichs dieser Richtlinie regelt, sollten zumindest die Ziele, die zu verarbeitenden personenbezogenen Daten, die Zwecke der Verarbeitung sowie Verfahren zur Wahrung von Integrität und Vertraulichkeit der personenbezogenen Daten und Verfahren für ihre Vernichtung angegeben werden, um hinreichende Garantien gegen die Gefahr des Missbrauchs und der Willkür zu bieten.

(34) Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sollte jeden mit Hilfe automatisierter Verfahren oder auf anderem Wege ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, den Abgleich oder die Verknüpfung, die Einschränkung der Verarbeitung, das Löschen oder die Vernichtung abdecken. Insbesondere sollte diese Richtlinie Anwendung finden, wenn personenbezogene Daten für die Zwecke dieser Richtlinie an einen Empfänger übermittelt werden, der nicht dieser Richtlinie unterliegt. Unter einem solchen Empfänger sollte eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle zu verstehen sein, gegenüber der personenbezogene Daten von der zuständigen Behörde rechtmäßig offengelegt werden. Wurden personenbezogene Daten ursprünglich von einer zuständigen Behörde für einen der Zwecke dieser Richtlinie erhoben, so sollte die Verordnung (EU) 2016/679 für die Verarbeitung dieser Daten für andere Zwecke als diejenigen dieser Richtlinie gelten, wenn eine solche Verarbeitung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist. Insbesondere sollte die Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten für Zwecke gelten, die außerhalb des Anwendungsbereichs dieser Richtlinie liegen. Für die Verarbeitung personenbezogener Daten durch einen Empfänger, der keine zuständige Behörde im Sinne dieser Richtlinie ist oder nicht als solche handelt und gegenüber dem personenbezogene Daten von einer zuständigen Behörde rechtmäßig offengelegt werden, sollte die Verordnung (EU) 2016/679 gelten. Bei der Umsetzung dieser Richtlinie sollten die Mitgliedstaaten außerdem, die Anwendung der Vorschriften der Verordnung (EU) 2016/679 — vorbehaltlich der darin genannten Bedingungen — genauer regeln können.

(35) Die Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie sollte nur dann als rechtmäßig gelten, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die eine zuständige Behörde im öffentlichen Interesse auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausführt. Diese Tätigkeiten sollten sich auf die Wahrung lebenswichtiger Interessen der betroffenen Person erstrecken. Bei der Wahrnehmung der ihnen als gesetzlich begründeter Institution übertragenen Aufgaben, Straftaten zu verhüten, zu ermitteln, aufzudecken und zu verfolgen, können die zuständigen Behörden natürliche Personen auffordern oder anweisen, ihren Anordnungen nachzukommen. In einem solchen Fall sollte die Einwilligung der betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen. Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann. Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung.

(36) Die Mitgliedstaaten sollten vorsehen, dass immer dann, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem die übermittelnde zuständige Behörde unterliegt, für die Verarbeitung von personenbezogenen Daten unter bestimmten Umständen besondere Bedingungen, etwa zur Verwendung von Bearbeitungscodes, gelten, die übermittelnde zuständige Behörde den Empfänger der personenbezogenen Daten auf diese Bedingungen und die Verpflichtung sie einzuhalten hinweisen sollte. Hierzu könnte beispielsweise das Verbot, personenbezogene Daten an andere weiter zu übermitteln, oder das Verbot, sie für andere Zwecke, als die Zwecke zu denen sie an den Empfänger übermittelt wurden, zu verwenden, oder das Verbot, die betroffene Person im Falle der Einschränkung des Rechts auf Unterrichtung ohne vorheriger Genehmigung der übermittelnden zuständigen Behörde zu informieren, zählen. Diese Pflichten gelten auch für Übermittlungen durch die übermittelnde zuständige Behörde an Empfänger in Drittländern oder an internationale Organisationen. Die Mitgliedstaaten sollten sicherstellen, dass die übermittelnde zuständige Behörde auf Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel 4 und 5 AEUV errichtete Einrichtungen und sonstige Stellen nur solche Bedingungen anwendet, die auch für entsprechende Datenübermittlungen innerhalb ihres eigenen Mitgliedstaats gelten.

(37) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche

Risiken für die Grundrechte und Grundfreiheiten auftreten können. Diese personenbezogenen Daten sollten personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft hervorgeht, wobei die Verwendung des Begriffs „rassische Herkunft" in dieser Richtlinie nicht bedeutet, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Solche personenbezogenen Daten sollten nur dann verarbeitet werden, wenn die Verarbeitung vorbehaltlich geeigneter Garantien für die durch Rechtsvorschriften festgelegten Rechte und Freiheiten der betroffenen Person erfolgt und in durch Rechtsvorschriften geregelten Fällen erlaubt ist oder anderenfalls zur Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist oder aber sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat. Zu den geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person kann beispielsweise zählen, dass diese Daten nur in Verbindung mit anderen Daten über die betroffene natürliche Person erhoben werden dürfen, die erhobenen Daten hinreichend gesichert werden müssen, der Zugang der Mitarbeiter der zuständigen Behörde zu den Daten strenger geregelt und die Übermittlung dieser Daten verboten wird. Die Verarbeitung solcher Daten sollte ebenfalls durch Rechtsvorschriften erlaubt sein, wenn die betroffene Person der Datenverarbeitung, die besonders stark in ihre Privatsphäre eingreift, ausdrücklich zugestimmt hat. Die Einwilligung der betroffenen Person allein sollte jedoch noch keine rechtliche Grundlage für die Verarbeitung solch sensibler personenbezogener Daten durch die zuständigen Behörden liefern.

(38) Die betroffene Person sollte das Recht haben, keiner Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die nachteilige rechtliche Wirkung für sie entfaltet oder sie in erheblichem Maße beeinträchtigt. In jedem Fall sollte eine solche Verarbeitung mit geeigneten Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Rechts, das Eingreifen einer Person zu erwirken, insbesondere auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung oder auf Anfechtung der Entscheidung. Ein Profiling, das zur Folge hat, dass natürliche Personen aufgrund von personenbezogenen Daten diskriminiert werden, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, sollte gemäß den Bestimmungen der Artikel 21 und 52 der Charta verboten werden.

(39) Damit die betroffene Person ihre Rechte wahrnehmen kann, sollten alle Informationen für sie leicht zugänglich — auch auf der Website des Verantwortlichen — und verständlich, also in klarer und einfacher Sprache abgefasst sein. Diese Informationen sollten an die Bedürfnisse von schutzbedürftigen Personen, wie etwa Kindern, angepasst werden.

(40) Es sollten Modalitäten festgelegt werden, die einer betroffenen Person die Ausübung ihrer Rechte aufgrund der nach dieser Richtlinie erlassenen Vorschriften erleichtern, darunter auch Mechanismen, die dafür sorgen, dass sie unentgeltlich insbesondere Zugang zu personenbezogenen Daten und deren Berichtigung oder Löschung beantragen und gegebenenfalls erhalten oder von ihrem Widerspruchsrecht Gebrauch machen kann. Der Verantwortliche sollte verpflichtet werden, den Antrag der betroffenen Person unverzüglich zu beantworten, es sei denn, er wendet Einschränkungen in Bezug auf die Rechte der betroffenen Person gemäß dieser Richtlinie an. Bei offenkundig unbegründeten oder exzessiven Anträgen, zum Beispiel wenn die betroffene Person ungebührlich und wiederholt Informationen verlangt oder wenn die betroffene Person ihr Recht auf Unterrichtung missbraucht, beispielsweise indem sie in ihrem Antrag falsche oder irreführende Angaben macht, sollte der Verantwortliche, eine angemessene Gebühr erheben können oder sich weigern können, aufgrund des Antrags tätig zu werden.

(41) Fordert der Verantwortliche zusätzliche Informationen an, die zur Bestätigung der Identität der betroffenen Person erforderlich sind, so sollten diese Informationen nur für diesen konkreten Zweck verarbeitet werden und nicht länger gespeichert werden, als es für diesen Zweck notwendig ist.

(42) Der betroffenen Person sollten zumindest folgende Informationen zur Verfügung gestellt werden: die Identität des Verantwortlichen, die Existenz des Verarbeitungsvorgangs, die Zwecke der Verarbeitung, das Beschwerderecht und das Bestehen eines Rechts auf Auskunft und Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung durch den Verantwortlichen. Dies könnte auf der Website der zuständigen Behörde erfolgen. Außerdem sollte die betroffene Person in bestimmten Fällen und zur Ermöglichung der Ausübung ihrer Rechte über die Rechtsgrundlage der Verarbeitung und die Speicherfrist informiert werden, soweit diese zusätzlichen Informationen unter Berücksichtigung der spezifischen Umstände, unter denen die Daten verarbeitet werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

(43) Eine natürliche Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Jede betroffene Person sollte daher das Recht haben, zu wissen und zu erfahren, zu welchen Zwecken die Daten verarbeitet werden, wie lange sie verarbeitet werden und wer deren Empfänger, einschließlich solcher in Drittländern, sind. Enthalten solche Mitteilungen Informationen über den Ursprung der personenbezogenen Daten, so sollten die Informationen nicht die Identität natürlicher Personen und insbesondere keine vertraulichen Quellen preisgeben. Damit diesem Recht entsprochen wird, braucht die betroffene Person lediglich im Besitz einer vollständigen Übersicht über diese Daten in verständlicher Form zu sein, d. h. in einer Form, die es ihr ermöglicht, sich dieser Daten bewusst zu werden und nachzuprüfen, ob sie richtig sind und im Einklang mit dieser Richtlinie verarbeitet werden, so dass

sie die ihr durch diese Richtlinie verliehenen Rechte ausüben kann. Eine solche Übersicht könnte in Form einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, bereitgestellt werden.

(44) Die Mitgliedstaaten sollten Gesetzgebungsmaßnahmen erlassen können, mit denen die Unterrichtung der betroffenen Person aufgeschoben, eingeschränkt oder unterlassen oder die Auskunft über ihre personenbezogenen Daten ganz oder teilweise in dem Umfang und so lange eingeschränkt wird, wie dies in einer demokratischen Gesellschaft unter gebührender Berücksichtigung der Grundrechte und der berechtigten Interessen der betroffenen natürlichen Person eine erforderliche und verhältnismäßige Maßnahme darstellt, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und um die öffentliche und die nationale Sicherheit oder die Rechte und Freiheiten anderer zu schützen. Der Verantwortliche sollte im Wege einer konkreten Einzelfallprüfung feststellen, ob das Auskunftsrecht teilweise oder vollständig eingeschränkt werden sollte.

(45) Eine Verweigerung oder Einschränkung der Auskunft sollte der betroffenen Person grundsätzlich unter Angabe der sachlichen oder rechtlichen Gründe hierfür schriftlich mitgeteilt werden.

(46) Jede Einschränkung der Rechte der betroffenen Person muss mit der Charta und mit der EMRK in der Auslegung durch die Rechtsprechung des Gerichtshofs bzw. des Europäischen Gerichtshofs für Menschenrechte vereinbar sein und insbesondere den Wesensgehalt dieser Rechte und Freiheiten achten.

(47) Eine natürliche Person sollte das Recht auf Berichtigung sie betreffender unrichtiger personenbezogener Daten, insbesondere bei Bezug auf Tatsachen, sowie das Recht auf Löschung besitzen, wenn die Datenverarbeitung gegen diese Richtlinie verstößt. Das Recht auf Berichtigung sollte allerdings beispielsweise nicht den Inhalt einer Zeugenaussage berühren. Eine natürliche Person sollte auch das Recht auf Einschränkung der Verarbeitung besitzen, wenn sie die Richtigkeit personenbezogener Daten bestreitet und deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann oder wenn die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden müssen. Insbesondere sollte statt der Löschung personenbezogener Daten die Verarbeitung eingeschränkt werden, wenn in einem konkreten Fall berechtigter Grund zu der Annahme besteht, dass eine Löschung die berechtigten Interessen der betroffenen Person beeinträchtigen könnte. In einem solchen Fall sollten Daten mit Einschränkungsmarkierung nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand. Methoden zur Einschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte Daten, beispielsweise zu Archivierungszwecken, auf ein anderes Verarbeitungssystem übertragen oder gesperrt werden. In automatisierten Dateisystemen sollte die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel erfolgen. Auf die Tatsache, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde, sollte in dem System unmissverständlich hingewiesen werden. Entsprechende Berichtigungen oder Löschungen personenbezogener Daten oder Einschränkungen der Verarbeitung sollten den Empfängern, gegenüber dem die personenbezogenen Daten offengelegt wurden, und den zuständigen Behörden, von denen die unrichtigen Daten stammen, mitgeteilt werden. Der Verantwortliche sollte auch von jeglicher Weiterverbreitung dieser Daten Abstand nehmen.

(48) Verweigert ein Verantwortlicher einer betroffenen Person ihr Recht auf Unterrichtung, Auskunft, Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung, so sollte die betroffene Person die nationale Aufsichtsbehörde ersuchen können, die Rechtmäßigkeit der Verarbeitung zu überprüfen. Die betroffene Person sollte über dieses Recht unterrichtet werden. Handelt die Aufsichtsbehörde im Namen der betroffenen Person, so sollte sie die betroffene Person zumindest darüber informieren, dass alle erforderlichen Prüfungen oder Überprüfungen durchgeführt wurden. Die Aufsichtsbehörde sollte die betroffene Person zudem über ihr Recht auf gerichtlichen Rechtsbehelf in Kenntnis setzen.

(49) Werden personenbezogene Daten im Zusammenhang mit strafrechtlichen Ermittlungen und Gerichtsverfahren in Strafsachen verarbeitet, so sollten die Mitgliedstaaten vorsehen können, dass die Ausübung des Rechts auf Unterrichtung, Auskunft, Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung nach Maßgabe des einzelstaatlichen Strafverfahrensrechts erfolgt.

(50) Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Richtlinie stehen. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Im Rahmen der von ihm ergriffenen Maßnahmen sollte der Verantwortliche auch spezifische Garantien für die Verarbeitung personenbezogener Daten von schutzbedürftigen natürlichen Personen, wie etwa Kindern, ausarbeiten und implementieren.

(51) Risiken für die Rechte und Freiheiten der natürlichen Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Datenverarbeitung hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten, der unbefugten Umkehr der Pseudonymisierung oder anderen

erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, die Religion oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, wenn genetische Daten oder biometrische Daten zur eindeutigen Identifizierung einer Person oder Daten über die Gesundheit oder Daten über das Sexualleben und sexuelle Orientierung oder über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert und prognostiziert werden, um ein persönliches Profil zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von Personen betrifft.

(52) Eintrittswahrscheinlichkeit und Schwere des Risikos sollten nach der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein hohes Risiko birgt. Ein hohes Risiko ist ein besonderes Risiko der Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen.

(53) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Richtlinie erfüllt werden. Die Umsetzung dieser Maßnahmen sollte nicht ausschließlich von wirtschaftlichen Erwägungen abhängig gemacht werden. Um die Einhaltung dieser Richtlinie nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Genüge tun. Hat der Verantwortliche eine Datenschutz-Folgenabschätzung gemäß dieser Richtlinie vorgenommen, sollten die entsprechenden Ergebnisse bei der Entwicklung dieser Maßnahmen und Verfahren berücksichtigt werden. Die Maßnahmen könnten u. a. aus einer möglichst frühen Pseudonymisierung bestehen. Gerade durch die Pseudonymisierung für die Zwecke dieser Richtlinie könnte der freie Verkehr personenbezogener Daten im Raum der Freiheit, der Sicherheit und des Rechts erleichtert werden.

(54) Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es — auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden — einer klaren Zuteilung der Verantwortlichkeiten gemäß dieser Richtlinie, einschließlich der Fälle, in denen ein Verantwortlicher die Verarbeitungszwecke und -mittel gemeinsam mit anderen Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines Verantwortlichen durchgeführt wird.

(55) Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf der Grundlage eines Rechtsinstruments einschließlich eines Vertrags erfolgen, der den Auftragsverarbeiter an den Verantwortlichen bindet und in dem insbesondere vorgesehen ist, dass der Auftragsverarbeiter nur auf Weisung des Verantwortlichen handeln sollte. Der Auftragsverarbeiter sollte den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigen.

(56) Zum Nachweis der Einhaltung dieser Richtlinie sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis aller Kategorien von Tätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage dieses Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieses Verzeichnisses kontrolliert werden können. Der Verantwortliche oder der Auftragsverarbeiter, der personenbezogene Daten in nicht automatisierten Verarbeitungssystemen verarbeitet, sollte über wirksame Methoden zum Nachweis der Rechtmäßigkeit der Verarbeitung, zur Ermöglichung der Eigenüberwachung und zur Sicherstellung der Integrität und Sicherheit der Daten, wie etwa Protokolle oder andere Formen von Verzeichnissen, verfügen.

(57) In automatisierten Verarbeitungssystemen werden zumindest über folgende Verarbeitungsvorgänge Protokolle geführt: Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlungen, Kombination oder Löschung. Die Identifizierung der Person, die personenbezogene Daten abgefragt oder offengelegt hat, sollte protokolliert werden und aus dieser Identifizierung sollt sich die Begründung für die Verarbeitungsvorgänge ableiten lassen. Die Protokolle sollten ausschließlich zum Zwecke der Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der Daten sowie für Strafverfahren verwendet werden. Die Eigenüberwachung umfasst auch interne Disziplinarverfahren der zuständigen Behörden.

(58) Eine Datenschutz-Folgenabschätzung, die sich insbesondere mit den Maßnahmen, Garantien und Verfahren befasst, die geplant sind den Schutz personenbezogener Daten zu gewährleisten und die die Einhaltung der Bestimmungen dieser Richtlinie nachweisen sollen, sollte durch den Verantwortlichen durchgeführt werden, wenn die Verarbeitungsvorgänge aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge haben. Datenschutz-Folgenabschätzungen sollten auf maßgebliche Systeme und Verfahren im Rahmen von Verarbeitungsvorgängen abstellen, nicht jedoch auf Einzelfälle.

(59) Um einen wirksamen Schutz der Rechte und Freiheiten der betroffenen Personen zu gewährleisten, sollte der Verantwortliche oder der Auftragsverarbeiter in bestimmten Fällen vor der Verarbeitung die Aufsichtsbehörde konsultieren.

(60) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Richtlinie verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Solche Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau — auch hinsichtlich der Vertraulichkeit — gewährleisten, das dem von der Verarbeitung ausgehenden Risiko und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Datenverarbeitung verbundenen Risiken berücksichtigt werden, wie etwa Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte. Der Verantwortliche und der Auftragsverarbeiter sollten sicherstellen, dass personenbezogene Daten nicht durch Unbefugte verarbeitet werden.

(61) Eine Verletzung des Schutzes personenbezogener Daten kann — wenn nicht rechtzeitig und angemessen reagiert wird — einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

(62) Natürliche Personen, sollten unverzüglich benachrichtigt werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, damit sie die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Die Benachrichtigung der betroffenen Person sollte stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müsste die betroffene Person sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder ähnliche Verletzungen des Schutzes von Daten zu treffen. In Ausnahmefällen könnte die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen natürlichen Person unterbleiben, wenn ein Aufschub oder eine Einschränkung dieser Benachrichtigung nicht ausreicht, um behördliche oder gerichtliche Untersuchungen, Ermittlungen und Verfahren nicht zu behindern, die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht zu gefährden und um die öffentliche und die nationale Sicherheit oder die Rechte und Freiheiten anderer zu schützen.

(63) Der Verantwortliche sollte eine Person benennen, die ihn dabei unterstützt, die interne Einhaltung der nach dieser Richtlinie erlassenen Vorschriften zu überwachen, es sei denn, ein Mitgliedstaat beschließt eine Ausnahmeregelung für Gerichte und andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit. Bei dieser Person kann es sich um ein Mitglied des vorhandenen Personals des Verantwortlichen handeln, das eine besondere Schulung auf dem Gebiet der Datenschutzvorschriften und der Datenschutzpraxis erhalten hat, um einschlägiges Fachwissen in diesem Bereich zu erwerben. Der Grad des erforderlichen Fachwissens sollte sich insbesondere nach der Art der durchgeführten Datenverarbeitung und des erforderlichen Schutzes für die von dem Verantwortlichen verarbeiteten personenbezogenen Daten richten. Die betreffende Person kann ihre Aufgabe auf Teilzeit- oder Vollzeitbasis wahrnehmen. Mehrere Verantwortliche können unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe gemeinsam einen Datenschutzbeauftragten bestellen, zum Beispiel im Falle einer gemeinsamen Nutzung von Ressourcen in zentralen Stellen. Die betreffende Person kann auch für verschiedene Positionen innerhalb der Struktur der jeweils Verantwortlichen benannt werden. Sie sollte den Verantwortlichen und die Beschäftigten, die personenbezogene Daten verarbeiten, unterstützen, indem sie diese Personen über die Einhaltung ihrer jeweiligen Datenschutzpflichten unterrichtet und berät. Diese Datenschutzbeauftragten sollten ihren Auftrag und ihre Aufgaben auf unabhängige Weise gemäß dem Recht der Mitgliedstaaten wahrnehmen können.

(64) Die Mitgliedstaaten sollten dafür sorgen, dass Daten nur dann an ein Drittland oder eine internationale Organisation übermittelt werden, wenn dies für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von

Straftaten oder für die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, notwendig ist und es sich bei dem Verantwortlichen in dem Drittland oder in der internationalen Organisation um eine zuständige Behörde im Sinne dieser Richtlinie handelt. Eine Übermittlung sollte nur durch zuständige Behörden vorgenommen werden, die als Verantwortliche agieren, es sei denn, Auftragsverarbeiter werden ausdrücklich beauftragt, im Namen der Verantwortlichen Übermittlungen vorzunehmen. Derartige Übermittlungen können erfolgen, wenn die Kommission beschlossen hat, dass das betreffende Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau gewährleistet, oder wenn geeignete Garantien bestehen oder wenn Ausnahmen für bestimmte Fälle gelten. Das durch diese Richtlinie unionsweit gewährleistete Schutzniveau für natürliche Personen sollte bei der Übermittlung personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn aus dem Drittland oder von der internationalen Organisation personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weiterübermittelt werden.

(65) Werden personenbezogene Daten von einem Mitgliedstaat an Drittländer oder internationale Organisationen übermittelt, so sollte die Übermittlung grundsätzlich erst dann erfolgen, wenn der Mitgliedstaat, von dem die Daten stammen, die Übermittlung genehmigt hat. Im Interesse einer wirksamen Zusammenarbeit bei der Verhütung, Ermittlung und Aufdeckung von Straftaten ist es erforderlich, dass im Falle einer Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats, die so unvermittelt eintritt, dass es unmöglich ist, rechtzeitig eine vorherige Genehmigung einzuholen, die zuständige Behörde die maßgeblichen personenbezogenen Daten ohne vorherige Genehmigung an das betreffende Drittland oder die betreffende internationale Organisation übermitteln können sollte. Die Mitgliedstaaten sollten vorsehen, dass Drittländern oder internationalen Organisationen etwaige besondere Bedingungen für die Übermittlung mitgeteilt werden. Die Weiterübermittlung personenbezogener Daten sollte der vorherigen Genehmigung durch die zuständige Behörde bedürfen, die die ursprüngliche Übermittlung durchgeführt hat. Bei der Entscheidung über einen Antrag auf die Genehmigung einer Weiterübermittlung sollte die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, alle maßgeblichen Faktoren gebührend berücksichtigen, einschließlich der Schwere der Straftat, der spezifischen Auflagen und des Zwecks der ursprünglichen Datenübermittlung, der Art und der Bedingungen der Strafvollstreckung sowie des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weiterübermittelt werden sollen. Die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, sollte die Weiterübermittlung auch an besondere Bedingungen knüpfen können. Diese besonderen Bedingungen können zum Beispiel in Bearbeitungscodes dargelegt werden.

(66) Die Kommission sollte mit Wirkung für die gesamte Union beschließen können, dass bestimmte Drittländer, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau bieten, und auf diese Weise in Bezug auf die Drittländer und internationalen Organisationen, die für fähig gehalten werden, ein solches Schutzniveau zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen sollten personenbezogene Daten ohne besondere Genehmigung an diese Länder übermittelt werden können, es sei denn, dass ein anderer Mitgliedstaat, von dem die Daten stammen, die Übermittlung zu genehmigen hat.

(67) In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Bewertung des Drittlandes oder eines Gebiets oder eines bestimmten Sektors in einem Drittland berücksichtigen, inwieweit in einem bestimmten Drittland die Rechtsstaatlichkeit gewahrt ist, der Rechtsweg gewährleistet ist und die internationalen Menschenrechtsnormen und -standards eingehalten werden und welche allgemeinen und sektorspezifischen Vorschriften, wozu auch die Vorschriften über die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und öffentliche Ordnung sowie das Strafrecht zählen, dort gelten. Die Annahme eines Angemessenheitsbeschlusses in Bezug auf ein Gebiet oder einen bestimmten Sektor in einem Drittland sollte unter Berücksichtigung eindeutiger und objektiver Kriterien wie bestimmter Verarbeitungsvorgänge und des Anwendungsbereichs anwendbarer Rechtsnormen und geltender Rechtsvorschriften in dem Drittland erfolgen. Das Drittland sollte Garantien für ein angemessenes Schutzniveau bieten, das im Wesentlichen dem innerhalb der Union gewährleisteten Schutzniveau der Sache nach gleichwertig ist, insbesondere in Fällen, in denen Daten in einem oder mehreren spezifischen Sektoren verarbeitet werden. Das Drittland sollte insbesondere eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten und Mechanismen für eine Zusammenarbeit mit den Datenschutzbehörden der Mitgliedstaaten vorsehen, und den betroffenen Personen sollten wirksame und durchsetzbare Rechte sowie wirksame behördliche und gerichtliche Rechtsbehelfe eingeräumt werden.

(68) Die Kommission sollte neben den internationalen Verpflichtungen, die das Drittland oder die internationale Organisation eingegangen ist, auch die Verpflichtungen, die sich aus der Teilnahme des Drittlandes oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere im Hinblick auf den Schutz personenbezogener Daten ergeben, sowie die Umsetzung dieser Verpflichtungen berücksichtigen. Insbesondere sollte der Beitritt des Drittlandes zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen

Zusatzprotokoll berücksichtigt werden. Die Kommission sollte den durch die Verordnung (EU) 2016/679 eingesetzten Europäischen Datenschutzausschuss (im Folgenden „Ausschuss") konsultieren, wenn sie das Schutzniveau in Drittländern oder internationalen Organisationen bewertet. Die Kommission sollte ferner alle maßgeblichen Angemessenheitsbeschlüsse berücksichtigen, die sie nach Artikel 45 der Verordnung (EU) 2016/679 angenommen hat.

(69) Die Kommission sollte die Wirksamkeit von Feststellungen zum Schutzniveau in einem Drittland, einem Gebiet oder einem spezifischen Sektor in einem Drittland oder einer internationalen Organisation überwachen. In ihren Angemessenheitsbeschlüssen sollte die Kommission einen Mechanismus für die regelmäßige Überprüfung ihrer Wirkungsweise vorsehen. Diese regelmäßige Überprüfung sollte in Konsultation mit dem betreffenden Drittland oder der betreffenden internationalen Organisation erfolgen und allen maßgeblichen Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung tragen.

(70) Die Kommission sollte auch feststellen können, dass ein Drittland, ein Gebiet oder ein spezifischer Sektor in einem Drittland oder eine internationale Organisation kein angemessenes Datenschutzniveau mehr bietet. Die Übermittlung personenbezogener Daten an dieses Drittland oder an diese internationale Organisation sollte daraufhin verboten werden, es sei denn, die Anforderungen dieser Richtlinie in Bezug auf Datenübermittlung vorbehaltlich geeigneter Garantien und Ausnahmen für bestimmte Fälle werden erfüllt. Es sollten Verfahren für Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden. Die Kommission sollte dem Drittland oder der internationalen Organisation frühzeitig die Gründe mitteilen und Konsultationen aufnehmen, um Abhilfe für die Situation zu schaffen.

(71) Datenübermittlungen, die nicht auf der Grundlage eines Angemessenheitsbeschlusses erfolgen, sollten nur dann zulässig sein, wenn in einem rechtsverbindlichen Instrument geeignete Garantien festgelegt sind, die den Schutz personenbezogener Daten gewährleisten, oder wenn der Verantwortliche alle Umstände beurteilt hat, die bei der Datenübermittlung eine Rolle spielen, und auf der Grundlage dieser Beurteilung zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen. Solche rechtsverbindlichen Instrumente könnten beispielsweise rechtsverbindliche bilaterale Abkommen sein, die von den Mitgliedstaaten geschlossen und in ihre Rechtsordnung übernommen wurden und von ihren betroffenen Personen durchgesetzt werden können und die sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen einschließlich ihres Rechts auf wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe beachtet werden. Der Verantwortliche sollte Kooperationsvereinbarungen zwischen Europol oder Eurojust und Drittländern berücksichtigen können, die den Austausch personenbezogener Daten ermöglichen, wenn er alle Umstände im Zusammenhang mit der Datenübermittlung beurteilt. Der Verantwortliche sollte außerdem berücksichtigen können, dass die Übermittlung personenbezogener Daten Geheimhaltungspflichten und dem Grundsatz der Spezialität unterliegt, damit gewährleistet wird, dass die Daten nicht zu anderen Zwecken als zu den Zwecken, zu denen sie übermittelt wurden, verarbeitet werden. Darüber hinaus sollte der Verantwortliche berücksichtigen, dass die personenbezogenen Daten nicht verwendet werden, um die Todesstrafe oder eine Form der grausamen und unmenschlichen Behandlung zu beantragen, zu verhängen oder zu vollstrecken. Diese Bedingungen könnten zwar als geeignete Garantien angesehen werden, die die Datenübermittlung zulassen, jedoch sollte der Verantwortliche zusätzliche Garantien verlangen können.

(72) Sind weder ein Angemessenheitsbeschluss noch geeignete Garantien vorhanden, so sollte eine Übermittlung oder eine Kategorie von Übermittlungen nur in bestimmten Fällen erfolgen können, in denen dies erforderlich ist: zur Wahrung wesentlicher Interessen der betroffenen oder einer anderen Person; zum Schutz berechtigter Interessen der betroffenen Person, wenn dies nach dem Recht des Mitgliedstaats, aus dem die personenbezogenen Daten übermittelt werden, vorgesehen ist; zur Abwehr einer unmittelbaren, ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes; in einem Einzelfall zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit; oder in einem Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Diese Ausnahmen sollten restriktiv ausgelegt werden, häufige, umfassende und strukturelle Übermittlungen personenbezogener Daten sowie Datenübermittlungen in großem Umfang ausschließen und daher auf unbedingt notwendige Daten beschränkt sein. Derartige Übermittlungen sollten dokumentiert werden, und die entsprechende Dokumentation sollte der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden, damit diese die Rechtmäßigkeit der Übermittlung überprüfen kann.

(73) Die zuständigen Behörden der Mitgliedstaaten wenden die geltenden bilateralen oder multilateralen internationalen Übereinkünfte, die mit Drittländern auf den Gebieten der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit geschlossen wurden, für den Austausch maßgeblicher Informationen an, um ihnen zu ermöglichen, die ihnen rechtlich zugewiesenen Aufgaben wahrzunehmen. Grundsätzlich erfolgt dies über die im betreffenden Drittland für die Zwecke dieser Richtlinie zuständigen Behörden oder zumindest in Zusammenarbeit mit diesen Behörden des Drittlandes, mitunter auch dann, wenn keine bilaterale oder multilaterale internationale Übereinkunft existiert. In speziellen Einzelfällen können die regulären Verfahren, die eine Kontaktaufnahme mit dieser Behörde in dem betreffenden Drittland vorschreiben, wirkungslos oder ungeeignet sein, insbesondere weil die Übermittlung nicht rechtzeitig durchgeführt werden konnte oder weil diese Behörde in dem betreffenden Drittland die Rechtsstaatlichkeit oder die internationalen Menschenrechtsbestimmungen nicht achtet, so dass die zuständigen Behörden der Mitgliedstaaten beschließen

können, die personenbezogenen Daten direkt an in Drittländern niedergelassene Empfänger zu übermitteln. Dies kann der Fall sein, wenn es dringend geboten ist, personenbezogene Daten zu übermitteln, um das Leben einer Person zu schützen, die Gefahr läuft, Opfer einer Straftat zu werden, oder um die unmittelbar bevorstehende Begehung einer Straftat, einschließlich einer terroristischen Straftat, zu verhindern. Auch wenn eine solche Übermittlung zwischen zuständigen Behörden und in Drittländern niedergelassenen Empfängern nur in speziellen Einzelfällen erfolgen sollte, sollte diese Richtlinie die Voraussetzungen für die Regelung solcher Fälle vorsehen. Diese Bestimmungen sollten nicht als Ausnahmen von geltenden bilateralen oder multilateralen internationalen Übereinkünften auf den Gebieten der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit betrachtet werden. Diese Vorschriften sollten zusätzlich zu den sonstigen Vorschriften dieser Richtlinie gelten, insbesondere den Vorschriften über die Rechtmäßigkeit der Verarbeitung und Kapitel V.

(74) Wenn personenbezogene Daten in ein anderes Land übermittelt werden, kann dies dazu führen, dass natürliche Personen weniger Möglichkeiten haben, ihre Datenschutzrechte wahrzunehmen und sich gegen eine unrechtmäßige Nutzung oder Offenlegung dieser Daten zu schützen. Ebenso kann es vorkommen, dass Aufsichtsbehörden Beschwerden nicht nachgehen oder Untersuchungen nicht durchführen können, die einen Bezug zu Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats haben. Ihre Bemühungen um grenzübergreifende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse und durch widersprüchliche Rechtsordnungen behindert werden. Die Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden muss daher gefördert werden, um ihnen den Informationsaustausch mit Aufsichtsbehörden in anderen Ländern zu erleichtern.

(75) Die Einrichtung von Aufsichtsbehörden in den Mitgliedstaaten, die ihre Aufgaben völlig unabhängig erfüllen können, ist ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Aufsichtsbehörden sollten die Anwendung der nach dieser Richtlinie erlassenen Vorschriften überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen, um natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten zu schützen. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission.

(76) Die Mitgliedstaaten können einer bereits gemäß der Verordnung (EU) 2016/679 errichteten Aufsichtsbehörde die Verantwortung für die Aufgaben übertragen, die von den nach dieser Richtlinie einzurichtenden nationalen Aufsichtsbehörden auszuführen sind.

(77) Die Mitgliedstaaten sollten mehr als eine Aufsichtsbehörde einrichten können, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht. Jede Aufsichtsbehörde sollte mit Finanzmitteln, Personal, Räumlichkeiten und einer Infrastruktur ausgestattet werden, wie sie für die wirksame Wahrnehmung ihrer Aufgaben, auch der Aufgaben im Zusammenhang mit der Amtshilfe und Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union, notwendig sind. Jede Aufsichtsbehörde sollte über eigene, öffentliche, jährliche Haushaltspläne verfügen, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

(78) Die Aufsichtsbehörden sollten unabhängigen Kontroll- oder Überwachungsmechanismen hinsichtlich ihrer Ausgaben unterliegen, sofern diese Finanzkontrolle ihre Unabhängigkeit nicht berührt.

(79) Die allgemeinen Anforderungen an das Mitglied oder die Mitglieder der Aufsichtsbehörde sollten durch Recht der Mitgliedstaaten geregelt werden und insbesondere vorsehen, dass diese Mitglieder entweder vom Parlament oder von der Regierung oder dem Staatsoberhaupt des betreffenden Mitgliedstaats auf Vorschlag der Regierung oder eines Regierungsmitglieds oder des Parlaments oder dessen Kammer oder von einer unabhängigen Stelle ernannt werden, die nach dem Recht des Mitgliedstaats mit der Ernennung im Wege eines transparenten Verfahrens betraut wird. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollten ihre Mitglieder integer handeln, von allen mit den Aufgaben ihres Amts nicht zu vereinbarenden Handlungen absehen und während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit ausüben. Um die Unabhängigkeit der Aufsichtsbehörde zu gewährleisten, sollte ihr Personal von der Aufsichtsbehörde selbst ausgewählt werden; dabei kann eine unabhängige, nach dem Recht des Mitgliedstaats betraute Stelle eingeschaltet werden.

(80) Obgleich diese Richtlinie auch für die Tätigkeit der nationalen Gerichte und anderer Justizbehörden gilt, sollte sich die Zuständigkeit der Aufsichtsbehörden nicht auf die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Datenverarbeitungen erstrecken, damit die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Aufgaben gewahrt bleibt. Diese Ausnahme sollte allerdings begrenzt werden auf justizielle Tätigkeiten in Gerichtssachen und sich nicht auf andere Tätigkeiten beziehen, mit denen Richter nach dem Recht der Mitgliedstaaten betraut werden können. Die Mitgliedstaaten sollten außerdem vorsehen können, dass sich die Zuständigkeit der Aufsichtsbehörde nicht auf die Überwachung der Verarbeitung personenbezogener Daten erstreckt, die durch andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit, beispielsweise Staatsanwaltschaften, erfolgt. Die Einhaltung der Vorschriften dieser Richtlinie durch die Gerichte und andere unabhängige Justizbehörden unterliegt in jedem Fall stets der unabhängigen Überwachung gemäß Artikel 8 Absatz 3 der Charta.

(81) Jede Aufsichtsbehörde sollte sich mit Beschwerden von betroffenen Personen befassen und die Angelegenheit untersuchen oder an die zuständige Aufsichtsbehörde übermitteln. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich einer gerichtlichen Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die Aufsichtsbehörde sollte die betroffene Person innerhalb eines angemessenen Zeitraums über den Stand und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde erforderlich sein, so sollte die betroffene Person über den Zwischenstand informiert werden.

(82) Um die wirksame, zuverlässige und einheitliche Überwachung der Einhaltung und Durchsetzung dieser Richtlinie in der gesamten Union gemäß dem AEUV in der Auslegung durch den Gerichtshof sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter Untersuchungsbefugnisse, Abhilfebefugnisse und beratende Befugnisse, die notwendige Instrumente zur Erfüllung ihrer Aufgaben darstellen. Ihre Befugnisse dürfen jedoch weder die speziellen Vorschriften für Strafverfahren, einschließlich der Ermittlung und Verfolgung von Straftaten, noch die Unabhängigkeit der Gerichte berühren. Unbeschadet der Befugnisse der Strafverfolgungsbehörden nach dem Recht der Mitgliedstaaten sollten die Aufsichtsbehörden außerdem die Befugnis haben, Verstöße gegen diese Richtlinie den Justizbehörden zur Kenntnis zu bringen oder Gerichtsverfahren anzustrengen. Die Befugnisse der Aufsichtsbehörden sollten in Übereinstimmung mit den geeigneten Verfahrensgarantien nach dem Unionsrecht und dem Recht der Mitgliedstaaten unparteiisch, gerecht und innerhalb einer angemessenen Frist ausgeübt werden. Insbesondere sollte jede Maßnahme im Hinblick auf die Gewährleistung der Einhaltung dieser Richtlinie geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind, das Recht einer jeden Person, gehört zu werden, bevor eine individuelle Maßnahme getroffen wird, die nachteilige Auswirkungen auf die betroffene Person hätte, zu achten ist und überflüssige Kosten und übermäßige Unannehmlichkeiten für sie zu vermeiden sind. Untersuchungsbefugnisse im Hinblick auf den Zugang zu Räumlichkeiten sollten im Einklang mit besonderen Anforderungen im Recht der Mitgliedstaaten ausgeübt werden, wie etwa dem Erfordernis einer vorherigen richterlichen Genehmigung. Der Erlass eines rechtsverbindlichen Beschlusses sollte in dem Mitgliedstaat der Aufsichtsbehörde, die den Beschluss erlassen hat, einer gerichtlichen Überprüfung unterliegen.

(83) Die Aufsichtsbehörden sollten sich gegenseitig bei der Erfüllung ihrer Aufgaben unterstützen und einander Amtshilfe leisten, damit eine einheitliche Anwendung und Durchsetzung der nach dieser Richtlinie erlassenen Vorschriften gewährleistet ist.

(84) Der Ausschuss sollte zur einheitlichen Anwendung dieser Richtlinie in der Union beitragen, einschließlich der Beratung der Kommission und der Förderung der Zusammenarbeit der Aufsichtsbehörden in der Union.

(85) Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde eine Beschwerde einzureichen und gemäß Artikel 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten aufgrund von nach dieser Richtlinie erlassenen Vorschriften verletzt sieht oder wenn die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, eine Beschwerde teilweise oder ganz abweist oder ablehnt oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die zuständige Aufsichtsbehörde sollte die betroffene Person innerhalb eines angemessenen Zeitraums über den Stand und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde erforderlich sein, so sollte die betroffene Person über den Zwischenstand informiert werden. Jede Aufsichtsbehörde sollte Maßnahmen zur Erleichterung der Einreichung von Beschwerden treffen, wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(86) Jede natürliche oder juristische Person sollte das Recht auf einen wirksamen gerichtlichen Rechtsbehelf bei dem zuständigen einzelstaatlichen Gericht gegen einen Beschluss einer Aufsichtsbehörde haben, der gegenüber dieser Person Rechtswirkungen entfaltet. Ein derartiger Beschluss betrifft insbesondere die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen durch die Aufsichtsbehörde oder die Ablehnung oder Abweisung von Beschwerden. Dieses Recht umfasst jedoch nicht andere — rechtlich nicht bindende — Maßnahmen der Aufsichtsbehörden wie von ihr abgegebene Stellungnahmen oder Empfehlungen. Verfahren gegen eine Aufsichtsbehörde sollten bei den Gerichten des Mitgliedstaats angestrengt werden, in dem die Aufsichtsbehörde ihren Sitz hat, und sollten im Einklang mit dem Recht dieses Mitgliedstaats durchgeführt werden. Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den anhängigen Rechtsstreit maßgeblichen Sach- und Rechtsfragen zu prüfen, einschließt.

(87) Betroffene Personen, die sich in ihren Rechten gemäß dieser Richtlinie verletzt sehen, sollten das Recht haben, Einrichtungen, die sich den Schutz der Rechte und Interessen der betroffenen Personen im Bereich des Schutzes

ihrer personenbezogenen Daten zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, zu beauftragen, in ihrem Namen eine Beschwerde bei einer Aufsichtsbehörde einzureichen und einen gerichtlichen Rechtsbehelf einzulegen. Das Recht betroffener Personen auf Vertretung sollte das Verfahrensrecht der Mitgliedstaaten unberührt lassen, nach dem eine obligatorische Vertretung betroffener Personen durch einen Rechtsanwalt im Sinne der Richtlinie 77/249/EWG des Rates ([1]) vor nationalen Gerichten erforderlich sein kann.

(88) Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die gegen nach dieser Richtlinie erlassene Vorschriften verstößt, sollten von dem Verantwortlichen oder einer anderen nach dem Recht der Mitgliedstaaten zuständigen Behörde ersetzt werden. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit und auf eine Art und Weise ausgelegt werden, die den Zielen dieser Richtlinie in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Wird auf eine Verarbeitung Bezug genommen, die unrechtmäßig ist oder nicht im Einklang mit den nach dieser Richtlinie erlassenen Vorschriften steht, so gilt dies auch für Verarbeitungen, die gegen gemäß dieser Richtlinie erlassene Durchführungsrechtsakte verstoßen. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten.

(89) Gegen jede natürliche oder juristische — privatem oder öffentlichem Recht unterliegende — Person, die gegen diese Richtlinie verstößt, sollten Sanktionen verhängt werden. Die Mitgliedstaaten sollten dafür sorgen, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sind, und alle Maßnahmen zur Anwendung der Sanktionen treffen.

(90) Um einheitliche Bedingungen für die Anwendung dieser Richtlinie sicherzustellen, sollten der Kommission Durchführungsbefugnisse in Bezug auf Folgendes übertragen werden: die Angemessenheit des Datenschutzniveaus in einem Drittland, in einem Gebiet oder einem spezifischen Sektor in einem Drittland oder in einer internationalen Organisation, das Format und die Verfahren für Amtshilfe und die Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Ausschuss. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([2]) ausgeübt werden.

(91) Durchführungsrechtsakte über die Angemessenheit des Datenschutzniveaus in einem Drittland, in einem Gebiet oder einem spezifischen Sektor in einem Drittland oder in einer internationalen Organisation, über das Format und die Verfahren für Amtshilfe und die Vorkehrungen für den elektronischen Informationsaustausch zwischen Aufsichtsbehörden und zwischen Aufsichtsbehörden und dem Ausschuss sollten im Wege des Prüfverfahrens festgelegt werden, da es sich um Rechtsakte von allgemeiner Tragweite handelt.

(92) Die Kommission sollte in hinreichend begründeten Fällen äußerster Dringlichkeit, die ein Drittland, ein Gebiet oder einen spezifischen Sektor in einem Drittland oder eine internationale Organisation betreffen, die kein angemessenes Schutzniveau mehr gewährleisten, sofort geltende Durchführungsrechtsakte erlassen.

(93) Da die Ziele dieser Richtlinie, nämlich die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz ihrer personenbezogenen Daten und den ungehinderten Austausch personenbezogener Daten im Verkehr zwischen den zuständigen Behörden innerhalb der Union zu gewährleisten, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 EUV verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus.

(94) Besondere Bestimmungen, die in vor Erlass dieser Richtlinie im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit erlassenen Rechtsakten der Union enthalten sind, die die Verarbeitung personenbezogener Daten im Verkehr der Mitgliedstaaten untereinander sowie den Zugang der von den Mitgliedstaaten bestimmten Behörden zu den gemäß den Verträgen errichteten Informationssystemen im

([1]) Richtlinie 77/249/EWG des Rates vom 22. März 1977 zur Erleichterung der tatsächlichen Ausübung des freien Dienstleistungsverkehrs der Rechtsanwälte (ABl. L 78 vom 26.3.1977, S. 17).

([2]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

Anwendungsbereich dieser Richtlinie regeln, sollten unberührt bleiben, beispielsweise die besonderen Bestimmungen betreffend den Schutz personenbezogener Daten gemäß dem Beschluss 2008/615/JI des Rates ([1]) oder Artikel 23 des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union ([2]). Da Artikel 8 der Charta und Artikel 16 AEUV vorschreiben, dass das Grundrecht auf Schutz personenbezogener Daten in der Union einheitlich angewendet werden sollte, sollte die Kommission das Verhältnis zwischen dieser Richtlinie und den vor ihrem Erlass angenommenen Rechtsakten, die die Verarbeitung personenbezogener Daten im Verkehr der Mitgliedstaaten untereinander oder den Zugang der von den Mitgliedstaaten bestimmten Behörden zu den gemäß den Verträgen errichteten Informationssystemen regeln, daraufhin prüfen, inwieweit die besonderen Bestimmungen dieser Rechtsakte an diese Richtlinie angepasst werden müssen. Die Kommission sollte gegebenenfalls Vorschläge zur Gewährleistung einheitlicher Rechtsvorschriften in Bezug auf die Verarbeitung personenbezogener Daten unterbreiten.

(95) Zur Gewährleistung eines umfassenden und einheitlichen Schutzes personenbezogener Daten in der Union sollten internationale Übereinkünfte, die von den Mitgliedstaaten vor Inkrafttreten dieser Richtlinie geschlossen wurden und die im Einklang mit dem maßgeblichen vor Inkrafttreten dieser Richtlinie geltenden Unionsrecht stehen, in Kraft bleiben, bis sie geändert, ersetzt oder gekündigt werden.

(96) Die Mitgliedstaaten sollten gehalten sein, diese Richtlinie innerhalb von höchstens zwei Jahren nach ihrem Inkrafttreten umzusetzen. Verarbeitungen, die zu diesem Zeitpunkt bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Richtlinie mit ihr in Einklang gebracht werden. Stehen die Verarbeitungen jedoch im Einklang mit dem vor Inkrafttreten dieser Richtlinie geltenden Unionsrecht, so sollten die Anforderungen der vorliegenden Richtlinie betreffend die vorherige Konsultation der Aufsichtsbehörde nicht für Verarbeitungsvorgänge gelten, die bereits vor diesem Zeitpunkt begonnen wurden, da diese Anforderungen naturgemäß vor der Verarbeitung erfüllt sein müssen. Nehmen Mitgliedstaaten die längere Umsetzungsfrist, die sieben Jahre nach dem Inkrafttreten dieser Richtlinie endet, in Anspruch, um den Protokollierungspflichten für vor dem Inkrafttreten dieser Richtlinie eingerichtete automatisierte Verarbeitungssysteme nachzukommen, so sollte der Verantwortliche oder der Auftragsverarbeiter über wirksame Methoden zum Nachweis der Rechtmäßigkeit der Datenverarbeitung, zur Ermöglichung der Eigenüberwachung und zur Sicherstellung der Integrität und Sicherheit der Daten, wie etwa Protokolle oder andere Formen von Verzeichnissen, verfügen.

(97) Diese Richtlinie lässt die Vorschriften zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie nach Maßgabe der Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates ([3]) unberührt.

(98) Der Rahmenbeschluss 2008/977/JI sollte daher aufgehoben werden.

(99) Nach Artikel 6a des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts sind die Bestimmungen dieser Richtlinie über die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 AEUV fallen, für das Vereinigte Königreich und Irland nicht bindend, wenn das Vereinigte Königreich und Irland nicht durch die Vorschriften gebunden sind, die Formen der justiziellen Zusammenarbeit in Strafsachen oder der polizeilichen Zusammenarbeit regeln, in deren Rahmen die auf der Grundlage des Artikels 16 AEUV festgelegten Vorschriften eingehalten werden müssen.

(100) Nach den Artikeln 2 und 2a des dem EUV und dem AEUV beigefügten Protokolls Nr. 22 über die Position Dänemarks ist Dänemark durch die Bestimmungen dieser Richtlinie, die sich auf die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten beziehen, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 AEUV fallen, weder gebunden noch zu ihrer Anwendung verpflichtet. Da diese Richtlinie den Schengen-Besitzstand gemäß dem Dritten Teil Titel V AEUV ergänzt, beschließt Dänemark gemäß Artikel 4 des genannten Protokolls innerhalb von sechs Monaten nach Erlass dieser Richtlinie, ob es sie in nationales Recht umsetzt.

(101) Für Island und Norwegen stellt diese Richtlinie eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar. ([4])

([1]) Rahmenbeschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1).

([2]) Rechtsakt des Rates vom 29. Mai 2000 über die Erstellung — gemäß Artikel 34 des Vertrags über die Europäische Union — des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (ABl. C 197 vom 12.7.2000, S. 1).

([3]) Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1).

([4]) ABl. L 176 vom 10.7.1999, S. 36.

(102) Für die Schweiz stellt diese Richtlinie eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar. ([1])

(103) Für Lichtenstein stellt diese Richtlinie eine Weiterentwicklung von Bestimmungen des Schengen-Besitzstands im Sinne des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar. ([2])

(104) Diese Richtlinie steht im Einklang mit den Grundrechten und Grundsätzen, die mit der Charta anerkannt wurden und im AEUV verankert sind, insbesondere mit dem Recht auf Achtung des Privat- und Familienlebens, dem Recht auf Schutz personenbezogener Daten sowie dem Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren. Die Einschränkungen dieser Rechte stehen im Einklang mit Artikel 52 Absatz 1 der Charta, da sie erforderlich sind, um den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und der Freiheiten anderer zu entsprechen.

(105) Gemäß der Gemeinsamen Politischen Erklärung der Mitgliedstaaten und der Kommission vom 28. September 2011 zu erläuternden Dokumenten haben sich die Mitgliedstaaten verpflichtet, in begründeten Fällen zusätzlich zur Mitteilung ihrer Umsetzungsmaßnahmen ein oder mehrere Dokumente zu übermitteln, in denen der Zusammenhang zwischen den Bestandteilen einer Richtlinie und den entsprechenden Teilen einzelstaatlicher Umsetzungsmaßnahmen erläutert wird. In Bezug auf diese Richtlinie hält der Gesetzgeber die Übermittlung derartiger Dokumente für gerechtfertigt.

(106) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert und hat seine Stellungnahme am 7. März 2012 abgegeben ([3]).

(107) Diese Richtlinie sollte die Mitgliedstaaten nicht daran hindern, die Bestimmungen über die Ausübung der Rechte der betroffenen Personen auf Unterrichtung, Auskunft und Berichtigung oder Löschung personenbezogener Daten und Beschränkung der Verarbeitung im Rahmen eines Strafverfahrens sowie mögliche Beschränkungen dieser Rechte in ihr einzelstaatliches Strafverfahrensrecht umzusetzen —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Ziele

(1) Diese Richtlinie enthält Bestimmungen 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

(2) Gemäß dieser Richtlinie haben die Mitgliedstaaten

a) die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, zu schützen und

b) sicherzustellen, dass der Austausch personenbezogener Daten zwischen den zuständigen Behörden in der Union — sofern er nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen ist — nicht aus Gründen, die mit dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten verbunden sind, eingeschränkt oder verboten wird.

([1]) ABl. L 53 vom 27.2.2008, S. 52.
([2]) ABl. L 160 vom 18.6.2011, S. 21.
([3]) ABl. C 192, 30.6.2012, S. 7

(3) Diese Richtlinie hindert die Mitgliedstaaten nicht daran, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie.

Artikel 2

Anwendungsbereich

(1) Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu den in Artikel 1 Absatz 1 genannten Zwecken.

(2) Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(3) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

b) durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union.

Artikel 3

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. „zuständige Behörde“

   a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder

   b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;

8. „Verantwortlicher“ die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

9. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

10. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

11. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

12. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

13. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

14. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

15. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 41 eingerichtete unabhängige staatliche Stelle;

16. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

KAPITEL II

Grundsätze

Artikel 4

Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten

(1) Die Mitgliedstaaten sehen vor dass personenbezogene Daten

a) auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

c) dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind,

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,

e) nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

(2) Eine Verarbeitung durch denselben oder einen anderen Verantwortlichen für einen anderen der in Artikel 1 Absatz 1 genannten Zwecke als den, für den die personenbezogenen Daten erhoben werden, ist erlaubt, sofern

a) der Verantwortliche nach dem Unionsrecht oder dem Recht der Mitgliedstaaten befugt ist, solche personenbezogenen Daten für diesen anderen Zweck zu verarbeiten, und

b) die Verarbeitung für diesen anderen Zweck nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich und verhältnismäßig ist.

(3) Die Verarbeitung durch denselben oder einen anderen Verantwortlichen kann die Archivierung im öffentlichen Interesse und die wissenschaftliche, statistische oder historische Verwendung für die in Artikel 1 Absatz 1 genannten Zwecke umfassen, sofern geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorhanden sind.

(4) Der Verantwortliche ist für die Einhaltung der Absätze 1, 2 und 3 verantwortlich und muss deren Einhaltung nachweisen können.

Artikel 5

Fristen für die Speicherung und Überprüfung

Die Mitgliedstaaten sehen vor, dass für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen sind. Durch verfahrensrechtliche Vorkehrungen ist sicherzustellen, dass diese Fristen eingehalten werden.

Artikel 6

Unterscheidung verschiedener Kategorien betroffener Personen

Die Mitgliedstaaten sehen vor, dass der Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen klar unterscheidet, darunter:

a) Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden,

b) verurteilte Straftäter,

c) Opfer einer Straftat oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und

d) andere Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den unter den Buchstaben a und b genannten Personen in Kontakt oder in Verbindung stehen.

Artikel 7

Unterscheidung zwischen personenbezogenen Daten und Überprüfung der Qualität der personenbezogenen Daten

(1) Die Mitgliedstaaten sehen vor, dass bei personenbezogenen Daten so weit wie möglich zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten unterschieden wird.

(2) Die Mitgliedstaaten sehen vor, dass die zuständigen Behörden alle angemessenen Maßnahmen ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Zu diesem Zweck überprüft jede zuständige Behörde, soweit durchführbar, die Qualität der personenbezogenen Daten vor ihrer Übermittlung oder Bereitstellung. Bei jeder Übermittlung personenbezogener Daten werden nach Möglichkeit die erforderlichen Informationen beigefügt, die es der empfangenden zuständigen Behörde gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der personenbezogenen Daten sowie deren Aktualitätsgrad zu beurteilen.

(3) Wird festgestellt, dass unrichtige personenbezogene Daten übermittelt worden sind oder die personenbezogenen Daten unrechtmäßig übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. In diesem Fall ist gemäß Artikel 16 eine Berichtigung oder Löschung oder die Einschränkung der Verarbeitung der personenbezogenen Daten vorzunehmen.

Artikel 8

Rechtmäßigkeit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass die Verarbeitung nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Artikel 1 Absatz 1 genannten Zwecken wahrgenommenen wird, und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt.

(2) Im Recht der Mitgliedstaaten, das die Verarbeitung innerhalb des Anwendungsbereichs dieser Richtlinie regelt, werden zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben.

Artikel 9

Besondere Verarbeitungsbedingungen

(1) Personenbezogene Daten, die von zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke erhoben werden, dürfen nicht für andere als die in Artikel 1 Absatz 1 genannten Zwecke verarbeitet werden, es sei denn, eine derartige Verarbeitung ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig. Wenn personenbezogene Daten für solche andere Zwecke verarbeitet werden, gilt die Verordnung (EU) 2016/679, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

(2) Sind nach dem Recht der Mitgliedstaaten zuständige Behörden mit der Wahrnehmung von Aufgaben betraut, die sich nicht mit den für die in Artikel 1 Absatz 1 genannten Zwecke wahrgenommenen Aufgaben decken, gilt die Verordnung (EU) 2016/679 für die Verarbeitung zu diesen Zwecken — wozu auch im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke zählen —, es sei denn, die Verarbeitung erfolgt im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

(3) Die Mitgliedstaaten sehen vor, dass immer dann, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem die übermittelnde zuständige Behörde unterliegt, für die Verarbeitung besondere Bedingungen gelten, die übermittelnde zuständige Behörde den Empfänger der Daten darauf hinweist, dass diese Bedingungen gelten und einzuhalten sind.

(4) Die Mitgliedstaaten sehen vor, dass die übermittelnde zuständige Behörde auf Empfänger in anderen Mitgliedstaaten oder nach Titel V Kapitel 4 und 5 AEUV errichtete Einrichtungen und sonstige Stellen keine Bedingungen nach Absatz 3 anwendet, die nicht auch für entsprechende Datenübermittlungen innerhalb ihres eigenen Mitgliedstaats gelten.

Artikel 10

Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung ist nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und

a) wenn sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist

b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder

c) wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.

Artikel 11

Automatisierte Entscheidungsfindung im Einzelfall

(1) Die Mitgliedstaaten sehen vor, dass eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung — einschließlich Profiling —, die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt, verboten ist, es sei denn, sie ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt und das geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen, erlaubt.

(2) Entscheidungen nach Absatz 1 dieses Artikels dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 10 beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

(3) Profiling, das zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Datenkategorien nach Artikel 10 diskriminiert werden, ist nach dem Unionsrecht verboten.

KAPITEL III

Rechte der betroffenen Person

Artikel 12

Mitteilungen und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche alle angemessenen Maßnahmen trifft, um der betroffenen Person alle Informationen gemäß Artikel 13 sowie alle Mitteilungen gemäß den Artikeln 11, 14 bis 18 und 31, die sich auf die Verarbeitung beziehen, in präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Übermittlung der Informationen erfolgt in einer beliebigen geeigneten Form, wozu auch die elektronische Übermittlung zählt. Grundsätzlich übermittelt der Verantwortliche die Informationen in derselben Form, in der er den Antrag erhalten hat.

(2) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die Ausübung der den betroffenen Personen gemäß den Artikeln 11 und 14 bis 18 zustehenden Rechte erleichtert.

(3) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person unverzüglich schriftlich darüber in Kenntnis setzt, wie mit ihrem Antrag verfahren wurde.

(4) Die Mitgliedstaaten sehen vor, dass die Informationen gemäß Artikel 13 und alle gemachten Mitteilungen und getroffenen Maßnahmen gemäß den Artikeln 11, 14 bis 18 und 31 unentgeltlich zur Verfügung gestellt werden. Bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

a) eine angemessene Gebühr verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder

b) er kann sich weigern, aufgrund des Antrags tätig zu werden.

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(5) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 14 oder 16 stellt, so kann er zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

Artikel 13

Der betroffenen Person zur Verfügung zu stellende oder zu erteilende Informationen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche der betroffenen Person zumindest die folgenden Informationen zur Verfügung stellt:

a) den Namen und die Kontaktdaten des Verantwortlichen,

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten,

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden,

d) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,

e) das Bestehen eines Rechts auf Auskunft und Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person durch den Verantwortlichen.

(2) Zusätzlich zu den in Absatz 1 genannten Informationen sehen die Mitgliedstaaten durch Rechtsvorschriften vor, dass der Verantwortliche der betroffenen Person in besonderen Fällen die folgenden zusätzlichen Informationen erteilt, um die Ausübung der Rechte der betroffenen Person zu ermöglichen:

a) die Rechtsgrundlage der Verarbeitung,

b) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

c) gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittländern oder in internationalen Organisationen,

d) erforderlichenfalls weitere Informationen, insbesondere wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben werden.

(3) Die Mitgliedstaaten können Gesetzgebungsmaßnahmen erlassen, nach denen die Unterrichtung der betroffenen Person gemäß Absatz 2 soweit und so lange aufgeschoben, eingeschränkt oder unterlassen werden kann, wie diese Maßnahme in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und sofern den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird:

a) zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

b) zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,

c) zum Schutz der öffentlichen Sicherheit,

d) zum Schutz der nationalen Sicherheit,

e) zum Schutz der Rechte und Freiheiten anderer.

(4) Die Mitgliedstaaten können Gesetzgebungsmaßnahmen zur Festlegung der Verarbeitungskategorien erlassen, für die einer der Buchstaben des Absatz 3 vollständig oder teilweise zur Anwendung kommt.

Artikel 14

Auskunftsrecht der betroffenen Person

Vorbehaltlich des Artikels 15 sehen die Mitgliedstaaten vor, dass die betroffene Person das Recht hat, von dem Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie das Recht, Auskunft über personenbezogene Daten und zu folgenden Informationen zu erhalten:

a) die Zwecke der Verarbeitung und deren Rechtsgrundlage,

b) die Kategorien personenbezogener Daten, die verarbeitet werden,

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen,

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

e) das Bestehen eines Rechts auf Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung personenbezogener Daten der betroffenen Person durch den Verantwortlichen,

f) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,

g) Mitteilung zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten.

Artikel 15

Einschränkung des Auskunftsrechts

(1) Die Mitgliedstaaten können Gesetzgebungsmaßnahmen erlassen, die zu nachstehenden Zwecken das Recht der betroffenen Person auf Auskunft teilweise oder vollständig einschränken, soweit und so lange wie diese teilweise oder vollständige Einschränkung in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird:

a) Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

b) Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,

c) Schutz der öffentlichen Sicherheit,

d) Schutz der nationalen Sicherheit,

e) Schutz der Rechte und Freiheiten anderer.

(2) Die Mitgliedstaaten können Gesetzgebungsmaßnahmen zur Festlegung der Verarbeitungskategorien erlassen, für die Absatz 1 Buchstaben a bis e vollständig oder teilweise zur Anwendung kommen.

(3) Für die in den Absätzen 1 und 2 genannten Fälle sehen die Mitgliedstaaten vor, dass der Verantwortliche die betroffene Person unverzüglich schriftlich über die Verweigerung oder die Einschränkung der Auskunft und die Gründe hierfür unterrichtet. Dies gilt nicht, wenn die Erteilung dieser Informationen einem der in Absatz 1 genannten Zwecke zuwiderliefe. Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person über die Möglichkeit unterrichtet, bei der Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(4) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die sachlichen oder rechtlichen Gründe für die Entscheidung dokumentiert. Diese Angaben sind der Aufsichtsbehörde zur Verfügung zu stellen.

Artikel 16

Recht auf Berichtigung oder Löschung personenbezogener Daten und Einschränkung der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass die betroffene Person das Recht hat, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung sehen die Mitgliedstaaten vor, dass die betroffene Person das Recht hat, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

(2) Die Mitgliedstaaten verlangen vom Verantwortlichen, personenbezogene Daten unverzüglich zu löschen, und sehen vor, dass die betroffene Person das Recht hat, von dem Verantwortlichen die Löschung von sie betreffenden personenbezogenen Daten unverzüglich zu verlangen, wenn die Verarbeitung gegen die nach den Artikeln 4, 8 und 10 erlassenen Vorschriften verstößt oder wenn die personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen, der der Verantwortliche unterliegt.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

a) die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, oder

b) die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden müssen.

Unterliegt die Verarbeitung einer Beschränkung gemäß Unterabsatz 1 Buchstabe a, unterrichtet der Verantwortliche die betroffene Person, bevor er die Beschränkung aufhebt.

(4) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person schriftlich über eine Verweigerung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung und über die Gründe für die Verweigerung unterrichtet. Die Mitgliedstaaten können Gesetzgebungsmaßnahmen erlassen, die zu nachstehenden Zwecken die Pflicht, diese Informationen zur Verfügung zu stellen, teilweise oder vollständig einschränken, soweit diese Einschränkung in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird:

a) Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden,

b) Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlungen oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,

c) Schutz der öffentlichen Sicherheit,

d) Schutz der nationalen Sicherheit,

e) Schutz der Rechte und Freiheiten anderer.

Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person über die Möglichkeit unterrichtet, bei der Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die Berichtigung von unrichtigen personenbezogenen Daten der zuständigen Behörde, von der die unrichtigen Daten stammen, mitteilt.

(6) Die Mitgliedstaaten sehen vor, dass in Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1, 2 und 3 der Verantwortliche die Empfänger in Kenntnis setzt und dass die Empfänger die ihrer Verantwortung unterliegenden personenbezogenen Daten berichtigen, löschen oder deren Verarbeitung einschränken.

Artikel 17

Ausübung von Rechten durch die betroffene Person und Prüfung durch die Aufsichtsbehörde

(1) In den in Artikel 13 Absatz 3, Artikel 15 Absatz 3 und Artikel 16 Absatz 4 genannten Fällen erlassen die Mitgliedstaaten Maßnahmen, in denen vorgesehen ist, dass die Rechte der betroffenen Person auch über die zuständige Aufsichtsbehörde ausgeübt werden können.

(2) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die betroffene Person über die Möglichkeit unterrichtet, ihr Recht auf Befassung der Aufsichtsbehörde gemäß Absatz 1 auszuüben.

(3) Wird das in Absatz 1 genannte Recht ausgeübt, unterrichtet die Aufsichtsbehörde die betroffene Person zumindest darüber, dass alle erforderlichen Prüfungen oder eine Überprüfung durch die Aufsichtsbehörde erfolgt sind. Die Aufsichtsbehörde hat zudem die betroffene Person über ihr Recht auf einen gerichtlichen Rechtsbehelf zu unterrichten.

Artikel 18

Rechte der betroffenen Person in strafrechtlichen Ermittlungen und in Strafverfahren

Die Mitgliedstaaten können vorsehen, dass die Ausübung der Rechte nach den Artikeln 13, 14 und16 im Einklang mit dem Recht der Mitgliedstaaten erfolgt, wenn es um personenbezogene Daten in einer gerichtlichen Entscheidung oder einem Dokument oder einer Verfahrensakte geht, die in strafrechtlichen Ermittlungen und in Strafverfahren verarbeitet werden.

KAPITEL IV

Verantwortlicher und Auftragsverarbeiter

Abschnitt 1

Allgemeine Pflichten

Artikel 19

Pflichten des Verantwortlichen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung in Übereinstimmung mit dieser Richtlinie erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

Artikel 20

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Richtlinie zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Die Mitgliedstaaten sehen vor, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen trifft, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Artikel 21

Gemeinsam Verantwortliche

(1) Die Mitgliedstaaten sehen vor, dass in dem Fall, dass zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen, sie gemeinsam Verantwortliche sind. Sie legen in einer Vereinbarung in transparenter Form ihre jeweiligen Aufgaben gemäß dieser Richtlinie fest insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß Artikel 13 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch das Unionsrecht oder das Recht der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung wird eine Anlaufstelle für die betroffenen Personen angegeben. Die Mitgliedstaaten können angeben, welcher der gemeinsam Verantwortlichen als zentrale Anlaufstelle für die betroffenen Personen handeln kann, wenn es um die Ausübung ihrer Rechte geht.

(2) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 können die Mitgliedstaaten vorsehen, dass die betroffene Person ihre Rechte im Rahmen der nach dieser Richtlinie erlassenen Vorschriften bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen kann.

Artikel 22

Auftragsverarbeiter

(1) Die Mitgliedstaaten sehen vor, dass in dem Fall, dass eine Verarbeitung im Auftrag eines Verantwortlichen erfolgt, dieser nur mit Auftragsverarbeitern arbeitet, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Richtlinie erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Die Mitgliedstaaten sehen vor, dass der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nimmt. Im Fall einer allgemeinen schriftlichen Genehmigung unterrichtet der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Mitgliedstaaten sehen vor, dass die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erfolgt, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und der den Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) nur auf Weisung des Verantwortlichen handelt,

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,

c) den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten,

d) alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen — nach Wahl des Verantwortlichen — zurückgibt bzw. löscht und bestehende Kopien vernichtet, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,

e) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt,

f) die in den Absätzen 2 und 3 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält.

(4) Der Vertrag oder das andere Rechtsinstrument im Sinne von Absatz 3 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(5) Ein Auftragsverarbeiter, der unter Verstoß gegen diese Richtlinie die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

Artikel 23

Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Die Mitgliedstaaten sehen vor, dass der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Artikel 24

Verzeichnis von Verarbeitungstätigkeiten

(1) Die Mitgliedstaaten sehen vor, dass jeder Verantwortliche ein Verzeichnis aller Kategorien von Tätigkeiten der Verarbeitung, die seiner Zuständigkeit unterliegen, führt. Dieses Verzeichnis enthält alle der folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen, gegebenenfalls des gemeinsam mit ihm Verantwortlichen und eines etwaigen Datenschutzbeauftragten,

b) die Zwecke der Verarbeitung,

c) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängern in Drittländern oder internationalen Organisationen,

d) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,

e) gegebenenfalls die Verwendung von Profiling,

f) gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation,

g) Angaben über die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind,

h) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Kategorien personenbezogener Daten,

i) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 29 Absatz 1.

(2) Die Mitgliedstaaten sehen vor, dass jeder Auftragsverarbeiter ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung führt, die Folgendes enthält:

a) Name und Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines etwaigen Datenschutzbeauftragten,

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, wenn vom Verantwortlichen entsprechend angewiesen, einschließlich der Identifizierung des Drittlandes oder der internationalen Organisation,

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 29 Absatz 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

Der Verantwortliche und der Auftragsverarbeiter stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

Artikel 25

Protokollierung

(1) Die Mitgliedstaaten sehen vor, dass in automatisierten Verarbeitungssystemen zumindest die folgenden Verarbeitungsvorgänge protokolliert werden: Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung. Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identifizierung der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers solcher personenbezogenen Daten festzustellen.

(2) Die Protokolle werden ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für Strafverfahren verwendet.

(3) Der Verantwortliche sowie der Auftragsverarbeiter stellen die Protokolle der Aufsichtsbehörde auf Anforderung zur Verfügung.

Artikel 26

Zusammenarbeit mit der Aufsichtsbehörde

Die Mitgliedstaaten sehen vor, dass der Verantwortliche und der Auftragsverarbeiter auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten.

Artikel 27

Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so sehen die Mitgliedstaaten vor, dass der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführt.

(2) Die Folgenabschätzung gemäß Absatz 1 trägt den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung und enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Richtlinie eingehalten wird.

Artikel 28

Vorherige Konsultation der Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche oder der Auftragsverarbeiter vor der Verarbeitung personenbezogener Daten in neu anzulegenden Dateisystemen die Aufsichtsbehörde konsultiert, wenn

a) aus einer Datenschutz-Folgenabschätzung gemäß Artikel 27 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, oder

b) die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.

(2) Die Mitgliedstaaten sehen vor, dass bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung betreffen, die Aufsichtsbehörde konsultiert wird.

(3) Die Mitgliedstaaten sehen vor, dass die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge erstellen kann, die der Pflicht zur vorherigen Konsultation nach Absatz 1 unterliegen.

(4) Die Mitgliedstaaten sehen vor, dass der Verantwortliche der Aufsichtsbehörde die Datenschutz-Folgenabschätzung gemäß Artikel 27 vorlegt und ihr auf Anfrage alle sonstigen Informationen übermittelt, die sie benötigt, um die Ordnungsgemäßheit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Person bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(5) Die Mitgliedstaaten sehen vor, dass die Aufsichtsbehörde, wenn sie der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 dieses Artikels gegen die nach dieser Richtlinie erlassenen Vorschriften verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu sechs Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen unterbreitet und ihre in Artikel 47 genannten Befugnisse ausüben kann. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um einen weiteren Monat verlängert werden. Die Aufsichtsbehörde unterrichtet den Verantwortliche oder gegebenenfalls den Auftragsverarbeiter über eine solche Fristverlängerung innerhalb eines Monats nach Eingang des Antrags auf Konsultation zusammen mit den Gründen für die Verzögerung.

Abschnitt 2

Sicherheit personenbezogener Daten

Artikel 29

Sicherheit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Artikel 10.

(2) Die Mitgliedstaaten sehen im Hinblick auf die automatisierte Verarbeitung vor, dass der Verantwortliche oder der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen ergreift, die Folgendes bezwecken:

a) Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),

b) Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle),

c) Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),

d) Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),

e) Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugangskontrolle),

f) Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

g) Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle),

h) Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

i) Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung),

j) Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

Artikel 30

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass im Falle einer Verletzung des Schutzes personenbezogener Daten der Verantwortliche diese unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der Aufsichtsbehörde meldet, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien personenbezogener Daten und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,

b) Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Die Mitgliedstaaten sehen vor, dass der Verantwortliche Verletzungen des Schutzes personenbezogener Daten nach Absatz 1 einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen dokumentiert. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.

(6) Die Mitgliedstaaten sehen vor, dass, soweit von der Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von dem oder an den Verantwortlichen eines anderen Mitgliedstaats übermittelt wurden, die in Absatz 3 genannten Informationen dem Verantwortlichen jenes Mitgliedstaats unverzüglich übermittelt werden.

Artikel 31

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Die Mitgliedstaaten sehen vor, dass, wenn die Verletzung des Schutzes personenbezogener voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, der Verantwortliche die betroffene Person unverzüglich von der Verletzung benachrichtigt.

(2) Die in Absatz 1 dieses Artikels genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 30 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung,

b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht,

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

(5) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 dieses Artikels kann unter zu den in Artikel 13 Absatz 3 genannten Voraussetzungen und aus den dort genannten Gründen aufgeschoben, eingeschränkt oder unterlassen werden.

Abschnitt 3

Datenschutzbeauftragter

Artikel 32

Benennung eines Datenschutzbeauftragten

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche einen Datenschutzbeauftragten benennt. Mitgliedstaaten können Gerichte und andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit von dieser Pflicht befreien.

(2) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 34 genannten Aufgaben.

(3) Ein Datenschutzbeauftragter kann für mehrere zuständige Behörden gemeinsam ernannt werden, wobei deren Organisationsstruktur und Größe Rechnung getragen wird.

(4) Die Mitgliedstaaten sehen vor, dass der Verantwortliche die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und der Aufsichtsbehörde mitteilt.

Artikel 33

Stellung des Datenschutzbeauftragten

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche sicherstellt, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Der Verantwortliche unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 34, indem er die hierfür erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

Artikel 34

Aufgaben des Datenschutzbeauftragten

Die Mitgliedstaaten sehen vor, dass der Verantwortliche den Datenschutzbeauftragten mit zumindest folgenden Aufgaben betraut:

a) Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Richtlinie sowie anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten,

b) Überwachung der Einhaltung dieser Richtlinie, anderer Datenschutzvorschriften der Union oder der Mitgliedstaaten sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen,

c) Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 27,

d) Zusammenarbeit mit der Aufsichtsbehörde,

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 28, und gegebenenfalls Beratung zu allen sonstigen Fragen.

KAPITEL V

Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen

Artikel 35

Allgemeine Grundsätze für die Übermittlung personenbezogener Daten

(1) Die Mitgliedstaaten sehen vor, dass jedwede von einer zuständigen Behörde vorgenommene Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, einschließlich der Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation, nur unter Einhaltung der nach Maßgabe anderer Bestimmungen dieser Richtlinie erlassenen nationalen Bestimmungen, zulässig ist, wenn die in diesem Kapitel festgelegten Bedingungen eingehalten werden, nämlich

a) die Übermittlung für die in Artikel 1 Absatz 1 genannten Zwecke erforderlich ist;

b) die personenbezogenen Daten an einen Verantwortlichen in einem Drittland oder einer internationalen Organisation, die eine für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde ist, übermittelt werden;

c) in Fällen, in denen personenbezogene Daten aus einem anderen Mitgliedstaat übermittelt oder zur Verfügung gestellt werden, dieser Mitgliedstaat die Übermittlung zuvor in Einklang mit seinem nationalen Recht genehmigt hat;

d) die Kommission gemäß Artikel 36 einen Angemessenheitsbeschluss gefasst hat oder, wenn kein solcher Beschluss vorliegt, geeignete Garantien im Sinne des Artikels 37 erbracht wurden oder bestehen oder, wenn kein Angemessenheitsbeschluss gemäß Artikel 36 vorliegt und keine geeigneten Garantien im Sinne des Artikels 37 vorhanden sind, Ausnahmen für bestimmte Fälle gemäß Artikel 38 anwendbar sind und

e) im Fall der Weiterübermittlung an ein anderes Drittland oder eine andere internationale Organisation die zuständige Behörde, die die ursprüngliche Übermittlung durchgeführt hat, oder eine andere zuständige Behörde des gleichen Mitgliedstaats die Weiterübermittlung genehmigt nach gebührender Berücksichtigung sämtlicher maßgeblicher Faktoren, einschließlich der Schwere der Straftat, des Zwecks der ursprünglichen Übermittlung personenbezogener Daten und des Schutzniveaus für personenbezogene Daten in dem Drittland oder der internationalen Organisation, an das bzw. die personenbezogene Daten weiterübermittelt werden.

(2) Die Mitgliedstaaten sehen vor, dass Übermittlungen ohne vorherige Genehmigung durch einen anderen Mitgliedstaat gemäß Absatz 1 Buchstabe c nur dann zulässig sind, wenn die Übermittlung der personenbezogenen Daten erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Die Behörde, die für die Erteilung der vorherigen Genehmigung zuständig ist, wird unverzüglich unterrichtet.

(3) Sämtliche Bestimmungen dieses Kapitels werden angewendet, um sicherzustellen, dass das durch diese Richtlinie gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Artikel 36

Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt werden dürfen, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlungen bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des Schutzniveaus berücksichtigt die Kommission insbesondere

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. der betreffenden internationalen Organisation geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, auch in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, und der Zugang der Behörden zu personenbezogenen Daten sowie die Durchsetzung dieser Vorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Rechtsinstrumenten sowie aus der Teilnahme des Drittlandes oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland beziehungsweise ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 dieses Artikels bietet. In dem Durchführungsrechtsakt wird ein Mechanismus für die regelmäßige Überprüfung vorgesehen, die mindestens alle vier Jahre erfolgt und bei der allen maßgeblichen Entwicklungen in dem Drittland oder der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b dieses Artikels genannte Aufsichtsbehörde oder die dort genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 erlassenen Beschlüsse beeinträchtigen könnten.

(5) Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen — insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung — dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels mehr gewährleistet. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren oder in äußerst dringlichen Fällen gemäß dem in Artikel 58 Absatz 3 genannten Verfahren erlassen.

In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 58 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

(6) Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem Beschluss nach Absatz 5 geführt hat.

(7) Die Mitgliedstaaten sehen vor, dass Übermittlungen personenbezogener Daten an das betreffende Drittland, an das Gebiet oder einen oder mehrere spezifischen Sektoren in einem Drittland oder an die betreffende internationale Organisation gemäß den Artikeln 37 und 38 durch einen Beschluss nach Absatz 5 nicht berührt werden.

(8) Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* und auf ihrer Website eine Liste aller Drittländern beziehungsweise Gebiete und spezifischen Sektoren in einem Drittland und aller internationalen Organisationen, bei denen sie durch Beschluss festgestellt hat, dass diese ein beziehungsweise kein angemessenes Schutzniveau für personenbezogene Daten bieten.

Artikel 37

Datenübermittlung vorbehaltlich geeigneter Garantien

(1) Liegt kein Beschluss nach Artikel 36 Absatz 3 vor, so sehen die Mitgliedstaaten vor, dass eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgen darf, wenn

a) in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder

b) der Verantwortliche alle Umstände beurteilt hat, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, und zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen.

(2) Der Verantwortliche unterrichtet die Aufsichtsbehörde über Kategorien von Übermittlungen gemäß Absatz 1 Buchstabe b.

(3) Übermittlungen gemäß Absatz 1 Buchstabe b werden dokumentiert und die Dokumentation einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, Begründung der Übermittlung und übermittelte personenbezogenen Daten, der Aufsichtsbehörde auf Anforderung zur Verfügung gestellt.

Artikel 38

Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 36 vorliegt noch geeignete Garantien nach Artikel 37 bestehen, sehen die Mitgliedstaaten vor, dass eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur zulässig ist, wenn die Übermittlung aus einem der folgenden Gründe erforderlich ist

a) zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person,

b) zur Wahrung berechtigter Interessen der betroffenen Person, wenn dies im Recht des Mitgliedstaats, aus dem die personenbezogenen Daten übermittelt werden, vorgesehen ist,

c) zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes,

d) im Einzelfall für die in Artikel 1 Absatz 1 genannten Zwecke, oder

e) im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in Artikel 1 Absatz 1 genannten Zwecken.

(2) Personenbezogene Daten dürfen nicht übermittelt werden, wenn die übermittelnde zuständige Behörde feststellt, dass Grundrechte und Grundfreiheiten der betroffenen Person das öffentliche Interesse an der Übermittlung im Sinne des Absatzes 1 Buchstaben d und e überwiegen.

(3) Übermittlungen gemäß Absatz 1 werden dokumentiert und die Dokumentation einschließlich Datum und Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, Begründung der Übermittlung und übermittelte personenbezogene Daten, der Aufsichtsbehörde auf Anforderung zur Verfügung gestellt.

Artikel 39

Übermittlung personenbezogener Daten an in Drittländern niedergelassene Empfänger

(1) Abweichend von Artikel 35 Absatz 1 Buchstabe b und unbeschadet der in Absatz 2 dieses Artikels genannten internationalen Übereinkünfte kann das Unionsrecht oder das Recht der Mitgliedstaaten vorsehen, dass die in Artikel 3 Nummer 7 Buchstabe a genannten zuständigen Behörden im speziellen Einzelfall nur dann personenbezogene Daten direkt an in Drittländern niedergelassene Empfänger übermitteln dürfen, wenn die übrigen Bestimmungen dieser Richtlinie eingehalten werden und alle der folgende Voraussetzungen gegeben sind:

a) Die Übermittlung ist für die Ausübung einer Aufgabe der übermittelnden zuständigen Behörde gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten für die in Artikel 1 Absatz 1 genannten Zwecke unbedingt erforderlich,

b) die übermittelnde zuständige Behörde stellt fest, dass im konkreten Fall keine Grundrechte und Grundfreiheiten der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,

c) die übermittelnde zuständige Behörde hält die Übermittlung an eine für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde in dem Drittland für wirkungslos oder ungeeignet, insbesondere weil die Übermittlung nicht rechtzeitig durchgeführt werden kann,

d) die für die in Artikel 1 Absatz 1 genannten Zwecke zuständige Behörde in dem Drittland wird unverzüglich unterrichtet, es sei denn, dies ist wirkungslos oder ungeeignet, und

e) die übermittelnde zuständige Behörde teilt dem Empfänger den festgelegten Zweck oder die festgelegten Zwecke mit, für die die personenbezogenen Daten nur dann durch diesen verarbeitet werden dürfen, wenn eine derartige Verarbeitung erforderlich ist.

(2) Eine internationale Übereinkunft im Sinne des Absatzes 1 ist jede in Kraft befindliche bilaterale oder multilaterale internationale Übereinkunft zwischen Mitgliedstaaten und Drittländern im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit.

(3) Die übermittelnde zuständige Behörde unterrichtet die Aufsichtsbehörde über die Übermittlungen gemäß diesem Artikel.

(4) Übermittlungen gemäß Absatz 1 werden dokumentiert.

Artikel 40

Internationale Zusammenarbeit zum Schutz personenbezogener Daten

In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Mitgliedstaaten geeignete Maßnahmen zur

a) Entwicklung von Mechanismen der internationalen Zusammenarbeit, durch die die wirksame Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtert wird,

b) gegenseitigen Leistung internationaler Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, unter anderem durch Meldungen, Beschwerdeverweisungen, Amtshilfe bei Untersuchungen und Informationsaustausch, sofern geeignete Garantien für den Schutz personenbezogener Daten und anderer Grundrechte und Grundfreiheiten bestehen,

c) Einbindung maßgeblicher Interessenträger in Diskussionen und Tätigkeiten, die zum Ausbau der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten dienen,

d) Förderung des Austausches und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten einschließlich Zuständigkeitskonflikten mit Drittländern.

KAPITEL VI

Unabhänge Aufsichtsbehörden

Abschnitt 1

Unabhängigkeit

Artikel 41

Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Richtlinie zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden „Aufsichtsbehörde").

(2) Jede Aufsichtsbehörde leistet einen Beitrag zur einheitlichen Anwendung dieser Richtlinie in der gesamten Union. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander sowie mit der Kommission gemäß Kapitel VII.

(3) Die Mitgliedstaaten können vorsehen, dass die gemäß der Verordnung (EU) 2016/679 in den Mitgliedstaaten errichtete Aufsichtsbehörde die in dieser Richtlinie genannte Aufsichtsbehörde ist und die Verantwortung für die Aufgaben der nach Absatz 1 zu errichtenden Aufsichtsbehörde übernimmt.

(4) Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedstaat die Aufsichtsbehörde, die diese Behörden im in Artikel 51 genannten Ausschuss zu vertreten hat.

Artikel 42

Unabhängigkeit

(1) Jeder Mitgliedstaat sieht vor, dass jede Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Richtlinie völlig unabhängig handelt.

(2) Die Mitgliedstaaten sehen vor, dass das Mitglied oder die Mitglieder ihrer Aufsichtsbehörden bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Richtlinie weder direkter noch indirekter Beeinflussung von außen unterliegen und dass sie weder um Weisung ersuchen noch Weisungen entgegennehmen.

(3) Die Mitglieder der Aufsichtsbehörden der Mitgliedstaaten sehen von allen mit den Aufgaben ihres Amts nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.

(4) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können.

(5) Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde ihre eigenes Personal auswählt und hat, das ausschließlich der Leitung des Mitglieds oder der Mitglieder der betreffenden Aufsichtsbehörde untersteht.

(6) Jeder Mitgliedstaaten stellt sicher, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt, und dass sie über eigene, öffentliche, jährliche Haushaltspläne verfügt, die Teil des gesamten Staatshaushalts oder nationalen Haushalts sein können.

Artikel 43

Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass jedes Mitglied ihrer Aufsichtsbehörden im Wege eines transparenten Verfahrens ernannt wird, und zwar

— vom Parlament;

— von der Regierung;

— vom Staatsoberhaupt oder

— von einer unabhängigen Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird.

(2) Jedes Mitglied muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.

(3) Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder verpflichtender Versetzung in den Ruhestand gemäß dem Recht des betroffenen Mitgliedstaats.

(4) Ein Mitglied wird seines Amtes nur enthoben, wenn es eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Erfüllung seiner Aufgaben nicht mehr erfüllt.

Artikel 44

Errichtung der Aufsichtsbehörde

(1) Jeder Mitgliedstaat sieht durch Rechtsvorschriften Folgendes vor

a) die Errichtung jeder Aufsichtsbehörde,

b) die erforderlichen Qualifikationen und sonstigen Voraussetzungen für die Ernennung zum Mitglied jeder Aufsichtsbehörde,

c) die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde,

d) die Amtszeit des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde von mindestens vier Jahren, außer für die erste Amtszeit nach dem 6. Mai 2016, die für einen Teil der Mitglieder kürzer sein kann, wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist,

e) die Frage, ob und — wenn ja — wie oft das Mitglied oder die Mitglieder jeder Aufsichtsbehörde wiederernannt werden können,

f) die Bedingungen im Hinblick auf die Pflichten des Mitglieds oder der Mitglieder und der Bediensteten jeder Aufsichtsbehörde, die Verbote von Handlungen, beruflichen Tätigkeiten und Vergütungen während und nach der Amtszeit, die mit diesen Pflichten unvereinbar sind, und die Regeln für die Beendigung des Beschäftigungsverhältnisses.

(2) Das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde sind gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. Während ihrer Amts- beziehungsweise Dienstzeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstöße gegen diese Richtlinie.

Abschnitt 2

Zuständigkeit, Aufgaben und Befugnisse

Artikel 45

Zuständigkeit

(1) Jeder Mitgliedstaat sieht vor, dass jede Aufsichtsbehörde dafür zuständig ist, im Hoheitsgebiet ihres eigenen Mitgliedstaats die ihr gemäß dieser Richtlinie zugewiesenen Aufgaben und übertragenen Befugnisse zu erfüllen bzw. auszuüben.

(2) Jeder Mitgliedstaat sieht vor, dass jede Aufsichtsbehörde nicht für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zuständig ist. Die Mitgliedstaaten können vorsehen, dass ihre Aufsichtsbehörde nicht für die Überwachung der von anderen unabhängigen Justizbehörden im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zuständig ist.

Artikel 46

Aufgaben

(1) Jeder Mitgliedstaat sieht vor, dass jede Aufsichtsbehörde in seinem Hoheitsgebiet

a) die Anwendung der nach dieser Richtlinie erlassenen Vorschriften sowie deren Durchführungsvorschriften überwacht und durchsetzt;

b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisiert und sie darüber aufklärt;

c) im Einklang mit dem Recht der Mitgliedstaaten das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung berät;

d) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Richtlinie entstehenden Pflichten sensibilisiert;

e) auf Antrag jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Richtlinie zur Verfügung stellt und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenarbeitet;

f) sich mit Beschwerden einer betroffenen Person oder einer Stelle, einer Organisation oder eines Verbandes gemäß Artikel 55 befasst, den Gegenstand der Beschwerde in angemessenem Umfang untersucht und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichtet, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

g) die Rechtmäßigkeit der Verarbeitung gemäß Artikel 17 überprüft und die betroffene Person innerhalb einer angemessenen Frist über das Ergebnis der Überprüfung gemäß Absatz 3 des genannten Artikels unterrichtet oder ihr die Gründe mitteilt, aus denen die Überprüfung nicht vorgenommen wurde;

h) mit anderen Aufsichtsbehörden zusammenarbeitet, auch durch Informationsaustausch, und ihnen Amtshilfe leistet, um die einheitliche Anwendung und Durchsetzung dieser Richtlinie zu gewährleisten;

i) Untersuchungen über die Anwendung dieser Richtlinie durchführt, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;

j) maßgebliche Entwicklungen verfolgt, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie;

k) Beratung in Bezug auf die in Artikel 28 genannten Verarbeitungsvorgänge leistet; und

l) Beiträge zur Tätigkeit des Ausschusses leistet.

(2) Jede Aufsichtsbehörde erleichtert das Einreichen von in Absatz 1 Buchstabe f genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(3) Die Erfüllung der Aufgaben jeder Aufsichtsbehörde ist für die betroffene Person und für den Datenschutzbeauftragten unentgeltlich.

(4) Bei offenkundig unbegründeten oder — besonders wegen häufiger Wiederholung — exzessiven Anträgen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage ihrer Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast dafür, dass der Antrag offensichtlich unbegründet oder exzessiv ist.

Artikel 47

Befugnisse

(1) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Untersuchungsbefugnisse verfügt. Diese Befugnisse umfassen zumindest die Befugnis, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten, die verarbeitet werden, und auf alle Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten.

(2) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Abhilfebefugnisse wie etwa die beispielhaft genannten folgenden verfügt, die es ihr gestatten,

a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die nach dieser Richtlinie erlassenen Vorschriften verstoßen;

b) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung gemäß Artikel 16;

c) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen.

(3) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde über wirksame Beratungsbefugnisse verfügt, die es ihr gestatten, gemäß dem Verfahren der vorherigen Konsultation nach Artikel 28 den Verantwortlichen zu beraten und zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Antrag Stellungnahmen an ihr nationales Parlament, ihre Regierung oder im Einklang mit seinem nationalen Recht an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten.

(4) Die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta.

(5) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass jede Aufsichtsbehörde befugt ist, Verstöße gegen nach dieser Richtlinie erlassene Vorschriften den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die nach dieser Richtlinie erlassenen Vorschriften durchzusetzen.

Artikel 48

Meldung von Verstößen

Die Mitgliedstaaten sehen vor, dass die zuständigen Behörden wirksame Vorkehrungen treffen, um vertrauliche Meldungen über Verstöße gegen diese Richtlinie zu fördern.

Artikel 49

Tätigkeitsbericht

Jede Aufsichtsbehörde erstellt einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der verhängten Sanktionen enthalten kann. Die Berichte werden dem nationalen Parlament, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden übermittelt. Sie werden der Öffentlichkeit, der Kommission und dem Ausschuss zugänglich gemacht.

KAPITEL VII

Zusammenarbeit

Artikel 50

Gegenseitige Amtshilfe

(1) Jeder Mitgliedstaat sieht vor, dass seine Aufsichtsbehörden einander maßgebliche Informationen übermitteln und Amtshilfe gewähren, um diese Richtlinie einheitlich durchzuführen und anzuwenden, und treffen Vorkehrungen für eine wirksame Zusammenarbeit. Die Amtshilfe bezieht sich insbesondere auf Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Jeder Mitgliedstaaten sieht vor, dass jede Aufsichtsbehörde alle geeigneten Maßnahmen ergreift, um dem Ersuchen einer anderen Aufsichtsbehörde unverzüglich und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Dazu kann insbesondere auch die Übermittlung maßgeblicher Informationen über die Durchführung einer Untersuchung gehören.

(3) Amtshilfeersuchen enthalten alle erforderlichen Informationen, einschließlich Zweck und Begründung des Ersuchens. Die übermittelten Informationen werden ausschließlich für den Zweck verwendet, für den sie angefordert wurden.

(4) Die ersuchte Aufsichtsbehörde lehnt das Ersuchen nur ab, wenn

a) sie für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie durchführen soll, nicht zuständig ist oder

b) ein Eingehen auf das Ersuchen gegen diese Richtlinie oder gegen das Unionsrecht verstoßen würde oder gegen das Recht des Mitgliedstaats, dem die Aufsichtsbehörde, bei der das Ersuchen eingeht, unterliegt.

(5) Die ersuchte Aufsichtsbehörde informiert die ersuchende Aufsichtsbehörde über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen, die getroffen wurden, um dem Ersuchen nachzukommen. Die ersuchte Aufsichtsbehörde erläutert gemäß Absatz 4 die Gründe für die Ablehnung des Ersuchens.

(6) Die ersuchten Aufsichtsbehörden übermitteln die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, in der Regel auf elektronischem Wege unter Verwendung eines standardisierten Formats.

(7) Ersuchte Aufsichtsbehörden verlangen für Maßnahmen, die sie aufgrund eines Amtshilfeersuchens getroffen haben, keine Gebühren. Die Aufsichtsbehörden können untereinander Regeln vereinbaren, um einander in Ausnahmefällen besondere aufgrund der Amtshilfe entstandene Ausgaben zu erstatten.

(8) Die Kommission kann im Wege von Durchführungsrechtsakten Form und Verfahren der Amtshilfe nach diesem Artikel und die Ausgestaltung des elektronischen Informationsaustauschs zwischen den Aufsichtsbehörden sowie zwischen den Aufsichtsbehörden und dem Ausschuss festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 58 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 51

Aufgaben des Ausschusses

(1) Der mit der Verordnung (EU) 2016/679 eingesetzte Europäische Ausschuss nimmt in Bezug auf Verarbeitungsvorgänge im Anwendungsbereich dieser Richtlinie folgende Aufgaben wahr:

a) Beratung der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten in der Union stehen, einschließlich etwaiger Vorschläge zur Änderung dieser Richtlinie;

b) Prüfung — von sich aus, auf Antrag eines seiner Mitglieder oder auf Ersuchen der Kommission — von die Anwendung dieser Richtlinie betreffenden Fragen und Ausarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren zwecks Sicherstellung einer einheitlichen Anwendung dieser Richtlinie;

c) Ausarbeitung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Artikel 47 Absätze 1 und 3;

d) Ausarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe b dieses Unterabsatzes für die Feststellung von Verletzungen des Schutzes personenbezogener Daten und die Festlegung der Unverzüglichkeit im Sinne des Artikels 30 Absätze 1 und 2 und für die konkreten Umstände, unter denen der Verantwortliche und der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden haben;

e) Ausarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe b dieses Absatzes in Bezug auf die Umstände, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der natürlichen Personen im Sinne des Artikels 31 Absatz 1 zur Folge hat;

f) Überprüfung der praktischen Anwendung der unter den Buchstaben b und c genannten Leitlinien, Empfehlungen und bewährten Verfahren;

g) Abgabe einer Stellungnahme gegenüber der Kommission zur Beurteilung der Angemessenheit des in einem Drittland, einem Gebiet oder einem oder mehrere spezifischen Sektoren in einem Drittland oder einer internationalen Organisation gebotenen Schutzniveaus sowie zur Beurteilung der Frage, ob ein solches Drittland, das Gebiet, der spezifische Sektor oder die internationale Organisation kein angemessenes Schutzniveau mehr gewährleistet.

h) Förderung der Zusammenarbeit und eines wirksamen bilateralen und multilateralen Austauschs von Informationen und bewährten Verfahren zwischen den Aufsichtsbehörden;

i) Förderung von Schulungsprogrammen und Erleichterung des Personalaustauschs zwischen Aufsichtsbehörden sowie gegebenenfalls mit Aufsichtsbehörden von Drittländern oder mit internationalen Organisationen;

j) Förderung des Austausches von Fachwissen und von Dokumentationen über Datenschutzrecht und -praxis mit Datenschutzaufsichtsbehörden in aller Welt.

In Bezug auf Unterabsatz 1 Buchstabe g stellt die Kommission dem Ausschuss alle erforderlichen Unterlagen zur Verfügung, darunter den Schriftwechsel mit der Regierung des Drittlandes, mit dem Gebiet oder spezifischen Sektor in diesem Drittland oder mit der internationalen Organisation.

(2) Die Kommission kann, wenn sie den Ausschuss um Rat ersucht, unter Berücksichtigung der Dringlichkeit des Sachverhalts eine Frist angeben.

(3) Der Ausschuss leitet seine Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren an die Kommission und an den in Artikel 58 Absatz 1 genannten Ausschuss weiter und veröffentlicht sie.

(4) Die Kommission setzt den Ausschuss von allen Maßnahmen in Kenntnis, die sie im Anschluss an die von ihm herausgegebenen Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren ergriffen hat.

KAPITEL VIII

Rechtsbehelfe, Haftung und Sanktionen

Artikel 52

Recht auf Beschwerde bei einer Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde hat, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die nach dieser Richtlinie erlassenen Vorschriften verstößt.

(2) Die Mitgliedstaaten sehen vor, dass eine Beschwerde, die nicht bei der gemäß Artikel 45 Absatz 1 zuständigen Aufsichtsbehörde eingereicht wird, von der Aufsichtsbehörde, bei der die Beschwerde eingelegt wird, ohne unverzüglich an die zuständige Aufsichtsbehörde übermittelt wird. Die betroffene Person wird über die Übermittlung unterrichtet.

(3) Die Mitgliedstaaten sehen vor, dass die Aufsichtsbehörde, bei der die Beschwerde eingelegt wurde, auf Ersuchen der betroffenen Person weitere Unterstützung leistet.

(4) Die betroffene Person wird von der zuständigen Aufsichtsbehörde über den Stand und das Ergebnis der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 53 unterrichtet.

Artikel 53

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

(1) Die Mitgliedstaaten sehen vor, dass jede natürliche oder juristische Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde hat.

(2) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die gemäß Artikel 45 Absatz 1 zuständige Aufsichtsbehörde sich nicht mit der Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 52 erhobenen Beschwerde in Kenntnis gesetzt hat.

(3) Die Mitgliedstaaten sehen vor, dass für Verfahren gegen eine Aufsichtsbehörde die Gerichte des Mitgliedstaats zuständig sind, in dem die Aufsichtsbehörde ihren Sitz hat.

Artikel 54

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter

Die Mitgliedstaaten sehen vor, dass jede betroffene Person unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 52 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf hat, wenn sie der Ansicht ist, dass die Rechte, die ihr aufgrund von nach dieser Richtlinie erlassenen Vorschriften zustehen, infolge einer nicht mit diesen Vorschriften im Einklang stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

Artikel 55

Vertretung von betroffenen Personen

Die Mitgliedstaaten sehen im Einklang mit dem Verfahrensrecht der Mitgliedstaaten vor, dass die betroffene Person das Recht hat, nach dem Recht eines Mitgliedstaats ordnungsgemäß gegründete Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig sind, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen und in ihrem Namen die in den Artikeln 52, 53 und 54 genannten Rechte wahrzunehmen.

Artikel 56

Recht auf Schadenersatz

Die Mitgliedstaaten sehen vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen Handlung, die gegen nach Maßgabe dieser Richtlinie erlassenen nationalen Vorschriften verstößt, ein materieller oder immaterieller Schaden entstanden ist, Recht auf Schadenersatz seitens des Verantwortlichen oder jeder sonst nach dem Recht der Mitgliedstaaten zuständigen Stelle hat.

Artikel 57

Sanktionen

Die Mitgliedstaaten legen fest, welche Sanktionen bei einem Verstoß gegen die nach dieser Richtlinie erlassenen Vorschriften zu verhängen sind, und treffen die zu deren Anwendung erforderlichen Maßnahmen. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

KAPITEL IX

Durchführungsrechtsakte

Artikel 58

Ausschussverfahren

(1) Die Kommission wird von dem mit Artikel 93 der Verordnung (EU) 2016/679 eingesetzten Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

(3) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 8 der Verordnung (EU) Nr. 182/2011 in Verbindung mit deren Artikel 5.

KAPITEL X

Schlussbestimmungen

Artikel 59

Aufhebung des Rahmenbeschlusses 2008/977/JI

(1) Der Rahmenbeschluss 2008/977/JI wird mit Wirkung vom 6. Mai 2018 aufgehoben.

(2) Verweise auf den in Absatz 1 genannten aufgehobenen Beschluss gelten als Verweise auf diese Richtlinie.

Artikel 60

Bestehende Unionsrechtsakte

Die besonderen Bestimmungen zum Schutz personenbezogener Daten in Unionsrechtsakten, die am oder vor dem 6. Mai 2016 im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit erlassenen Rechtsakten der Union enthalten sind, die die Verarbeitung im Verkehr der Mitgliedstaaten untereinander sowie den Zugang der von den Mitgliedstaaten bestimmten Behörden zu den gemäß den Verträgen errichteten Informationssystemen im Anwendungsbereich dieser Richtlinie regeln, bleiben unberührt.

Artikel 61

Verhältnis zu bereits geschlossenen internationalen Übereinkünften im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit

Internationale Übereinkünfte, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, die von den Mitgliedstaaten vor dem 6. Mai 2016 geschlossen wurden und die mit dem vor dem genannten Datum geltenden Unionsrecht vereinbar sind, bleiben in Kraft, bis sie geändert, ersetzt oder gekündigt werden.

Artikel 62

Berichte der Kommission

(1) Bis zum 6. Mai 2022 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Richtlinie vor. Die Berichte werden öffentlich gemacht.

(2) Im Rahmen der Bewertungen und Überprüfungen gemäß Absatz 1prüft die Kommission insbesondere die Anwendung und Wirkungsweise des Kapitels V über die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen und vor allem die Beschlüsse nach Artikel 36 Absatz 3 und Artikel 39.

(3) Für die in den Absätzen 1 und 2 genannten Zwecke kann die Kommission Informationen von den Mitgliedstaaten und den Aufsichtsbehörden anfordern.

(4) Bei den in den Absätzen 1 und 2 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments, des Rates sowie der anderen einschlägigen Stellen und Quellen.

(5) Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Richtlinie vor und berücksichtigt dabei insbesondere die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft.

(6) Bis zum 6. Mai 2019 überprüft die Kommission andere Rechtsakte der Union über die Verarbeitung durch die zuständigen Behörden für die in Artikel 1 Absatz 1 genannten Zwecke, einschließlich der auf der Grundlage von Artikel 60 erlassenen Rechtsakte, um festzustellen, inwieweit eine Anpassung an diese Richtlinie notwendig ist, und um gegebenenfalls die erforderlichen Vorschläge zur Änderung dieser Rechtsakte zu unterbreiten, damit ein einheitliches Vorgehen beim Schutz personenbezogener Daten innerhalb des Anwendungsbereichs dieser Richtlinie gewährleistet ist.

Artikel 63

Umsetzung

(1) Die Mitgliedstaaten erlassen und veröffentlichen bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie teilen der Kommission unverzüglich den Wortlaut dieser Vorschriften mit. Sie wenden diese Vorschriften ab dem 6. Mai 2018 an.

Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Abweichend von Absatz 1 können die Mitgliedstaaten vorsehen, dass in Ausnahmefällen, in denen dies für die vor dem 6. Mai 2016 eingerichteten automatisierten Verarbeitungssysteme mit einem unverhältnismäßigen Aufwand verbunden ist, diese bis zum 6. Mai 2023 mit Artikel 25 Absatz 1 in Einklang gebracht werden müssen.

(3) Abweichend von Absätzen 1 und 2 dieses Artikels kann ein Mitgliedstaat in außergewöhnlichen Umständen ein automatisiertes Verarbeitungssystem im Sinne des Absatzes 2 dieses Artikels innerhalb einer bestimmten Frist nach Ablauf der in Absatz 2 dieses Artikels genannten Frist mit Artikel 25 Absatz 1 in Einklang bringen, wenn hierdurch sonst schwerwiegende Schwierigkeiten für den Betrieb dieses automatisierten Verarbeitungssystems entstehen würden. Der betreffende Mitgliedstaat begründet gegenüber der Kommission, weshalb diese schwerwiegenden Schwierigkeiten entstehen würden und die Gründe für die bestimmte Frist, innerhalb derer er das automatisierte Verarbeitungssystem mit Artikel 25 Absatz 1 in Einklang bringen wird. Diese Frist muss vor dem 6. Mai 2026 enden.

(4) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten nationalen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 64

Inkrafttreten

Diese Richtlinie tritt am Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Artikel 65

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 27. April 2016.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Die Präsidentin*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

Konkordanztabelle

Konkordanztabelle: Vorentwurf DSG / Reform des Europarats / Reform der Europäischen Union

Vorentwurf DSG	**Entwurf SEV 108**[1]	**Richtlinie (EU) 2016/680**[2]	**Verordnung (EU) 2016/679**[3]
1. Abschnitt: Zweck, Geltungsbereich und Begriffe			
Art. 1: Zweck	**Art. 1**: Gegenstand und Zweck	**Art. 1**: Gegenstand und Ziele	**Art. 1**: Gegenstand und Ziele
Art. 2 Abs. 1: Geltungsbereich	**Art. 3**: Geltungsbereich	**Art. 2**: Anwendungsbereich	**Art. 2**: Sachlicher Anwendungsbereich **Art. 3**: Räumlicher Anwendungsbereich
Art. 3: Begriffe	**Art. 2**: Begriffsbestimmungen	**Art. 3**: Begriffsbestimmungen	**Art. 4**: Begriffsbestimmungen
2. Abschnitt: Allgemeine Datenschutzbestimmungen			
Art. 4: Grundsätze	**Art. 5**: Rechtmässigkeit der Datenverarbeitung und Qualität der Daten	**Art. 4**: Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten	**Art. 5**: Grundsätze für die Verarbeitung personenbezogener Daten
Art. 5: Bekanntgabe ins Ausland **Art. 5 Abs. 2**: Bekanntgabe gestützt auf die Feststellung des Bundesrates betreffend das Bestehen eines angemessenen Schutzes im Ausland **Art. 5 Abs. 3 Bst. c**: Bekanntgabe gestützt auf standardisierte Garantien	**Art. 12**: Grenzüberschreitender Verkehr personenbezogener Daten	**Art. 35**: Allgemeine Grundsätze für die Übermittlung personenbezogener Daten **Art. 36**: Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses der Kommission **Art. 37**: Datenübermittlung vorbehaltlich geeigneter Garantien	**Art. 44**: Allgemeine Grundsätze der Datenübermittlung **Art. 45**: Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses der Kommission **Art. 46**: Datenübermittlung vorbehaltlich geeigneter Garantien

[1] Vgl. Anhang und http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Version%20consolidée%20convention%20108%20modernisée%20juillet%202016.pdf.
[2] Vgl. Anhang und http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1462349959720&uri=OJ:JOL_2016_119_R_0002.
[3] Vgl. Anhang und http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1462349959720&uri=OJ:JOL_2016_119_R_0001.

Vorentwurf DSG	Entwurf SEV 108[1]	Richtlinie (EU) 2016/680[2]	Verordnung (EU) 2016/679[3]
Art. 5 Abs. 3 Bst. d: Verbindliche unternehmensinterne Datenschutzvorschriften			**Art. 47**: Verbindliche interne Datenschutzvorschriften
Art. 6: Bekanntgabe ins Ausland in Ausnahmefällen	**Art. 12 Abs. 4**: Ausnahmen	**Art. 38**: Ausnahmen für bestimmte Fälle	**Art. 49**: Ausnahmen für bestimmte Fälle
Art. 7: Auftragsdatenbearbeitung	--	**Art. 22**: Auftragsverarbeiter	**Art. 28**: Auftragsverarbeiter
Art. 8: Empfehlungen der guten Praxis	--	--	**Art. 40**: Verhaltensregeln
Art. 9: Einhaltung der Empfehlungen der guten Praxis	--	--	**Art. 24 Abs. 3**: Die Einhaltung von Verhaltensregeln kann als Gesichtspunkt für den Nachweis der Erfüllung der Pflichten des Verantwortlichen herangezogen werden. **Art. 28 Abs. 5**: Idem für den Auftragsverarbeiter. **Art. 32 Abs. 3**: Die Einhaltung von Verhaltensregeln kann als Faktor für den Nachweis der Erfüllung der Anforderungen der Sicherheit der Verarbeitung herangezogen werden. **Art. 35 Abs. 8**: Die Einhaltung von Verhaltensregeln ist bei der Folgenabschätzung zu berücksichtigen.
Art. 10: Zertifizierung	--	--	**Art. 42**: Zertifizierungsverfahren **Art. 43**: Zertifizierungsstellen

Vorentwurf DSG	Entwurf SEV 108[1]	Richtlinie (EU) 2016/680[2]	Verordnung (EU) 2016/679[3]
Art. 11: Sicherheit von Personendaten	**Art. 7 Abs. 1**: Datensicherung	**Art. 29**: Sicherheit der Verarbeitung	**Art. 32**: Sicherheit der Verarbeitung
Art. 12: Daten einer verstorbenen Person	--	--	--
3. Abschnitt: Pflichten des Verantwortlichen und des Auftragsbearbeiters			
Art. 13: Informationspflicht bei der Beschaffung von Personendaten	**Art. 7bis**: Transparenz der Datenverarbeitung	**Art. 12**: Mitteilungen und Modalitäten für die Ausübung der Rechte der betroffenen Person **Art. 13**: Der betroffenen Person zur Verfügung zu stellende oder zu erteilende Informationen **Art. 18**: Rechte der betroffenen Person in strafrechtlichen Ermittlungen und in Strafverfahren	**Art. 12**: Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person **Art. 13**: Informationspflicht bei Erhebung von Daten bei der betroffenen Person **Art. 14**: Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden
Art. 14: Ausnahmen von der Informationspflicht und Einschränkungen	**Art. 9**: Ausnahmen und Einschränkungen	**Art. 13 Abs. 3**: Einschränkung der Information	**Art. 23**: Beschränkung der Information
Art. 15: Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung	**Art. 8 Abs. 1 Bst. a**: Recht der betroffenen Person im Falle einer automatisierten Einzelentscheidung	**Art. 11**: Automatisierte Entscheidungsfindung im Einzelfall	**Art. 22**: Automatisierte Entscheidungen im Einzelfall einschliesslich Profiling
Art. 16 Abs. 1: Datenschutz-Folgenabschätzung **Art. 16 Abs. 3**: Benachrichtigung des Beauftragten über die	**Art. 8bis Abs. 2**: Pflicht des Verantwortlichen, die möglichen Auswirkungen der Datenverarbeitung zu prüfen	**Art. 27**: Datenschutz-Folgenabschätzung **Art. 28**: Vorherige Konsultation der Aufsichtsbehörde	**Art. 35**: Datenschutz-Folgenabschätzung **Art. 36**: Vorherige Konsultation der Aufsichtsbehörde

Vorentwurf DSG	**Entwurf SEV 108[1]**	**Richtlinie (EU) 2016/680[2]**	**Verordnung (EU) 2016/679[3]**
Ergebnisse			
Art. 17 Abs. 1: Meldung von Verletzungen des Datenschutzes an den Beauftragten **Art. 17 Abs. 2**: Mitteilung von Verletzungen des Datenschutzes an die betroffene Person	**Art. 7 Abs. 2**: Meldung der Verstösse gegen die Datensicherheit zumindest der Aufsichtsbehörde	**Art. 30**: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde **Art. 31**: Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person	**Art. 33**: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde **Art. 34**: Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
Art. 18: Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen	**Art. 8bis Abs. 2 und 3**: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	**Art. 20**: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	**Art. 25**: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
Art. 19: Weitere Pflichten **Art. 19 Bst. a**: Pflicht, die Datenbearbeitung zu dokumentieren **Art. 19 Bst. b**: Pflicht, die Empfänger der Daten über Berichtigungen, Löschungen oder Einschränkungen der Bearbeitung zu informieren	**Art. 8bis**: Zusätzliche Pflichten **Art. 8bis Abs. 1**: Pflicht, die Übereinstimmung der Verarbeitung mit den gesetzlichen Anforderungen darzulegen	**Art. 19**: Pflichten des Verantwortlichen **Art. 19 Abs. 1**: Pflicht, die Übereinstimmung der Verarbeitung mit den gesetzlichen Anforderungen nachzuweisen; **Art. 24**: Verzeichnis von Verarbeitungstätigkeiten **Art. 7 Abs. 3**: Pflicht, dem Empfänger die Berichtigung von Daten mitzuteilen; **Art. 16 Abs. 5**: Pflicht, die Berichtigung von unrichtigen Daten der Behörde mitzuteilen, von der die Daten stammen; **Art. 16 Abs. 6**: Pflicht,	**Art. 24**: Verantwortung des für die Verarbeitung Verantwortlichen **Art. 24 Abs. 1**: Pflicht, die Übereinstimmung der Verarbeitung mit den gesetzlichen Anforderungen nachzuweisen; **Art. 30**: Verzeichnis von Verarbeitungstätigkeiten **Art. 19**: Pflicht, dem Empfänger die Berichtigung oder Löschung von Daten oder die Einschränkung der Verarbeitung mitzuteilen

Vorentwurf DSG	Entwurf SEV 108[1]	Richtlinie (EU) 2016/680[2]	Verordnung (EU) 2016/679[3]
		den Empfänger von einer Berichtigung, Löschung oder Einschränkung der Verarbeitung in Kenntnis zu setzen	
4. Abschnitt: Rechte der betroffenen Person			
Art. 20: Auskunftsrecht	**Art. 8 Abs. 1 Bst. b und c**: Auskunftsrecht der betroffenen Person	**Art. 12**: Mitteilungen und Modalitäten für die Ausübung der Rechte der betroffenen Person **Art. 14**: Auskunftsrecht der betroffenen Person **Art. 18**: Rechte der betroffenen Person in strafrechtlichen Ermittlungen und in Strafverfahren	**Art. 12**: Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person **Art. 15**: Auskunftsrecht der betroffenen Person
Art. 21: Einschränkung des Auskunftsrechts	**Art. 9**: Ausnahmen und Einschränkungen	**Art. 15**: Einschränkung des Auskunftsrechts	**Art. 23**: Beschränkung des Auskunftsrechts
Art. 22: Einschränkung des Auskunftsrechts für Medienschaffende	--	--	**Art. 85**: Verarbeitung und Freiheit der Meinungsäusserung und Informationsfreiheit
5. Abschnitt: Besondere Bestimmungen für das Bearbeiten von Daten durch private Personen			
Art. 23: Persönlichkeitsverletzungen **Art. 23 Abs. 2 Bst. b**: Bearbeitung von Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person *(opting-out)*	-- **Art. 8 Abs. 1 Bst. d**: Widerspruchsrecht	--	-- **Art. 21**: Widerspruchsrecht
Art. 24: Rechtfertigungsgründe	--	--	--

Vorentwurf DSG	Entwurf SEV 108[1]	Richtlinie (EU) 2016/680[2]	Verordnung (EU) 2016/679[3]
Art. 25: Rechtsansprüche **Art. 25 Abs. 1 Bst. a**: Recht auf Verbot der Bearbeitung **Art. 25 Abs. 1 Bst. c**: Recht auf Berichtigung, Löschung oder Vernichtung von Daten **Art. 25 Abs. 2**: Recht auf Einschränkung der Bearbeitung	**Art. 8 Abs. 1 Bst. f**: Recht auf ein Rechtsmittel **Art. 8 Abs. 1 Bst. d**: Widerspruchsrecht **Art. 8 Abs. 1 Bst. e**: Recht auf Berichtigung oder Löschung der Daten	**Art. 16**: Recht der betroffenen Person auf Berichtigung oder Löschung **Art. 16**: Recht auf Einschränkung der Verarbeitung	**Art. 21**: Widerspruchsrecht **Art. 16**: Recht auf Berichtigung **Art. 17**: Recht auf Löschung **Art. 18**: Recht auf Einschränkung der Verarbeitung
6. Abschnitt: Besondere Bestimmungen für das Bearbeiten von Daten durch Bundesorgane			
Art. 26: Verantwortliches Organ und Kontrolle	--	**Art. 21**: Gemeinsam Verantwortliche	**Art. 26**: Gemeinsam für die Verarbeitung Verantwortliche
Art. 27: Rechtsgrundlagen	**Art. 5 Abs. 2 und 3 und Art. 6 Abs. 1**: Grundsatz der Rechtmässigkeit	**Art. 8**: Rechtmässigkeit der Verarbeitung **Art. 10**: Verarbeitung besonderer Kategorien personenbezogener Daten	**Art. 6**: Rechtmässigkeit der Verarbeitung
Art. 28: Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen	--		--
Art. 29: Bekanntgabe von Personendaten	Siehe Art. 5 Abs. 2 und 3 und Art. 6 Abs. 1	Siehe Art. 8 und 10	Siehe Art. 6
Art. 30: Widerspruch gegen die Bekanntgabe von Personendaten	**Art. 8 Abs. 1 Bst. d**: Widerspruchsrecht	--	**Art. 21 Abs. 1**: Widerspruchsrecht
Art. 31: Angebot von Unterlagen an das Bundesarchiv	**Art. 5 Abs. 4 Bst. b** : Bearbeitung zu Archivzwecken im öffentlichen	--	**Art. 89 :** Garantien und Ausnahmen in Bezug auf die

Vorentwurf DSG	Entwurf SEV 108[1]	Richtlinie (EU) 2016/680[2]	Verordnung (EU) 2016/679[3]
	Interesse		Verarbeitung zu im öffentlichen Interesse liegenden Archzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
Art. 32: Datenbearbeitung für Forschung, Planung und Statistik	**Art. 5 Abs. 4 Bst. b**	--	**Art. 89**
Art. 33: Privatrechtliche Tätigkeit von Bundesorganen	--	--	--
Art. 34: Ansprüche und Verfahren **Art. 34 Abs. 2**: Recht auf Einschränkung der Bearbeitung **Art. 34 Abs. 3 Bst. a**: Recht auf Berichtigung, Löschung oder Vernichtung von Daten	**Art. 8 Abs. 1 Bst. f**: Recht auf ein Rechtsmittel **Art. 8 Abs. 1 Bst. e**: Recht auf Berichtigung oder Löschung	**Art. 16 Abs. 3**: Recht auf Einschränkung der Verarbeitung **Art. 16 Abs. 1 und 2**: Recht auf Berichtigung und Löschung	**Art. 18**: Recht auf Einschränkung der Verarbeitung **Art. 16**: Recht auf Berichtigung **Art. 17**: Recht auf Löschung
Art. 35: Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Daten enthalten	--	--	--
Art. 36: Register	--	**Art. 24**: Verzeichnis von Verarbeitungstätigkeiten	**Art. 30**: Verzeichnis von Verarbeitungstätigkeiten
7. Abschnitt: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter bzw. -beauftragte			
Art. 37: Ernennung und Stellung	**Art. 12bis**: Einsetzung einer unabhängigen Aufsichtsbehörde	**Art. 42 Abs. 1 und 2**: Unabhängige Aufsichtsbehörde **Art. 43 Abs. 1**: Ernennung der Mitglieder der Aufsichtsbehörde **Art. 44 Abs. 1 Bst. d**: Amtszeit der Mitglieder der	**Art. 52 Abs. 1 und 2**: Unabhängige Aufsichtsbehörde **Art. 53 Abs. 1**: Ernennung der Mitglieder der Aufsichtsbehörde **Art. 54 Abs. 1 Bst. d**: Amtszeit der Mitglieder der

Vorentwurf DSG	Entwurf SEV 108[1]	Richtlinie (EU) 2016/680[2]	Verordnung (EU) 2016/679[3]
		Aufsichtsbehörde	Aufsichtsbehörde
Art. 38: Wiederwahl und Beendigung der Amtsdauer	--	**Art. 44 Abs. 1 Bst. e**: Wiederernennung der Mitglieder der Aufsichtsbehörde	**Art. 54 Abs. 1 Bst. e**: Wiederernennung der Mitglieder der Aufsichtsbehörde
Art. 39: Nebenbeschäftigung	--	**Art. 42 Abs. 3**: Verbot unvereinbarer entgeltlicher oder unentgeltlicher Tätigkeit	**Art. 52 Abs. 3**: Verbot unvereinbarer entgeltlicher oder unentgeltlicher Tätigkeit
Art. 40: Aufsicht	**Art. 12bis Abs. 1 und 9**: Aufsichtsbehörde	**Art. 41 und 45 Abs. 2**: Aufsichtsbehörde	**Art. 41 und Art. 55 Abs. 3**: Aufsichtsbehörde
Art. 41: Untersuchung	**Art. 12bis Abs. 2 Bst. a**: Ermittlungs- und Einschreitungsbefugnisse der Aufsichtsbehörde	**Art. 47 Abs. 1**: Untersuchungsbefugnisse der Aufsichtsbehörde	**Art. 58 Abs. 1**: Untersuchungsbefugnisse der Aufsichtsbehörde
Art. 42: Vorsorgliche Massnahmen	**Art. 12bis Abs. 2 Bst. a**: Einschreitungsbefugnisse der Aufsichtsbehörde **Art. 12 Abs. 6**: Befugnis, Datenweitergaben ins Ausland auszusetzen	**Art. 47 Abs. 2**: Abhilfebefugnisse	**Art. 58 Abs. 2**: Abhilfebefugnisse
Art. 43: Verwaltungsmassnahmen	**Art. 12bis Abs. 2**: Einschreitungs-, Ermittlungs- und Klagebefugnis **Art. 12bis Abs. 2 Bst. c**: Befugnis, Entscheidungen und verwaltungsrechtliche Sanktionen zu erlassen **Art. 12 Abs. 6**: Befugnis, Datenweitergaben ins Ausland zu verbieten oder auszusetzen	**Art. 47 Abs. 2**: Abhilfebefugnisse	**Art. 58 Abs. 2**: Abhilfebefugnisse

Vorentwurf DSG	Entwurf SEV 108[1]	Richtlinie (EU) 2016/680[2]	Verordnung (EU) 2016/679[3]
Art. 44: Verfahren	--	--	--
Art. 45: Anzeigepflicht	**Art. 12bis Abs. 1 Bst. d**: Anzeigebefugnis der Aufsichtsbehörde	**Art. 47 Abs. 5**: Anzeigebefugnis der Aufsichtsbehörde	**Art. 58 Abs. 5**: Anzeigebefugnis der Aufsichtsbehörde
Art. 46: Amtshilfe zwischen schweizerischen Behörden	--	--	--
Art. 47: Amtshilfe zwischen schweizerischen und ausländischen Behörden	**Art. 12bis Abs. 7, 7bis und 8**: Zusammenarbeit zwischen Aufsichtsbehörden	**Art. 50**: Gegenseitige Amtshilfe	**Art. 61**: Gegenseitige Amtshilfe
Art. 48: Information	**Art. 12bis Abs. 5bis**: Pflicht der Aufsichtsbehörde, periodisch einen Tätigkeitsbericht zu erstellen	**Art. 49**: Tätigkeitsbericht	**Art. 59**: Tätigkeitsbericht
Art. 49: Weitere Aufgaben	**Art. 12bis Abs. 2 Bst. b**: Zulassung von Standardsicherheiten **Art. 12bis Abs. 2 Bst. e**: Sensibilisierung der Öffentlichkeit und der für die Verarbeitung Verantwortlichen **Art. 14 Abs. 1**: Unterstützung von Betroffenen	**Art. 46 Abs. 1**: insbesondere Aufgaben der Sensibilisierung, der Beratung der Verantwortlichen, der Unterstützung der betroffenen Personen	**Art. 57 Abs. 1**: insbesondere Aufgaben der Sensibilisierung, der Beratung der Verantwortlichen, der Unterstützung der betroffenen Personen
8. Abschnitt: Strafbestimmungen			
Art. 50: Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten	**Art. 10**: Sanktionen und Rechtsmittel	**Art. 57**: Sanktionen	**Art. 84**: Sanktionen
Art. 51: Verletzung der	**Art. 10**: Sanktionen und	**Art. 57**: Sanktionen	**Art. 84**: Sanktionen

Vorentwurf DSG	Entwurf SEV 108[1]	Richtlinie (EU) 2016/680[2]	Verordnung (EU) 2016/679[3]
Sorgfaltspflichten	Rechtsmittel		
Art. 52: Verletzung der beruflichen Schweigepflicht	**Art. 10**: Sanktionen und Rechtsmittel	**Art. 57**: Sanktionen	**Art. 84**: Sanktionen
Art. 53: Übertretungen in Geschäftsbetrieben	**Art. 10**: Sanktionen und Rechtsmittel	**Art. 57**: Sanktionen	**Art. 84**: Sanktionen
Art. 54: Anwendbares Recht und Verfahren	--	--	--
Art. 55: Verfolgungsverjährung für Übertretungen	--	--	--
9. Abschnitt: Abschluss von Staatsverträgen			
Art. 56: Abschluss von Staatsverträgen	--	--	--
10. Abschnitt: Schlussbestimmungen			
Art. 57: Vollzug durch die Kantone	--	--	--
Art. 58: Aufhebung und Änderung anderer Erlasse			
Art. 59: Übergangsbestimmung	--		
Art. 60: Referendum und Inkrafttreten	--	--	--

Brief Bundesverwaltung

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bern, 21. Dezember 2016

Adressaten:
die politischen Parteien
die Dachverbände der Gemeinden, Städte und Berggebiete
die interessierten Kreise

Eröffnung des Vernehmlassungsverfahrens:

- **Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz**
- **Bundesbeschluss über die Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen**
- **Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten**

Sehr geehrte Damen und Herren

Der Bundesrat hat am 21. Dezember 2016 das Eidgenössische Justiz- und Polizeidepartement (EJPD) beauftragt, zu den drei im Betreff genannten Erlassen ein Vernehmlassungsverfahren durchzuführen.

Die Vernehmlassungsfrist dauert bis am 4. April 2017.

Zur Vernehmlassung unterbreitet wird erstens Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (im Folgenden «VE»). Er geht zurück auf den mit Beschluss vom 1. April 2015 erteilten Auftrag des Bundesrates an das EJPD, unter Berücksichtigung der Reformen in Europa einen Vorentwurf zur Revision der Datenschutzgesetzgebung des Bundes zu erarbeiten. Der VE umfasst die Totalrevision des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz[1] (im Folgenden «VE-DSG») sowie die Teilrevision bestimmter Bundesgesetze.

Ziel des VE ist es, den Datenschutz zu verbessern, insbesondere indem die Datenbearbeitung transparenter gestaltet wird, die betroffenen Personen mehr Kontrolle über ihre Daten erhalten und die Pflichten der Verantwortlichen ausgebaut werden. Die staatlichen Eingriffe werden jedoch auf ein absolutes Minimum begrenzt. Die Absicht ist vielmehr, das Verantwortungsbewusstsein der privaten Personen, die Daten bearbeiten, zu fördern und diese zur Einhaltung nicht verbindlicher Instrumente zu

[1] SR 235.1

ermutigen. Der VE dient ausserdem dazu, durch die Gewährleistung eines Datenschutzniveaus, das den europäischen Anforderungen entspricht, den grenzüberschreitenden Datenverkehr zu erleichtern. Schliesslich erhält der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte durch den VE Verfügungskompetenzen und damit umfassendere Aufsichtsbefugnisse.

Der Bundesbeschluss zur Genehmigung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen (im Folgenden «Richtlinie [EU] 2016/680») bildet den zweiten Erlass, der hiermit zur Vernehmlassung unterbreitet wird. Am 27. April 2016 hat die Europäische Union eine Reform ihrer Datenschutzgesetzgebung verabschiedet, die zwei Erlasse umfasst. Dabei handelt es sich zum einen um die Grundverordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (im Folgenden «Verordnung [EU] 2016/679»)[2], zum anderen um die erwähnte Richtlinie (EU) 2016/680. Gemäss der Europäischen Union stellt für die Schweiz ausschliesslich die Richtlinie (EU) 2016/680 eine Weiterentwicklung des Schengen-Besitzstands dar. Gemäss dem Schengen-Assoziierungsabkommen ist die Schweiz verpflichtet, die Anforderungen dieses Erlasses innerhalb von zwei Jahren ab der Notifikation durch die Europäische Union, die am 1. August 2016 erfolgt ist, in ihre innerstaatliche Rechtsordnung umzusetzen.

Ende des ersten Halbjahrs 2016 hat der vom Ministerkomitee des Europarates eingesetzte Ad-hoc-Ausschuss seine Arbeiten zur Revision des Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[3] (im Folgenden «Übereinkommen SEV 108») und des entsprechenden Zusatzprotokolls vom 8. November 2001[4] abgeschlossen. Das Änderungsprotokoll betreffend den Entwurf zur Revision des Übereinkommens SEV 108 sollte grundsätzlich anfangs nächstes Jahr verabschiedet werden. Dessen Inhalt entspricht grösstenteils dem obenerwähnten Reformvorhaben der Europäischen Union, ist aber weniger detailliert als letzteres. Der Wortlaut dieses Erlasses ist grundsätzlich definitiv. Um nicht innerhalb weniger Monate zwei verschiedene Vernehmlassungen zum selben Thema durchzuführen, hat der Bundesrat beschlossen, das revidierte Übereinkommen SEV 108 und den Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz gleichzeitig in die Vernehmlassung zu geben. Für den Genehmigungsbeschluss zu dessen Ratifikation sollte keine weitere Vernehmlassung erforderlich sein. Der Bund sieht dementsprechend vor, die Anforderungen der Richtlinie (EU) 2016/680 sowie des Entwurfs zur Revision des Übereinkommens SEV 108 im Rahmen desselben Gesetzgebungsverfahrens umzusetzen. Mit dem VE können die Anforderungen beider Erlasse erfüllt werden, ohne darüber hinauszugehen. Durch die Vorlage erfolgt auch eine Annäherung an die Anforderungen der Verordnung

[2] Unter folgendem Link abrufbar: http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679.
[3] SR 0.235.1
[4] Sr 235.11

(EU) 2016/679. So sollte die Schweiz in der Lage sein, im Bereich des Datenschutzes eine Bundesgesetzgebung in Einklang mit den europäischen Anforderungen beizubehalten und von der europäischen Union weiterhin als Drittstaat mit einem angemessen Datenschuztzniveau anerkannt werden.

Die Vorlage, die Vernehmlassungsunterlagen sowie die Ergebnisse der Regulierungsfolgenabschätzung können über folgende Internetadresse bezogen werden : http://www.admin.ch/ch/d/gg/pc/pendent.html.

Wir sind bestrebt, die Dokumente im Sinne des Behindertengleichstellungsgesetzes[5] barrierefrei zu publizieren.

Wir bitten Sie für die Vernehmlassung **das elektronische Formular** zu verwenden, das Sie unter der obenstehenden Internetadresse herunterladen können. Wir ersuchen Sie, Ihre Stellungnahmen innert der Vernehmlassungsfrist, elektronisch (**ausschliesslich als Word-Datei**) an folgende E-Mail-Adresse zu senden:

jonas.amstutz@bj.admin.ch

Für Rückfragen und allfällige Informationen stehen Ihnen
Frau Camille Dubois (Tel. 058 462 41 44; camille.dubois@bj.admin.ch),
Frau Bettina Bacher (Tel. 058 466 18 07; bettina.bacher@bj.admin.ch) und
Frau Simone Füzesséry (Tel. 058 462 47 59; simone.fuzessery@bj.admin.ch) zur Verfügung.

Freundliche Grüsse

Simonetta Sommaruga
Bundesrätin

[5] SR 151.3

Liste der Vernehmlassungsadressaten
Liste des destinataires consultés
Elenco dei destinatari della consultazione

Art. 4 Abs. 3 Vernehmlassungsgesetz (SR 172.061)

1. Tribunaux fédéraux

Bundesgericht - BGer	1000 Lausanne 14 direktion@bger.ch
Bundesverwaltungsgericht - BVger	Kreuzackerstrasse 12 9023 St. Gallen behoerden@bvger.admin.ch
Bundesstrafgericht - BStGer	Postfach 2720 6501 Bellinzona Info@bstger.ch
Bundespatentgericht - BPatGer	St. Leonhardstrasse 49 9001 St. Gallen Kanzlei@bpatger.ch

2. Kantone / Cantons / Cantoni

Staatskanzlei des Kantons Zürich	Neumühlequai 10 8090 Zürich staatskanzlei@sk.zh.ch
Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8 info@sta.be.ch
Staatskanzlei des Kantons Luzern	Bahnhofstrasse 15 6002 Luzern staatskanzlei@lu.ch
Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf ds.la@ur.ch
Staatskanzlei des Kantons Schwyz	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz stk@sz.ch
Staatskanzlei des Kantons Obwalden	Rathaus 6061 Sarnen staatskanzlei@ow.ch
Staatskanzlei des Kantons Nidwalden	Dorfplatz 2 Postfach 1246 6371 Stans staatskanzlei@nw.ch

Staatskanzlei des Kantons Glarus	Rathaus 8750 Glarus staatskanzlei@gl.ch
Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug info@zg.ch
Chancellerie d'Etat du Canton de Fribourg	Rue des Chanoines 17 1701 Fribourg chancellerie@fr.ch relations.exterieures@fr.ch
Staatskanzlei des Kantons Solothurn	Rathaus Barfüssergasse 24 4509 Solothurn kanzlei@sk.so.ch
Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel staatskanzlei@bs.ch
Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal landeskanzlei@bl.ch
Staatskanzlei des Kantons Schaffhausen	Beckenstube 7 8200 Schaffhausen staatskanzlei@ktsh.ch
Kantonskanzlei des Kantons Appenzell Ausserrhoden	Regierungsgebäude 9102 Herisau Kantonskanzlei@ar.ch
Ratskanzlei des Kantons Appenzell Innerrhoden	Marktgasse 2 9050 Appenzell info@rk.ai.ch
Staatskanzlei des Kantons St. Gallen	Regierungsgebäude 9001 St. Gallen info.sk@sg.ch
Standeskanzlei des Kantons Graubünden	Reichsgasse 35 7001 Chur info@gr.ch
Staatskanzlei des Kantons Aargau	Regierungsgebäude 5001 Aarau staatskanzlei@ag.ch

Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld staatskanzlei@tg.ch
Cancelleria dello Stato del Cantone Ticino	Palazzo delle Orsoline 6501 Bellinzona can-scds@ti.ch
Chancellerie d'Etat du Canton de Vaud	Place du Château 4 1014 Lausanne info.chancellerie@vd.ch
Chancellerie d'Etat du Canton du Valais	Planta 3 1950 Sion Chancellerie@admin.vs.ch
Chancellerie d'Etat du Canton de Neuchâtel	Le Château Rue de la Collégiale 12 2000 Neuchâtel Secretariat.chancellerie@ne.ch
Chancellerie d'Etat du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3 service-adm.ce@etat.ge.ch
Chancellerie d'Etat du Canton du Jura	2, rue de l'Hôpital 2800 Delémont chancellerie@jura.ch
Konferenz der Kantonsregierungen (KdK) Conférence des gouvernements cantonaux (CdC) Conferenza dei Governi cantonali (CdC)	Sekretariat Haus der Kantone Speichergasse 6 Postfach 3001 Bern mail@kdk.ch

3. In der Bundesversammlung vertretene politische Parteien / partis politiques représentés à l'Assemblée fédérale / partiti rappresentati nell' Assemblea federale

Bürgerlich-Demokratische Partei BDP Parti bourgeois-démocratique PBD Partito borghese democratico PBD	Postfach 119 3000 Bern 6 mail@bdp.info

Christlichdemokratische Volkspartei CVP Parti démocrate-chrétien PDC Partito popolare democratico PPD	Generalsekretariat Klaraweg 6 Postfach 3001 Bern info@cvp.ch
Christlich-soziale Partei Obwalden csp-ow	Frau Linda Hofmann St. Antonistrasse 9 6060 Sarnen ch.schaeli@gmx.net
Christlichsoziale Volkspartei Oberwallis	Geschäftsstelle Postfach 132 3930 Visp info@cspo.ch
Evangelische Volkspartei der Schweiz EVP Parti évangélique suisse PEV Partito evangelico svizzero PEV	Nägeligasse 9 Postfach 3001 Bern vernehmlassungen@evppev.ch
FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLR.I Liberali Radicali	Generalsekretariat Neuengasse 20 Postfach 3001 Bern jean-richard@fdp.ch hofer@fdp.ch
Grüne Partei der Schweiz GPS Parti écologiste suisse PES Partito ecologista svizzero PES	Waisenhausplatz 21 3011 Bern gruene@gruene.ch
Grünliberale Partei glp Parti vert'libéral pvl	Laupenstrasse 2 3008 Bern schweiz@grunliberale.ch
Lega dei Ticinesi (Lega)	Via Monte Boglia 3 Case postale 4562 6904 Lugano lorenzo.quadri@mattino.ch
Mouvement Citoyens Romand (MCR)	Case postale 1211 Genève 17 info@mcge.ch
Partei der Arbeit PDA Parti suisse du travail PST	Postfach 8640 8026 Zürich pdaz@pda.ch
Schweizerische Volkspartei SVP Union Démocratique du Centre UDC Unione Democratica di Centro UDC	Generalsekretariat Postfach 8252 3001 Bern info@svp.ch

Sozialdemokratische Partei der Schweiz SPS Parti socialiste suisse PSS Partito socialista svizzero PSS	Zentralsekretariat Spitalgasse 34 Postfach 3001 Bern verena.loembe@spschweiz.ch

4. Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete / associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national / associazioni mantello nazionali dei Comuni delle città e delle regioni di montagna

Schweizerischer Gemeindeverband	Laupenstrasse 35 3001 Bern verband@chgemeinden.ch
Schweizerischer Städteverband	Monbijoustrasse 8 Postfach 3001 Bern info@staedteverband.ch
Schweizerische Arbeitsgemeinschaft für die Berggebiete	Seilerstrasse 4 Postfach 3001 Bern info@sab.ch

5. Gesamtschweizerische Dachverbände der Wirtschaft / associations faîtières de l'économie qui œuvrent au niveau national / associazioni mantello nazionali dell'economia

economiesuisse Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere Swiss business federation	Hegibachstrasse 47 Postfach 8032 Zürich info@economiesuisse.ch bern@economiesuisse.ch
Schweizerischer Gewerbeverband (SGV) Union suisse des arts et métiers (USAM) Unione svizzera delle arti e mestieri (USAM)	Schwarztorstrasse 26 Postfach 3001 Bern info@sgv-usam.ch
Schweizerischer Arbeitgeberverband Union patronale suisse Unione svizzera degli imprenditori	Hegibachstrasse 47 Postfach 8032 Zürich verband@arbeitgeber.ch

Schweiz. Bauernverband (SBV) Union suisse des paysans (USP) Unione svizzera dei contadini (USC)	Laurstrasse 10 5201 Brugg info@sbv-usp.ch
Schweizerische Bankiervereinigung (SBV) Association suisse des banquiers (ASB) Associazione svizzera dei banchieri (ASB) Swiss Bankers Association	Postfach 4182 4002 Basel office@sba.ch
Schweiz. Gewerkschaftsbund (SGB) Union syndicale suisse (USS) Unione sindacale svizzera (USS)	Monbijoustrasse 61 Postfach 3000 Bern 23 info@sgb.ch
Kaufmännischer Verband Schweiz Société suisse des employés de commerce Società svizzera degli impiegati di commercio	Hans-Huber-Strasse 4 Postfach 1853 8027 Zürich stephan.alexander@kfmv.ch manuel.Keller@kfmv.ch
Travail.Suisse	Hopfenweg 21 Postfach 5775 3001 Bern info@travailsuisse.ch

6. Im Einzelfall interessierte ausserparlamentarische Kommissionen und weitere Kreise / Autres milieux et commissions extraparlementaires concernés par le projet dans le cas d'espèce / altri ambienti e commissioni extraparlamentari interessati nel singolo caso

Privatim, l'association des commissaires suisses à la protection des données	Henric Petri-Strasse 15 Postfach 205 4010 Basel beat.rudin@dsb.bs.ch
Verein Unternehmens-Datenschutz VUD	Verein Unternehmens-Datenschutz VUD c/o IT & Law Consulting GmbH Grafenaustrasse 5, 6300 Zug info@vud.ch
Fédération romande des consommateurs	Rue de Genève 17 CP 6151 1002 Lausanne info@frc.ch
Comité international de la Croix-Rouge	19 Avenue de la paix 1202 Genève mmarelli@icrc.org

Associazione consumatrici e consumatori della Svizzera italiana ASCI	Strada di Pregassona 33 6963 Pregassona info@asci.ch
Schweizerisches Konsumentenforum kf	Geschäftsstelle Konsumentenforum kf Belpstrasse 11 3007 Bern forum@konsum.ch
Stiftung für Konsumentenschutz SKS	Monbijoustrasse 61 Postfach 3000 Bern 23 info@konsumentenschutz.ch
Commission fédérale de la consommation CFC	Bundeshaus Ost 3003 Bern konsum@gs-wbf.admin.ch