Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

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

Oktober 2018

Erläuternder Bericht zum Bundesgesetz über die Umsetzung 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)

Inhaltsverzeichnis

1 Ausgangslage

Am 15. September 2017 hat der Bundesrat die Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz[1] verabschiedet. Ziel der Vorlage ist insbesondere:

- die Anforderungen 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 (Richtlinie [EU] 2016/680)[2] als Weiterentwicklung des Schengen-Besitzstands umzusetzen;[3]
- die Empfehlungen der Europäischen Union aufgrund der Evaluierung der Schweiz im Jahr 2014 im Rahmen der Schengen-Assoziierungsabkommen umzusetzen;[4]
- das Bundesrecht an die Anforderungen der Verordnung (EU) 2016/679 anzunähern;[5]
- die Anforderungen des Entwurfs zur Revision des Übereinkommens SEV 108 des Europarates[6] («E-SEV 108») zu übernehmen.[7]

Im Rahmen der parlamentarischen Beratung hat das Parlament entschieden, die Vorlage zur Totalrevision des DSG in zwei Teile aufzuspalten und in einem ersten Schritt die Änderungen zu behandeln, die für die Übernahme des Schengen-Besitzstands erforderlich sind. Nach diesem Entscheid hat es am 28. September 2018 das Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 verabschiedet. Der Erlass besteht einerseits aus dem Schengen-Datenschutzgesetz (SDSG). Andererseits ändert er die im Bereich der Schengener Zusammenarbeit in Strafsachen anwendbaren Gesetze, insbesondere das Strafgesetzbuch (StGB)[8], die Strafprozessordnung vom 5. Oktober 2007[9] (StPO), das Bundesgesetz vom 20. März 1981[10] über internationale Rechtshilfe in Strafsachen (IRSG), das Bundesgesetz vom 22. Juni 2001[11] über die Zusammenarbeit mit dem Internationalen Strafgerichtshof (ZISG), das Bundesgesetz vom 7. Oktober 1994[12] über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten (ZentG), das Bundesgesetz vom 13. Juni 2008[13] über die polizeilichen Informationssysteme des Bundes (BPI) und das Bundesgesetz vom 12. Juni 2009[14] über den Informationsaustausch zwischen den Strafverfolgungsbehörden des Bundes und denjenigen der anderen Schengen-Staaten (SIaG).

---

1 BBl **2017** 6941

2 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.

3 BBl **2017** 6989

4 BBl **2017** 6965

5 BBl **2017** 6996; 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), Fassung gemäss ABl. L 119 vom 4.5.2016, S. 1.

6 Entwurf zur Revision des Übereinkommens des Europarates SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

7 BBl **2017** 6993

8 SR **311.0**

9 SR **312.0**

10 SR **351.1**

11 SR **351.6**

12 SR **360**

13 SR **361**

14 SR **362.2**

Was die Totalrevision des DSG betrifft, schreiten die Arbeiten im Parlament voran. Um Doppelspurigkeiten mit dem künftigen DSG zu vermeiden, ist vorgesehen, das SDSG aufzuheben, sobald das Parlament die Totalrevision des DSG verabschiedet hat.

2 Erläuterungen zu den Bestimmungen des SDSG

2.1 Ingress

Das SDSG stützt sich auf folgende Bestimmungen der Bundesverfassung (BV)[15]: Artikel 54 Absatz 1, nach welchem dem Bund eine Gesetzgebungskompetenz in auswärtigen Angelegenheiten zukommt, Artikel 123, wonach ihm eine Gesetzgebungskompetenz in Strafsachen zusteht, und Artikel 173 Absatz 2, welcher der Bundesversammlung eine subsidiäre Kompetenz für Geschäfte verleiht, die in die Zuständigkeit des Bundes fallen und keiner anderen Bundesbehörde zugewiesen sind.

Das SDSG hat zum Ziel, die Richtlinie (EU) 2016/680, bei welcher es sich für die Schweiz um eine Weiterentwicklung des Schengen-Besitzstands handelt, umzusetzen. Diese Richtlinie enthält gemäss ihrem Artikel 1 Absatz 1 «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».

Die Richtlinie (EU) 2016/680 ersetzt den Rahmenbeschluss 2008/977/JI[16]. Dieser Rahmenbeschluss hat für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen gewisse Datenschutzgrundsätze aufgestellt, welche allerdings nur für den Datenaustausch zwischen Schengen-Staaten gelten (Erwägungsgrund 6). Gemäss Erwägungsgrund 7 der Richtlinie (EU) 2016/680 erachtet es der europäische Gesetzgeber für eine wirksame polizeiliche und justizielle Zusammenarbeit in Strafsachen als entscheidend, ein einheitliches und hohes Datenschutzniveau zu gewährleisten und den Austausch von Personendaten zwischen den zuständigen Behörden der Schengen-Staaten zu erleichtern. Es soll dafür gesorgt werden, dass die Privatsphäre der betroffenen Personen bei der Datenbearbeitung durch die zuständigen Behörden 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, in allen Schengen-Staaten gleichwertig geschützt wird (Erwägungsgrund 7).

2.2 Allgemeine Bestimmungen

Art. 1 Gegenstand

Abs. 1 Einleitungssatz

Absatz 1 übernimmt den Wortlaut von Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 mit zwei Unterschieden. Anders als in der Richtlinie (EU) 2016/680 werden – wie nach geltendem DSG – sowohl die Grundrechte von natürlichen Personen als auch von juristischen Personen geschützt. Der zweite Unterschied ist redaktioneller Natur: Das SDSG ersetzt die Begriffe der «Ermittlung» und «Aufdeckung» durch den Ausdruck der «Aufklärung» von Straftaten, da sich die ersten beiden Begriffe nicht klar voneinander abgrenzen lassen.

---

15 SR **101**

16 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. 350 vom 30.12.2008, S. 60.

Bundesorgane, auf welche das SDSG Anwendung findet

Die dem SDSG zu unterstellenden Bundesorgane bestimmen sich mit Blick auf die Legaldefinition der «zuständigen Behörden» nach Artikel 3 Ziffer 7 der Richtlinie (EU) 2016/680. Gemäss dieser Bestimmung und dem Erwägungsgrund 11 der Richtlinie handelt es sich dabei einerseits um die entsprechenden staatlichen Stellen wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden (Bst. a) sowie andererseits um alle anderen Stellen oder Einrichtungen, denen durch das Recht eines Schengen-Mitgliedstaats die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke der Richtlinie (EU) 2016/680 übertragen worden ist (Bst. b). Das SDSG findet deshalb hauptsächlich Anwendung auf die Strafbehörden des Bundes und die für die internationale Rechtshilfe in Strafsachen zuständigen Bundesbehörden. Nach dem Erwägungsgrund 80 der Richtlinie (EU) 2016/680 gilt diese – unter Vorbehalt gewisser Bestimmungen – auch für Datenbearbeitungen der nationalen Gerichte und anderer Justizbehörden im Rahmen ihrer justiziellen Tätigkeit. Zu den betreffenden Bundesorganen gehören also nicht nur das Bundesamt für Polizei (fedpol), das BJ im Bereich der internationalen Rechtshilfe in Strafsachen und die Bundesanwaltschaft, sondern auch das Bundesstrafgericht, das Bundesgericht und die kantonalen Zwangsmassnahmengerichte, wenn sie für den Bund tätig werden (vgl. Art. 2 Abs. 2 des Bundesgesetzes vom 19. März 2010[17] über die Organisation der Strafbehörden des Bundes [StBOG]).

Dagegen findet das SDSG keine Anwendung auf kantonale Behörden. Zwar ist die Richtlinie (EU) 2016/680 auch für die Kantone verbindlich. Es obliegt jedoch den kantonalen Gesetzgebern, die neuen Anforderungen der Europäischen Union wenn nötig in ihre Gesetzgebung zu übertragen.[18]

Datenbearbeitungen, auf welche das SDSG Anwendung findet

Im Einleitungssatz von Artikel 1 Absatz 1 wird der Zweck der Datenbearbeitungen, die in den Anwendungsbereich des SDSG fallen, gleich umschrieben wie in der Richtlinie (EU) 2016/680 (unter Vorbehalt der vorne erläuterten Abweichungen). Gemäss dem Erwägungsgrund 12 der Richtlinie (EU) 2016/680 sind die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet, wobei auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht, dazu zählen. Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen (zum Beispiel bei Demonstrationen). Sie umfassen auch die Aufrechterhaltung der öffentlichen Ordnung, soweit diese Aufgabe der Polizei oder anderen Strafverfolgungsbehörden zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit, die zu einer Straftat führen können, übertragen worden ist. Nicht von der Richtlinie (EU) 2016/680 erfasst werden dagegen Tätigkeiten, welche die nationale Sicherheit betreffen, oder Tätigkeiten von Agenturen und Stellen, die mit Fragen der nationalen Sicherheit befasst sind (Erwägungsgrund 14).

Vor diesem Hintergrund findet das SDSG auf Bundesebene beispielsweise auf Datenbearbeitungen in den folgenden Bereichen Anwendung: bei der Erfüllung der gesetzlichen Aufgaben des BJ im Rahmen der internationalen Rechtshilfe in Strafsachen, bei Tätigkeiten des Direktionsbereichs der internationalen Polizeikooperation von fedpol, bei Ermittlungen der Bundeskriminalpolizei in den Zuständigkeitsbereichen des Bundes oder beim kriminalpolizeilichen Informationsaustausch mit den Strafverfolgungsbehörden anderer Staaten oder internationale Organe wie INTERPOL und Europol, namentlich im Zusammenhang mit organisierter Kriminalität, Menschenhandel und Menschenschmuggel, Pädokriminalität und strafbarer Pornografie, Internetkriminalität, Betäubungsmitteln, illegalem Handel mit Kulturgütern

[17] SR **173.71**

[18] BBl **2017** 7180

sowie Falschgeld. Auch Tätigkeiten der Bundesanwaltschaft fallen in den Anwendungsbereich des SDSG, nämlich die Verfolgung von Straftaten gemäss den Artikeln 23 und 24 StPO sowie anderer Bundesgesetze.

Datenbearbeitungen durch den Nachrichtendienst des Bundes werden vom SDSG indessen nicht erfasst (Erwägungsgrund 14 der Richtlinie [EU] 2016/680). Dasselbe gilt für Datenbearbeitungen in den anderen Bereichen der Schengen-Zusammenarbeit (namentlich Visa, Grenzkontrollen und Waffen), die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen und folglich vom SDSG nicht erfasst sind.

Abs. 1 Bst. a

Das SDSG gilt für die Bearbeitung von Personendaten durch Bundesorgane in Strafsachen im Rahmen der Anwendung des Schengen-Besitzstands. Der Begriff des Schengen-Besitzstands leitet sich aus dem Schengen-Assoziierungsabkommen (SAA)[19] ab: Dabei geht es vorliegend um die in den Anhängen A und B aufgeführten Bestimmungen sowie sämtliche Weiterentwicklungen, welche die Schweiz aufgrund von Artikel 2 Absatz 3 SAA namentlich in Bezug auf den Austausch von Informationen und Personendaten im Bereich der polizeilichen Zusammenarbeit und der Rechtshilfe in Strafsachen akzeptieren, umsetzen und anwenden muss.

Wenn Bundesorgane im Rahmen der Anwendung der Bestimmungen des Schengen-Besitzstands Personendaten für die Zwecke nach Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 bearbeiten, so müssen sie die Daten gemäss den Datenschutzstandards dieser Richtlinie behandeln und folglich das SDSG anwenden. Die Daten geniessen gewissermassen einen besonderen Schutz, wenn die zuständigen Bundesorgane ihre gesetzlichen Aufgaben erfüllen. Als «Schengen»-Daten werden dabei nicht nur die Daten qualifiziert, welche die Bundesorgane über die Kommunikationskanäle des SIRENE-Büros von einem Schengen-Staat erhalten, sondern auch diejenigen Daten, welche die Bundesorgane in einem Informationssystem bearbeiten oder abfragen, das auf der Grundlage eines Rechtsakts des Schengen-Besitzstands errichtet worden ist. Dies ist zum Beispiel der Fall, wenn sie Daten im Schengener Informationssystem (Art. 16 BPI) bearbeiten oder wenn fedpol oder die Bundesanwaltschaft das Visa-Informationssystem (VIS) nach Artikel 109*a* des Bundesgesetzes vom 16. Dezember 2005[20] über die Ausländerinnen und Ausländer abfragen.

Das SDSG wird auch bei künftigen Schengen-Weiterentwicklungen gelten, sobald die Schweiz diese übernommen hat.

Abs. 1 Bst. b

Das SDSG regelt auch die Bearbeitung von Personendaten in Strafsachen im Rahmen der Anwendung internationaler Verträge, wenn diese mit der Europäischen Union oder mit Schengen-Staaten abgeschlossen worden sind und bezüglich des Datenschutzes auf die Richtlinie (EU) 2016/680 verweisen. Diese Bestimmung bezieht sich auf Verträge, die zwar keine Weiterentwicklung des Schengen-Besitzstands darstellen, aber in denen die Richtlinie (EU) 2016/680 als anwendbar erklärt wird. Von Absatz 1 Buchstabe b erfasst sind ausschliesslich Staatsverträge zwischen der Schweiz und der Europäischen Union oder einem Schengen-Staat; Verträge mit Drittstaaten sind nicht inbegriffen.

Absatz 1 Buchstabe b ist insbesondere auf den Vertrag zwischen der Schweiz und der Europäischen Union zur Vertiefung der internationalen Polizeikooperation sowie das Protokoll zum Zugriff der Strafverfolgungsbehörden auf die Datenbank Eurodac gerichtet.

---

[19] SR **0.362.31**

[20] SR **142.20**

Abs. 2: Schengen-Assoziierungsabkommen

In dieser Bestimmung wird präzisiert, dass die Schengen-Assoziierungsabkommen im Anhang aufgeführt sind.

Art. 2 Verhältnis zu anderen Erlassen

Abs. 1: Rechte der betroffenen Personen in Verfahren

Nach dem geltenden Artikel 2 Absatz 2 Buchstabe c des Bundesgesetzes vom 19. Juni 1992[21] über den Datenschutz (DSG) ist das Gesetz unter anderem nicht auf hängige Strafverfahren und Verfahren der internationalen Rechtshilfe anwendbar. Diese Ausnahme ist mit dem Geltungsbereich der Richtlinie (EU) 2016/680 gemäss deren Artikeln 1 und 2 nicht vereinbar. In Artikel 2 Absatz 1 SDSG wird deshalb zwar ein Vorbehalt in Bezug auf solche Verfahren angebracht, dieser beschränkt sich jedoch auf die Rechte der betroffenen Personen. Ein solcher Vorbehalt ist gestützt auf Artikel 18 der Richtlinie (EU) 2016/680 möglich. Gemäss dieser Bestimmung und dem Erwägungsgrund 49 der Richtlinie können die Schengen-Staaten vorsehen, dass die Ausübung der Rechte der betroffenen Personen, nämlich des Rechts auf Information, Auskunft, Berichtigung, Einschränkung oder Löschung, nach Massgabe des einzelstaatlichen Strafverfahrensrechts erfolgt, wenn Personendaten im Zusammenhang mit strafrechtlichen Ermittlungen und Gerichtsverfahren in Strafsachen bearbeitet werden.

Artikel 2 Absatz 1 SDSG hält entsprechend fest, dass die Rechte der betroffenen Personen in hängigen Verfahren vor den eidgenössischen Gerichten und in hängigen Verfahren nach der StPO oder dem IRSG durch das anwendbare Verfahrensrecht geregelt werden. Dabei handelt es sich um eine Norm zur Koordination des SDSG mit dem Verfahrensrecht. Deren Zweck besteht darin, einen Normkonflikt zu vermeiden. Absatz 1 verankert den Grundsatz, dass sich die Rechte der betroffenen Personen ausschliesslich nach dem anwendbaren Verfahrensrecht richten. Das bedeutet mit anderen Worten, dass die Verfahrensparteien beispielsweise nicht das Auskunftsrecht (Art. 17 SDSG) geltend machen können, um die Straf- oder Rechtshilfeakten einzusehen. Sie können auch keine Ansprüche nach Artikel 19 SDSG wie das Recht auf Löschung oder auf Berichtigung von Daten geltend machen. Solange das Verfahren hängig ist, richten sich diese Ansprüche ausschliesslich nach dem anwendbaren Verfahrensrecht.

Sobald das Verfahren abgeschlossen ist, sind das SDSG und subsidiär das DSG anwendbar. Diese Regelung entspricht dem geltenden Recht (Art. 2 Abs. 2 Bst. c DSG e contrario). Sie entspricht ausserdem der Lösung gemäss Artikel 99 Absatz 1 StPO: Nach Abschluss des Strafverfahrens richten sich das Bearbeiten von Personendaten, das Verfahren und der Rechtsschutz nach den Bestimmungen des Datenschutzrechts von Bund und Kantonen.

Abs. 2: Subsidiäre Anwendung des DSG

Diese Bestimmung regelt das Verhältnis zwischen dem SDSG, dem DSG und den bereichsspezifischen Datenschutzvorschriften in anderen Bundesgesetzen. Sie hält fest, dass sich der Datenschutz im Schengen-Bereich grundsätzlich nach dem SDSG sowie den Vorschriften in den Spezialgesetzen, einschliesslich der neu eingeführten Bestimmungen im StGB, in der StPO, im IRSG und im BPI, richtet. Beispielhaft können für den Bereich der internationalen Rechtshilfe in Strafsachen die neuen Vorschriften nach Artikel 11*b* ff. IRSG und die bereits in Kraft stehenden Bestimmungen wie Artikel 52 IRSG betreffend den Anspruch der verfolgten Person auf rechtliches Gehör und Artikel 80*b* IRSG betreffend das Recht auf Teilnahme am Verfahren und auf Akteneinsicht, welche die Anforderungen der Richtlinie (EU) 2016/680 hinsichtlich der Transparenz von Datenbearbeitungen erfüllen, genannt werden.

[21] SR **235.1**

Enthält weder das SDSG noch die Spezialgesetzgebung eine besondere Regelung, gelangen die allgemeinen Datenschutzbestimmungen des DSG zur Anwendung, beispielsweise in Bezug auf den Zweck (Art. 1), bestimmte Definitionen nach Artikel 3, die Datensicherheit (Art. 7), das Register der Datensammlungen (Art. 11*a*), die Informationspflicht beim Beschaffen von Personendaten (Art. 18*a* und 18*b*), das Angebot von Unterlagen an das Bundesarchiv (Art. 21) usw.

Art. 3 Begriffe

Nebst den Begriffsbestimmungen nach Artikel 3 DSG definiert das SDSG neue Begriffe, die in den Artikeln 3 und 10 der Richtlinie (EU) 2016/680 zu finden sind.

Abs. 1 Bst. a: besonders schützenswerte Personendaten

Buchstabe a definiert den Katalog der besonders schützenswerten Personendaten.

Abweichend von der Begriffsbestimmung nach Artikel 3 Buchstabe c Ziffer 1 DSG werden die Daten über die gewerkschaftlichen Ansichten oder Tätigkeiten im SDSG nicht als besonders schützenswert eingestuft. Das Parlament vertrat die Auffassung, dass diese Art von Daten im Begriff der «Daten über die politischen Ansichten oder Tätigkeiten» inbegriffen ist und es deshalb nutzlos ist, sie in Artikel 3 Buchstabe a Ziffer 1 SDSG zu nennen. Wie in den Materialien deutlich festgehalten wird,[22] hat diese Änderung keine materiellen Folgen.

Von Ziffer 2 erfasst sind nicht nur die Daten über die Zugehörigkeit zu einer Rasse, sondern entsprechend der Richtlinie (EU) 2016/680 (Art. 10) auch diejenigen über die Zugehörigkeit zu einer Ethnie. Die Verwendung des Begriffs der «Rasse» bedeutet nicht, dass Theorien gutgeheissen werden, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen.

Der Begriff der «besonders schützenswerte Personendaten» wird ausserdem auf genetische Daten (Ziff. 3) und biometrische Daten, die ein Individuum eindeutig identifizieren, (Ziff. 4) ausgeweitet. Diese Änderung trägt den Anforderungen von Artikel 10 der Richtlinie (EU) 2016/680 Rechnung.

Genetische Daten sind Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden; darin eingeschlossen ist auch das DNA-Profil (Art. 3 Bst. l des Bundesgesetzes vom 8. Oktober 2004[23] über genetische Untersuchungen beim Menschen [GUMG]).

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

Abs. 1 Bst. b: Profiling

Im SDSG wird neu der Begriff des «Profilings» eingeführt.

Die Begriffsbestimmung entspricht derjenigen nach Artikel 3 Ziffer 4 der Richtlinie (EU) 2016/680. Das Parlament hat entschieden, von der Definition, die der Bundesrat in seinem Entwurf zur Totalrevision des DSG vorgeschlagen hatte, abzuweichen und sich an den euro-

---

[22] Amtl. Bull. **2018** N 977 und Amtl. Bull. **2018** E 620.

[23] SR **810.12**

päischen Rechtsakt anzulehnen. Demnach ist unter «Profiling» jede Art der automatisierten Bearbeitung von Personendaten zu verstehen, die darin besteht, dass diese 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. Dazu können auch Algorithmen verwendet werden, aber deren Verwendung ist nicht konstitutiv für das Vorliegen eines Profilings. Es ist hingegen verlangt, dass eine automatisierte Datenbearbeitung stattfindet; werden lediglich Daten angesammelt, erfolgt noch kein Profiling. Als Datenbearbeitung, welche zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Personen führen kann, ist für Profiling eine Grundlage in einem formellen Gesetz erforderlich (Art. 36 BV; vgl. die Erläuterungen zu Art. 6 Abs. 2 Bst. c SDSG).

Abs. 1 Bst c: Verletzung der Datensicherheit

Des Weiteren wird im SDSG der Begriff der «Verletzung der Datensicherheit» bestimmt. Eine Verletzung der Datensicherheit liegt vor, wenn ein Vorgang dazu führt, dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Dies gilt ungeachtet dessen, ob der Vorgang mit Absicht geschieht oder nicht, und, ob er widerrechtlich ist oder nicht. Der Begriff knüpft an Artikel 7 DSG an, wonach Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen. Inhaltlich entspricht der Begriff Artikel 3 Ziffer 11 der Richtlinie (EU) 2016/680.

Massgebend ist alleine, ob die fraglichen Vorgänge geschehen. Irrelevant für das Vorliegen einer Verletzung der Datensicherheit ist ebenfalls, ob lediglich die Möglichkeit besteht, dass die Personendaten Unbefugten offengelegt oder zugänglich gemacht worden sind, oder ob ein solcher Zugang tatsächlich stattgefunden hat. Geht beispielsweise ein Datenträger verloren, lässt sich oft kaum nachweisen, ob die darauf gespeicherten Daten tatsächlich durch Unbefugte eingesehen oder verwendet worden sind. Daher stellt bereits der Verlust als solcher eine Verletzung der Datensicherheit dar. Für die nach einem solchen Vorfall zu treffenden Massnahmen, insbesondere für die Einschätzung des Risikos nach Artikel 15 Absatz 1 SDSG, sind der Umfang und die Bedeutung einer Verletzung der Datensicherheit relevant.

Abs. 1 Bst. d: automatisierte Einzelentscheidung

Um den Anforderungen von Artikel 11 der Richtlinie (EU) 2016/680 Rechnung zu tragen, wird im SDSG der Begriff der «automatisierten Einzelentscheidung» eingeführt. Eine solche Entscheidung liegt vor, wenn die inhaltliche Bewertung von Daten und die darauf gestützte Entscheidung nicht durch eine natürliche Person vorgenommen wird. Es kann sich selbst dann um eine automatisierte Einzelentscheidung handeln, wenn sie anschliessend durch eine natürliche Person, d. h. eine Angestellte oder einen Angestellten des zuständigen Bundesorgans, mitgeteilt wird, sofern diese Person die automatisch gefällte Entscheidung nicht mehr beeinflussen kann. Massgebend ist, inwieweit eine natürliche Person eine inhaltliche Prüfung vornehmen und darauf aufbauend die endgültige Entscheidung fällen kann. Erforderlich ist allerdings, dass die Entscheidung eine gewisse Komplexität aufweist. Im Übrigen wird auf die Erläuterungen zu Artikel 11 SDSG verwiesen.

Abs. 1 Bst. e: Auftragsbearbeiter

Beim Auftragsbearbeiter handelt es sich um eine private Person oder ein Bundesorgan, die oder das im Auftrag des verantwortlichen Bundesorgans Daten bearbeitet. Dieser Begriff entspricht demjenigen der Richtlinie (EU) 2016/680 (Art. 3 Ziff. 9).

Die Rechtsbeziehung zwischen dem Bundesorgan und dem Auftragsbearbeiter kann unterschiedlicher Natur sein. Es kann es sich um einen Vertrag oder die Übertragung einer öffentlichen Aufgabe, welche die Bearbeitung von Personendaten beinhaltet, handeln. Der Auf-

tragsbearbeiter ist ab dem Zeitpunkt, an dem er seine Tätigkeit im Auftrag des Bundesorgans beginnt, kein Dritter mehr.

Art. 4 Grundsätze

Abs. 1 und 2

Die Absätze 1 und 2 halten die Grundsätze der Rechtmässigkeit, von Treu und Glauben und der Verhältnismässigkeit fest. Sie entsprechen dem Artikel 4 Absätze 1 und 2 DSG. Um zu vermeiden, dass die datenschutzrechtlichen Grundsätze in zwei verschiedenen Gesetzen geregelt werden (DSG und SDSG), werden sie alle im SDSG aufgeführt. So ist die Rechtssicherheit besser gewährleistet.

Abs. 3: Zweckbindung und Erkennbarkeit

Absatz 3 vereinigt die Grundsätze der Zweckbindung und der Erkennbarkeit, die in Artikel 4 Absätze 3 und 4 DSG enthalten sind. Die neue Formulierung hat im Vergleich zum geltenden Recht keine materiellen Änderungen zur Folge. Sowohl die Beschaffung der Daten als auch der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein. Es wird davon ausgegangen, dass dies grundsätzlich der Fall ist, wenn die Bearbeitung gesetzlich vorgesehen ist.

Absatz 3 hält ausserdem fest, dass Daten nur in einer Weise bearbeitet werden dürfen, die mit dem anfänglichen Zweck zu vereinbaren ist.

Ist die Änderung des anfänglichen Zwecks gesetzlich vorgesehen oder wird sie durch eine Gesetzesänderung verlangt, so gilt die Weiterbearbeitung ebenfalls als mit dem anfänglichen Zweck vereinbar. Ein Anwendungsfall dazu findet sich in Artikel 96 Absatz 1 StPO. Gemäss dieser Bestimmung darf die Strafbehörde aus einem hängigen Verfahren Personendaten zwecks Verwendung in einem anderen hängigen Verfahren bekanntgeben, wenn anzunehmen ist, dass die Daten wesentliche Aufschlüsse geben können

Im Bereich der internationalen justiziellen Zusammenarbeit in Strafsachen entspricht der Grundsatz der Zweckbindung dem Grundsatz der Spezialität: Die übermittelten Daten dürfen nur für das Strafverfahren verwendet werden, das dem Ersuchen zugrunde liegt. Jegliche andere Verwendung durch die zuständige Behörde des ersuchenden Staates unterliegt der Bewilligung durch den ersuchten Staat.

Abs. 4: Dauer der Aufbewahrung der Personendaten

Gemäss Absatz 4 müssen Personendaten vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. Dies entspricht den Vorgaben der Richtlinie (EU) 2016/680 (Art. 4 Abs. 1 Bst. e). Die genannte Verpflichtung ergibt sich zwar bereits implizit aus dem allgemeinen Verhältnismässigkeitsgrundsatz, der in Artikel 4 Absatz 2 SDSG festgehalten ist. Es ist jedoch wichtig, diese Verpflichtung im Hinblick auf die technologischen Entwicklungen und die beinahe unbegrenzten Speichermöglichkeiten auch noch ausdrücklich festzuhalten. Im öffentlichen Sektor werden die Aufbewahrungsfristen grundsätzlich vom Gesetzgeber festlegt.

Abs. 5: Richtigkeit

Absatz 5 übernimmt den Grundsatz der Richtigkeit der Daten, der heute in Artikel 5 DSG enthalten ist. Im französischen Text wird der Begriff «correctes» durch «exactes» ersetzt; auf Deutsch und Italienisch stimmt die verwendete Terminologie bereits heute überein.

Absatz 5 hält fest, dass sich jede Person, welche Daten bearbeitet, über deren Richtigkeit zu vergewissern hat. Sie hat alle angemessenen Massnahmen zu treffen, damit die Daten, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind, berichtigt, gelöscht oder vernichtet werden. Daten, die nicht berichtigt oder vervollstän-

digt werden können, sind zu löschen oder zu vernichten. Der Umfang dieser Vergewisserungspflicht ist im Einzelfall zu bestimmen. Er hängt insbesondere vom Zweck und Umfang der Bearbeitung sowie von der Art der bearbeiteten Daten ab. Je nach Fall kann diese Pflicht bedeuten, dass die Daten aktuell gehalten werden müssen.

Bestimmte gesetzliche Vorgaben können der Berichtigung, der Löschung oder der Aktualisierung der Daten entgegenstehen.[24]

Anders als im DSG wird im SDSG der Begriff der «Einwilligung» nicht definiert. Denn gemäss der Richtlinie (EU) 2016/680 ist in ihrem Anwendungsbereich eine ausschliesslich auf die Einwilligung der betroffenen Person gestützte Bearbeitung von Personendaten nicht rechtmässig.[25] Bei der Einwilligung der betroffenen Person kann es sich um eine Modalität der Datenbearbeitung, nicht aber um deren rechtliche Grundlage handeln. Gemäss dem in Erwägungsgrund 35 der Richtlinie (EU) 2016/680 angeführten Beispiel dürfen die Schengen-Staaten *gesetzlich* vorsehen, dass die betroffene Person der Bearbeitung ihrer Daten zustimmen kann, etwa im Falle von DNA-Tests in strafrechtlichen Ermittlungen. Ein anderer Anwendungsfall ist in Artikel 80*c* IRSG enthalten. Diese Bestimmung regelt die vereinfachte Ausführung der Rechtshilfe und legt in Absatz 1 fest, dass die Inhaber von Schriftstücken oder Auskünften einer Herausgabe dieser Informationen an den ersuchenden Staat zustimmen können.

Art. 5 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Artikel 5 SDSG führt die Pflicht zum Datenschutz durch Technik sowie durch datenschutzfreundliche Voreinstellungen ein. Weil diese Pflicht eng mit den datenschutzrechtlichen Grundsätzen zusammenhängt, wird sie in die allgemeinen Bestimmungen des Gesetzes übernommen. Die Norm setzt die Anforderungen von Artikel 20 der Richtlinie (EU) 2016/680 um.

Zum Schutz der Privatsphäre der Personen, über die Daten bearbeitet werden, müssen angemessene technische und organisatorische Massnahmen ergriffen werden (Art. 7 DSG und Art. 8, 10 und 20 der Verordnung vom 14. Juni 1993[26] zum Bundesgesetz über den Datenschutz [VDSG]). Die Umsetzung dieser Massnahmen darf nicht ausschliesslich von wirtschaftlichen Überlegungen abhängig gemacht werden. Um die Einhaltung der Datenschutzvorschriften nachweisen zu können, muss das Bundesorgan die nötigen internen Vorkehren treffen und Massnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen gerecht werden. Hat das Bundesorgan eine Datenschutz-Folgenabschätzung nach Artikel 13 SDSG vorgenommen, so müssen die entsprechenden Ergebnisse bei der Entwicklung der Massnahmen berücksichtigt werden.

Abs. 1: Datenschutz durch Technik

Absatz 1 verlangt vom Bundesorgan, eine Datenbearbeitung bereits ab dem Zeitpunkt der Planung so auszugestalten, dass die Datenschutzvorschriften eingehalten werden. Damit wird neu die Pflicht zum sogenannten «Datenschutz durch Technik» (*Privacy by Design*) eingeführt. Die Grundidee des technikgestützten Datenschutzes besteht darin, dass sich Technik und Recht gegenseitig ergänzen. So kann datenschutzfreundliche Technik den Bedarf nach rechtlichen Regeln reduzieren, indem technische Vorkehren den Verstoss gegen Datenschutzvorschriften verunmöglichen oder zumindest die Gefahr erheblich verringern. Zugleich sind datenschutzfreundliche Technologien unabdingbar für die praktische Umset-

---

[24] Wie zum Beispiel die in Art. 7 des Geldwäschereigesetzes vom 10. Oktober 1997 (SR **955.0**) vorgesehene Pflicht, Daten unversehrt zu halten.

[25] Siehe Erwägungsgrund 35 der Richtlinie (EU) 2016/680.

[26] SR **235.11**

zung der Datenschutzvorschriften. Die technologische Entwicklung hat auch in den Bereichen der Verhütung, Aufklärung und Verfolgung von Straftaten dazu geführt, dass immer mehr Daten bearbeitet werden, die im Einklang mit den Datenschutzregeln behandelt 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 SDSG entsprechen. Die gesetzlichen Anforderungen für eine datenschutzkonforme Bearbeitung werden mit anderen Worten bereits so im System verwirklicht, dass dieses die Gefahr von Verstössen gegen Datenschutzvorschriften reduziert oder ausschliesst. Auf diese Weise kann z. B. dafür gesorgt werden, dass Daten in regelmässigen Abständen gelöscht oder standardmässig anonymisiert werden. Besonders bedeutsam für den technikgestützten Datenschutz ist dabei die sogenannte Datenminimierung. Entsprechend dem Konzept der Datenminimierung wird eine Datenbearbeitung bereits von Beginn weg so angelegt, dass möglichst wenige Daten anfallen und bearbeitet werden oder dass die Daten zumindest nur für möglichst kurze Zeit aufbewahrt werden.

Diese Bestimmung hat praktisch nur geringe Auswirkungen. Denn die Bundesorgane müssen schon heute den von ihnen bezeichneten Datenschutzverantwortlichen oder, falls keine solchen bestehen, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten («Beauftragter») unverzüglich alle Projekte zur automatisierten Bearbeitung von Personendaten melden, damit die Erfordernisse des Datenschutzes bereits bei der Planung berücksichtigt werden (siehe Art. 20 VDSG).

Abs. 2: Angemessenheit der Vorkehren

Absatz 2 präzisiert die Anforderungen an die Vorkehren nach Absatz 1. Diese müssen insbesondere nach dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken, welche die fragliche Bearbeitung für die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

Die Norm bringt den risikobasierten Ansatz des bundesrätlichen Gesetzesentwurfs vom 15. September 2017[27] zum Ausdruck. Das Risiko, das mit einer Bearbeitung einhergeht, muss in Beziehung gesetzt werden zu den technischen Möglichkeiten, um dieses zu verringern. Je höher das Risiko, je grösser die Eintrittswahrscheinlichkeit und je umfangreicher die Datenbearbeitung ist, umso höher sind die Anforderungen an die technischen Vorkehren, damit sie im Sinne der vorliegenden Bestimmung als angemessen gelten können.

Abs. 3: Datenschutzfreundliche Voreinstellungen

Gemäss Absatz 3 ist das Bundesorgan verpflichtet, mittels geeigneter Voreinstellungen dafür zu sorgen, dass grundsätzlich nur so wenige Personendaten bearbeitet werden, wie es im Hinblick auf den Verwendungszweck nötig ist (*Privacy by Default*). Ein Datenbearbeitungsvorgang muss standardmässig möglichst datenschutzfreundlich eingerichtet sein. Es besteht ein enger Zusammenhang zum Grundsatz der Verwendung datenschutzfreundlicher Technik. So gehören entsprechende Voreinstellungen regelmässig zur datenschutzfreundlichen Ausgestaltung eines gesamten Systems.

Art. 6 Rechtsgrundlagen betreffend die Bearbeitung von Personendaten

Artikel 6 SDSG regelt die Vorgaben an die gesetzlichen Grundlagen für die Bearbeitung von Personendaten. Er entspricht zum Teil Artikel 17 DSG, nennt aber auch neue Arten der Datenbearbeitung, für welche gemäss den Anforderungen der Richtlinie (EU) 2016/680 eine Grundlage in einem Gesetz im formellen Sinn erforderlich ist.

---

[27] BBl **2017** 6970 f.

Abs. 1: Grundsatz

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

Abs. 2: Grundlage in Gesetz im formellen Sinn

Wie nach geltendem Recht schreibt Absatz 2 Buchstaben a und b vor, dass für die Bearbeitung von besonders schützenswerten Daten und von Persönlichkeitsprofilen eine Grundlage in einem Gesetz im formellen Sinn erforderlich ist.

Zudem sind die Bundesorgane nach Absatz 2 Buchstabe c nur dann zu Profiling im Sinne von Artikel 3 Absatz 1 Buchstabe b SDSG befugt, wenn dies in einem Gesetz im formellen Sinn vorgesehen ist. Aufgrund des Risikos eines Eingriffs in die Grundrechte der betroffenen Personen muss die Rechtsgrundlage für das Profiling auf derselben Stufe bestehen wie für die Bearbeitung von besonders schützenswerten Daten und Persönlichkeitsprofilen.

Nach Absatz 2 Buchstabe d ist eine Grundlage in einem Gesetz im formellen Sinn schliesslich dann erforderlich, wenn die Art und Weise der Datenbearbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Personen führen kann. Es handelt sich hierbei nicht um eine völlig neue Anforderung, denn bereits nach Artikel 36 Absatz 1 BV bedürfen schwerwiegende Einschränkungen von Grundrechten einer formellgesetzlichen Grundlage.

So sind zum Beispiel automatisierte Einzelentscheidungen nach Artikel 3 Absatz 1 Buchstabe d SDSG eine Bearbeitungsart, die einen schwerwiegenden Eingriff in die Grundrechte der betroffenen Personen darstellen kann. Trifft dies in einem Fall jedoch nicht zu, so genügt eine Grundlage in einem Gesetz im materiellen Sinn. Eine Ermächtigung durch ein Gesetz im formellen Sinn ist grundsätzlich dann erforderlich, wenn die automatisierte Einzelentscheidung gestützt auf besonders schützenswerte Personendaten erfolgt. Damit wird auch den Anforderungen von Artikel 11 der Richtlinie (EU) 2016/680 Rechnung getragen.

Abs. 3: Ausnahmen

Gemäss Absatz 3 kann von der Anforderung der gesetzlichen Grundlage (Abs. 1 und 2) abgewichen werden, wenn eine der Voraussetzungen nach den Buchstaben a und b erfüllt ist.

Nach Buchstabe a dürfen die Bundesorgane Personendaten bearbeiten, wenn die Bearbeitung notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen. Diese Ausnahme ist im Vergleich zu Artikel 17 Absatz 2 DSG neu. Sie entspricht Artikel 10 Buchstabe b der Richtlinie (EU) 2016/680.

Gemäss Buchstabe b können Bundesorgane Personendaten ohne gesetzliche Grundlage bearbeiten, wenn die betroffene Person ihre Personendaten allgemein zugänglich gemacht und die Bearbeitung nicht ausdrücklich untersagt hat. Diese Bestimmung entspricht teilweise der Ausnahme nach Artikel 17 Absatz 2 Buchstabe c DSG.

Abweichend vom DSG sieht das SDSG nicht vor, dass ausnahmsweise keine gesetzliche Grundlage erforderlich ist, wenn die «Einwilligung» der betroffenen Person vorliegt. Denn gemäss der Richtlinie (EU) 2016/680 ist in ihrem Anwendungsbereich die Bearbeitung von Personendaten nicht rechtmässig, wenn sie sich ausschliesslich auf die Einwilligung der betroffenen Person stützt (vgl. die Erläuterungen zu Art. 4 SDSG).[28]

[28] Siehe Erwägungsgründe 35 und 37 der Richtlinie (EU) 2016/680.

Art. 7 Rechtsgrundlagen betreffend die Bekanntgabe von Personendaten

Artikel 7 SDSG übernimmt zum Teil den heutigen Artikel 19 DSG.

Mit Absatz 1 werden die Artikel 8 und 10 der Richtlinie (EU) 2016/680 umgesetzt. Gemäss diesen ist eine Datenbearbeitung im Anwendungsbereich der Richtlinie 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.

Absatz 2 erklärt ausserdem Artikel 19 Absätze 1bis–4 DSG für anwendbar.

Art. 8 Bekanntgabe von Personendaten ins Ausland

Absatz 1 setzt Artikel 9 Absätze 3 und 4 der Richtlinie (EU) 2016/680 um. Er führt die Gleichbehandlung der Behörden der Schengen-Staaten und der schweizerischen Strafbehörden im Datenschutzbereich ein.[29] Die Bestimmung 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.

Nach Absatz 2 wird die Bekanntgabe von Personendaten an einen Drittstaat oder an ein internationales Organ durch die Spezialbestimmungen des anwendbaren Bundesrechts geregelt, d. h. durch die Artikel 349*c*–349*e* und 355*a* Absatz 4 StGB im Bereich der polizeilichen Zusammenarbeit und die Artikel 11*f*–11*g* IRSG im Bereich der Rechtshilfe in Strafsachen.

Art. 9 Verantwortliches Bundesorgan und Kontrolle

Im Vergleich zu Artikel 16 DSG erfährt Artikel 9 Absatz 2 SDSG einige Änderungen, damit Artikel 21 der Richtlinie (EU) 2016/680 umgesetzt werden kann.

Absatz 1 entspricht Artikel 16 Absatz 1 DSG.

In Absatz 2 wird aus redaktionellen Gründen der Ausdruck «besonders regeln» gemäss Artikel 16 Absatz 2 DSG weggelassen. Darüber hinaus soll der Bundesrat nicht nur die Möglichkeit haben, Regeln über die Kontrolle und Verantwortung für den Datenschutz zu erlassen, wenn Bundesorgane Daten zusammen mit anderen Behörden oder Privaten bearbeiten, sondern dazu verpflichtet sein.

Art. 10 Bearbeitung durch Auftragsbearbeiter

Artikel 10 SDSG setzt die Anforderungen von Artikel 22 der Richtlinie (EU) 2016/680 um und verweist in Absatz 1 betreffend die Übertragung einer Datenbearbeitung an einen Auftragsbearbeiter (zur Legaldefinition vgl. Art. 3 Abs. 1 Bst. e SDSG) im Wesentlichen auf den geltenden Artikel 10*a* DSG.

Wie nach bisherigem Recht besteht bei der Auftragsbearbeitung eine Sorgfaltspflicht des verantwortlichen Bundesorgans. Es muss aktiv sicherstellen, dass der Auftragsbearbeiter das Datenschutzrecht im gleichen Umfang einhält, wie es dies selbst tut. Das gilt insbesondere für die allgemeinen Grundsätze des Datenschutzrechts wie die Löschung oder Anonymisierung von Personendaten, die zum Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 4 Abs. 4 SDSG), oder für die Datensicherheit, welche in Artikel 10*a* Absatz 2 DSG ausdrücklich erwähnt wird. Das Bundesorgan muss analog zu Artikel 55 des Obligationen-

[29] Siehe Erwägungsgrund 26 der Richtlinie (EU) 2016/680.

rechts[30] Verstösse gegen das Datenschutzrecht verhindern. Es ist daher verpflichtet, seinen Auftragsbearbeiter sorgfältig auszuwählen, ihn angemessen zu instruieren und soweit als nötig zu überwachen. Der Auftragsbearbeiter muss gemäss Artikel 12 SDSG ein Verzeichnis seiner Bearbeitungstätigkeiten führen.

Neu ist Artikel 10 Absatz 2 SDSG. Diese Bestimmung sieht vor, dass der Auftragsbearbeiter die Datenbearbeitung nur mit vorgängiger schriftlicher Genehmigung des verantwortlichen Bundesorgans einem weiteren Dritten übertragen darf. Es handelt sich dabei um eine Anforderung gemäss Artikel 22 Absatz 2 der Richtlinie (EU) 2016/680. Die Genehmigung durch das verantwortliche Bundesorgan kann spezifischer oder allgemeiner Art sein. In letzterem Fall muss der Auftragsbearbeiter das Bundesorgan über jede Änderung (Hinzuziehung oder Ersetzung anderer Auftragsbearbeiter) informieren, damit dieses gegebenenfalls Einspruch erheben kann.

Ein Auftragsbearbeiter darf Daten nur so bearbeiten, wie das verantwortliche Bundesorgan es tun dürfte (vgl. Art. 10*a* Abs. 1 Bst. a DSG). Dies bedeutet, dass auf den Auftragsbearbeiter ebenfalls das SDSG Anwendung findet. Dementsprechend richten sich auch die Aufsichtsbefugnisse des Beauftragten gegenüber dem Auftragsbearbeiter nach Artikel 22 ff. SDSG (und nicht nach Art. 27 DSG).

2.3 Pflichten der Bundesorgane und der Auftragsbearbeiter

Art. 11 Automatisierte Einzelentscheidung

Mit dieser Bestimmung wird Artikel 11 der Richtlinie (EU) 2016/680 umgesetzt. Der Begriff «automatisierte Einzelentscheidung» wird in Artikel 3 Absatz 1 Buchstabe d SDSG definiert. Dabei handelt es sich um eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung, einschliesslich Profiling, beruht und die für die betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt.

Abs. 1: Information der betroffenen Person

Nach diesem Absatz informiert das Bundesorgen die betroffene Person über eine ihr gegenüber ergangene automatisierte Einzelentscheidung. Es muss sie spezifisch darüber informieren, dass die Entscheidung ohne Dazutun einer natürlichen Person getroffen worden ist. Dies ist erforderlich, damit die betroffene Person ihre Rechte nach Absatz 2 geltend machen kann.

Bei der automatisierten Datenbearbeitung, auf welche sich die Entscheidung stützt, kann es sich um Profiling (Art. 3 Abs. 1 Bst. b SDSG) handeln. In diesem Zusammenhang hält Artikel 11 Absatz 3 der Richtlinie (EU) 2016/680 fest, dass das Unionsrecht Profiling verbietet, welches zur Folge hat, dass natürliche Personen auf der Grundlage von besonderen Datenkategorien nach Artikel 10 der Richtlinie (d.h. besonders schützenswerten Personendaten) diskriminiert werden. Diese Vorgabe entspricht dem in Artikel 9 BV gewährleisteten Schutz vor willkürlicher Behandlung.

Die betroffene Person muss nicht über jede automatisierte Einzelentscheidung informiert werden. Vielmehr ist dies nur erforderlich, wenn die Entscheidung für die betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (Art. 3 Abs. 1 Bst. d SDSG).

Die Entscheidung ist mit einer Rechtsfolge verbunden, wenn sie unmittelbare, rechtlich vorgesehene Konsequenzen für die betroffene Person nach sich zieht. Eine solche Rechtsfolge

[30] SR **220**

könnten zum Beispiel verschärfte Sicherheits- oder Aufsichtsmassnahmen gegenüber der betroffenen Person darstellen.[31]

Eine erhebliche Beeinträchtigung der betroffenen Person ist anzunehmen, wenn diese auf nachhaltige Weise in ihren persönlichen Belangen eingeschränkt wird. Eine blosse Belästigung reicht dafür nicht aus. Massgebend sind die konkreten Umstände des Einzelfalls. Zu berücksichtigen ist insbesondere, wie bedeutsam das fragliche Gut für die betroffene Person ist, wie dauerhaft sich die Entscheidung auswirkt und ob allenfalls Alternativen zugänglich sind. Eine erhebliche Beeinträchtigung könnte sich beispielsweise daraus ergeben, dass die betroffene Person an der Teilnahme an einer Flugreise gehindert wird, weil sie auf einer schwarzen Liste erscheint.[32]

Abs. 2: Recht auf Darlegung des eigenen Standpunktes

Gemäss Absatz 2 muss das Bundesorgan der betroffenen Person auf deren Antrag hin die Möglichkeit geben, ihren Standpunkt darzulegen. Die betroffene Person soll insbesondere Gelegenheit erhalten, ihre Ansicht zum Ergebnis der Entscheidung zu äussern und gegebenenfalls nachzufragen, wie die Entscheidung zustande gekommen ist. Die betroffene Person kann ausserdem verlangen, dass ihr das angewandte Verfahren mitgeteilt und die Entscheidung von einer natürlichen Person überprüft wird. Dadurch soll unter anderem verhindert werden, dass die Datenbearbeitung auf unvollständigen, veralteten oder unzutreffenden Daten beruht. Dies liegt auch im Interesse des Bundesorgans, weil unzutreffende automatisierte Einzelentscheidungen für es ebenfalls negative Konsequenzen nach sich ziehen können. Das Gesetz legt nicht fest, wann die betroffene Person informiert werden muss und wann sie Gelegenheit erhält, ihren Standpunkt darzulegen. Dementsprechend kann dies vor oder nach der Entscheidung geschehen. So ist es beispielsweise möglich, der betroffenen Person eine automatisierte Einzelentscheidung, die entsprechend gekennzeichnet ist, zuzustellen und die betroffene Person anschliessend im Rahmen des rechtlichen Gehörs anzuhören.

Abs. 3: Ausnahme

Absatz 3 sieht vor, dass Absatz 2 nicht gilt, wenn der betroffenen Person gegen die Entscheidung ein Rechtsmittel zur Verfügung steht. Die betroffene Person kann ihren Standpunkt in diesem Rahmen darlegen und den Entscheid durch eine natürliche Person überprüfen lassen. Die Rechte nach Artikel 11 Absatz 2 SDSG werden mit anderen Worten bereits durch den üblichen Rechtsweg gewährleistet.

Art. 12 Verzeichnis der Bearbeitungstätigkeiten

Mit dieser Bestimmung wird Artikel 24 der Richtlinie (EU) 2016/680 umgesetzt.

Die Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten obliegt nach Absatz 1 den Bundesorganen und den Auftragsbearbeitern.

Absatz 2 zählt die Mindestangaben auf, die das Verzeichnis enthalten muss. Dazu gehören zunächst der Name des Bundesorgans (Bst. a) und der Bearbeitungszweck (Bst. b). Enthalten sein muss weiter eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten (Bst. c). Die Kategorien bearbeiteter Personendaten bezeichnen die Art der bearbeiteten Daten, z. B. besonders schützenswerte Personendaten. Aufgeführt werden müssen ebenfalls die Kategorien von Empfängerinnen und Empfängern

---

[31] Vgl. dazu das Arbeitspapier «Opinion on some key issues of the Law Enforcement Directive (EU) 2016/680)» der Artikel-29-Datenschutzgruppe vom 29. November 2017, S. 14. Die Artikel-29-Datenschutzgruppe ist ein unabhängiges Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes.

[32] Vgl. dazu das Arbeitspapier «Opinion on some key issues of the Law Enforcement Directive (EU) 2016/680)» der Artikel-29-Datenschutzgruppe vom 29. November 2017, S. 14.

(Bst. d), denen die Personendaten gegebenenfalls bekanntgegeben werden. Nach Buchstabe e muss das Verzeichnis die Aufbewahrungsdauer der Personendaten enthalten. Da sich die Aufbewahrungsdauer gemäss Artikel 4 Absatz 4 SDSG nach dem Verwendungszweck richtet, lässt sich die Aufbewahrungsdauer mitunter nicht exakt bestimmen. Sind genaue Angaben nicht möglich, muss das Verzeichnis zumindest die Kriterien enthalten, nach denen die Aufbewahrungsdauer festgelegt wird. Gemäss Buchstabe f muss das Verzeichnis sodann eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 7 DSG enthalten, soweit dies möglich ist. Die Beschreibung dieser Massnahmen im Verzeichnis soll es erlauben, Mängel in den Sicherheitsvorkehren aufzuzeigen. Die Wendung «wenn möglich» macht deutlich, dass die Beschreibung nur erfolgen soll, wenn die Vorkehrungen hinreichend konkret umschrieben werden können. Schliesslich muss das Verzeichnis die Angaben von Drittstaaten oder internationalen Organen, welchen Personendaten bekanntgegeben werden, sowie die vorgesehenen Garantien zum Schutz der Personendaten enthalten. Die Bekanntgabe von Personendaten an Schengen-Staaten fällt unter Buchstabe d. Der Katalog gemäss Absatz 2 ist nicht abschliessend. Deshalb muss das Verzeichnis je nach Umständen weitere Angaben umfassen, wie z. B. die Verwendung von Profiling (Art. 24 Abs. 1 Bst. e der Richtlinie [EU] 2016/680).

Die Aufzählung in Absatz 2 macht deutlich, dass das Verzeichnis eine generelle Beschreibung der Bearbeitungstätigkeit ist, aus der sich Art und Umfang der Datenbearbeitungen ergeben. Das Verzeichnis ist mithin eine schriftliche Darstellung von wichtigen Informationen zu allen Datenbearbeitungen des Bundesorgans oder des Auftragsbearbeiters. Es lässt damit wesentliche Rückschlüsse darauf zu, ob eine Datenbearbeitung dem Grundsatz nach datenschutzkonform ausgestaltet ist oder nicht.

Absatz 3 enthält eine verkürzte Liste von Mindestangaben, welche das Verzeichnis des Auftragsbearbeiters enthalten muss. Dieser muss insbesondere die Kategorien der Datenbearbeitungen aufführen, die im Auftrag des Bundesorgans durchgeführt werden. Das Verzeichnis des Auftragsbearbeiters beinhaltet zudem den Namen des Bundesorgans, für das er tätig ist.

Art. 12 SDSG hat für die Bundesorgane keine Änderungen zur Folge, denn sie sind bereits heute zur Erstellung eines Bearbeitungsreglements verpflichtet (Art. 21 VDSG).

Art. 13 Datenschutz-Folgenabschätzung

Artikel 13 SDSG führt neu die Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung ein. Diese Bestimmung verwirklicht die Anforderungen von Artikel 27 ff. der Richtlinie (EU) 2016/680. Wie in Erwägungsgrund 58 der EU-Richtlinie erwähnt stellen Datenschutz-Folgenabschätzungen auf Systeme zur Bearbeitung von Personendaten ab und nicht auf Einzelfälle.

Begriff und Funktion der Datenschutz-Folgenabschätzung ergeben sich aus Artikel 13 Absatz 3 SDSG. Eine Datenschutz-Folgenabschätzung ist ein Instrument, um Risiken zu erkennen und zu bewerten, welche für die betroffenen Personen durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Auf der Basis der Datenschutz-Folgenabschätzung sollen gegebenenfalls angemessene Massnahmen definiert werden, um diese Risiken zu bewältigen.

Artikel 13 ist für die Bundesorgane von beschränkter Tragweite. Diese sind bereits heute verpflichtet, dem Datenschutzverantwortlichen oder, falls kein solcher besteht, dem Beauftragten Projekte zur automatisierten Bearbeitung von Daten zu melden (Art. 20 Abs. 2 VDSG). Das Vorgehen gemäss der Projektmanagementmethode Hermes dürfte den Anforderungen einer Datenschutz-Folgenabschätzung weitgehend entsprechen.

Abs. 1 und 2: Gründe für die Durchführung einer Datenschutz-Folgenabschätzung

Nach Absatz 1 muss das Bundesorgan eine Datenschutz-Folgenabschätzung durchführen, wenn die vorgesehene Datenbearbeitung ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringen kann.[33] Die Behörde ist demnach verpflichtet, eine Prognose darüber zu machen, welche Folgen eine geplante Datenbearbeitung hat. Massgebend ist hierfür insbesondere, auf welche Weise und in welchem Umfang sich eine Bearbeitung auf die Grundrechte der betroffenen Personen auswirkt.

Um das Risiko beurteilen zu können, muss das Recht auf Privatsphäre der betroffenen Personen zur fraglichen Datenbearbeitung in Beziehung gesetzt werden. Ein hohes Risiko für die Grundrechte der betroffenen Personen kann sich beispielsweise aus der Art der bearbeiteten Daten bzw. deren Inhalt (z. B. besonders schützenswerte Daten oder Persönlichkeitsprofile) oder der Art und dem Zweck des vorgesehenen Bearbeitungssystems (z. B. Profiling) ergeben.

Absatz 2 konkretisiert dies weiter und hält fest, dass sich das hohe Risiko insbesondere bei Verwendung neuer Technologien aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ergibt. Je umfangreicher die Bearbeitung, je sensibler die bearbeiteten Daten, je umfassender der Bearbeitungszweck, umso eher ist ein hohes Risiko anzunehmen. Beispielhaft zählt die Bestimmung zwei Fälle auf, in denen ein hohes Risiko vorliegt. Nach Buchstabe a liegt ein solches vor, wenn das Bearbeitungssystem in umfangreicher Form besonders schützenswerte Personendaten betrifft oder wenn in grossem Rahmen Persönlichkeitsprofile erstellt werden sollen. Nach Buchstabe b besteht bei einem Profiling ebenfalls ein hohes Risiko. Dasselbe kann gelten im Falle von Entscheidungen, die ausschliesslich auf einer automatisierten Bearbeitung, einschliesslich Profiling, beruhen und für die betroffenen Personen mit einer Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen. Solche Entscheidungen können für die betroffenen Personen gegebenenfalls mit erheblichen Folgen verbunden sein. In solchen Fällen ist eine Datenschutz-Folgenabschätzung erforderlich.

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

Abs. 3: Inhalt der Datenschutz-Folgenabschätzung

Nach Absatz 3 muss in der Datenschutz-Folgenabschätzung zunächst die geplante Bearbeitung dargelegt werden. So müssen beispielsweise die verschiedenen Bearbeitungsvorgänge (z. B. die verwendete Technologie), der Zweck der Bearbeitung oder die Aufbewahrungsdauer der Personendaten aufgeführt werden. Im Weiteren muss aufgezeigt werden, welche Risiken die fraglichen Bearbeitungsvorgänge für die Grundrechte der betroffenen Personen mit sich bringen können. Es handelt sich hier um eine Vertiefung der Risikobewertung, die bereits im Hinblick auf die Notwendigkeit einer Datenschutz-Folgenabschätzung vorzunehmen ist. So ist darzustellen, in welcher Hinsicht von der fraglichen Datenbearbeitung ein hohes Risiko für die Grundrechte der betroffenen Personen ausgeht und wie dieses Risiko zu bewerten ist. Schliesslich muss die Datenschutz-Folgenabschätzung nach Absatz 3 erläutern, mit welchen Massnahmen diese Risiken bewältigt werden sollen. Massgebend dafür sind insbesondere die Grundsätze nach Artikel 4 SDSG, aber auch die Pflicht zum Daten-

[33] Vgl. hierzu auch das Arbeitspapier «Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‹likely to result in a high risk› for the purposes of Regulation 2016/679» der Artikel-29-Datenschutzgruppe vom 4. April 2017, insbes. S. 7 ff.

schutz durch Technik und durch datenschutzfreundliche Voreinstellungen (*Privacy by Design/by Default*; Art. 5 SDSG) kann relevant sein.

Art. 14 Konsultation des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

Abs. 1: Pflicht zur Konsultation des Beauftragten

Nach Absatz 1 muss das Bundesorgan vorgängig die Stellungnahme des Beauftragten einholen, wenn sich aus der Datenschutz-Folgenabschätzung ergibt, dass die geplante Bearbeitung ein hohes Risiko für die Grundrechte der betroffenen Person zur Folge hätte, wenn das Bundesorgan keine Massnahmen träfe. Diese vorgängige Konsultation entspricht den Anforderungen von Artikel 28 der Richtlinie (EU) 2016/680.

Abs. 2 und 3: Einwände des Beauftragten

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

Nachdem er über das Ergebnis einer Datenschutz-Folgenabschätzung benachrichtigt worden ist, überprüft der Beauftragte, ob die vorgeschlagenen Massnahmen zum Schutz der Grundrechte der betroffenen Person ausreichend sind. Kommt er zum Schluss, dass die geplante Bearbeitung in der vorgeschlagenen Form gegen die Datenschutzvorschriften verstossen würde, berät er das Bundesorgan über die geeigneten Massnahmen, um die festgestellten Risiken einzudämmen.

Dem Beauftragten bleibt es indes unbenommen, zu einem späteren Zeitpunkt eine Untersuchung zu eröffnen, wenn die Voraussetzungen nach Artikel 22 SDSG 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 getroffenen Massnahmen nicht als zielgenau oder als nicht ausreichend erweisen.

Art. 15 Meldung von Verletzungen der Datensicherheit

Artikel 15 SDSG führt die Pflicht zur Meldung von Verletzungen der Datensicherheit ein. Diese Bestimmung setzt die Anforderungen von Artikel 30 f. der Richtlinie (EU) 2016/680 um.

Abs. 1: Begriff und Grundsatz

Nach Absatz 1 meldet das Bundesorgan dem Beauftragen so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führt. Diese Bestimmung weicht leicht von Artikel 30 Absatz 1 der Richtlinie (EU) 2016/680 ab, welcher vorsieht, dass der für die Datenbearbeitung Verantwortliche eine Verletzung der Datensicherheit unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der Datenschutzaufsichtsbehörde melden muss, es sei denn, dass die Verletzung der Datensicherheit voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Der Begriff der «Verletzung der Datensicherheit» ist in Artikel 3 Absatz 1 Buchstabe c SDSG definiert. Demnach handelt es sich dabei um eine Verletzung der Sicherheit, die ungeachtet der Absicht oder der Widerrechtlichkeit dazu führt, dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Die Verletzung kann durch Dritte erfolgen, aber auch durch Mitarbeiter, die ihre Kompetenzen missbrauchen oder fahrlässig handeln.

Das Bundesorgan muss eine unbefugte Bearbeitung zunächst dem Beauftragten melden und nur unter den Voraussetzungen von Absatz 4 auch den betroffenen Personen. Die Meldung hat ab dem Zeitpunkt der Kenntnisnahme so rasch als möglich zu erfolgen. Die Behörde muss grundsätzlich schnell handeln, aber es wird ihr ein gewisser Ermessensspielraum eingeräumt. Massgebend ist dabei unter anderem das Ausmass der Gefährdung der betroffenen Personen. Je erheblicher die Gefährdung, je grösser die Anzahl der betroffenen Personen, umso schneller muss das Bundesorgan handeln. Die Meldung an den Beauftragten ist jedoch nur nötig, wenn die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führt. Dies soll verhindern, dass selbst unbedeutende Verletzungen gemeldet werden müssen. Das Bundesorgan muss dafür eine Prognose in Bezug auf die möglichen Auswirkungen der Sicherheitsverletzung für die betroffenen Personen erstellen.

Abs. 2: Inhalt der Meldung

Absatz 2 enthält die Mindestanforderungen an die Meldung an den Beauftragten. Das Bundesorgan muss zunächst die Art der Verletzung der Datensicherheit nennen, soweit ihm dies möglich ist. Dabei lassen sich vier Arten der Verletzung unterscheiden: die Vernichtung oder Löschung, der Verlust, die Veränderung und die Bekanntgabe von Daten an Unbefugte. Ebenfalls muss es die Folgen der Verletzung der Datensicherheit soweit als möglich umschreiben. Schliesslich muss das Bundesorgan angeben, welche Massnahmen es aufgrund der Verletzung ergriffen hat bzw. welche Massnahmen es für die Zukunft vorschlägt. Dabei geht es um Massnahmen, welche die Verletzung beseitigen oder deren Folgen mildern. Insgesamt soll die Meldung dem Beauftragten erlauben, möglichst zeitnah und wirksam zu intervenieren.

Abs. 3: Meldung durch den Auftragsbearbeiter

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

Abs. 4: Information der betroffenen Personen

Gemäss Absatz 4 müssen die betroffenen Personen über eine Verletzung der Datensicherheit nur dann informiert werden, wenn es zu ihrem Schutz erforderlich ist oder wenn der Beauftragte es verlangt. Dabei besteht ein gewisser Ermessensspielraum.

Abs. 5: Einschränkung der Pflicht zur Information der betroffenen Personen

Das Bundesorgan kann nach Absatz 5 die Information an die betroffenen Personen einschränken, aufschieben oder darauf verzichten, wenn einer der Fälle nach den Buchstaben a–e vorliegt. Die Buchstaben a und b entsprechen den Einschränkungsgründen nach Artikel 9 DSG (Einschränkung des Auskunftsrechts). Nach Absatz 5 Buchstabe d ist die Einschränkung ausserdem zulässig, wenn die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert. Eine Information ist unmöglich, wenn das Bundesorgan nicht in der Lage ist, die von der Verletzung der Datensicherheit betroffenen Personen zu identifizieren, beispielsweise weil die Logfiles, aus denen dies ersichtlich wäre, nicht mehr vorhanden sind. Ein unverhältnismässiger Aufwand würde beispielsweise vorliegen, wenn bei einer grossen Anzahl Betroffener diese einzeln informiert werden müssten und die dadurch verursachten Kosten im Verhältnis zum Informationsgewinn für die betroffenen Personen unverhältnismässig erschienen. Insbesondere in solchen Konstellationen kann Absatz 5 Buchstabe e zur Anwendung kommen, welcher es dem Bundesorgan erlaubt, die betroffenen Personen durch eine öffentliche Bekanntmachung zu benachrichtigen, wenn deren Information dadurch auf vergleichbare Weise sichergestellt ist. Dies ist der Fall, wenn die Information der

betroffenen Personen durch eine individuelle Meldung nicht substanziell verbessert würde. Absatz 5 ist nach dem Grundsatz der Verhältnismässigkeit anzuwenden. Wenn ein Aufschub oder eine Einschränkung der Information der betroffenen Personen jedoch nicht ausreicht, um die Gefährdung einer Ermittlung, einer Untersuchung oder eines behördlichen oder gerichtlichen Verfahrens zu verhindern, so kann das Bundesorgan auf die Information verzichten (Abs. 5 Bst. c).[34] Dieser Ausnahme ist mit Artikel 31 Absatz 5 der Richtlinie (EU) 2016/680 vereinbar, wonach die Benachrichtigung der betroffenen Personen unter den in Artikel 13 Absatz 3 der Richtlinie genannten Voraussetzungen und aus den dort genannten Gründen aufgeschoben, eingeschränkt oder unterlassen werden kann. Artikel 13 Absatz 3 der Richtlinie (EU) 2016/680 lässt Einschränkungen der Informationspflicht des für die Datenbearbeitung Verantwortlichen zu, wenn dies zum Schutz überwiegender öffentlicher Interessen, wie der öffentlichen Sicherheit oder einer laufenden Ermittlung, erforderlich ist.

Art. 16 Datenschutzverantwortliche oder -verantwortlicher

Nach Artikel 32 der Richtlinie (EU) 2016/680 sind die Bundesorgane gehalten, eine Datenschutzverantwortliche oder einen Datenschutzverantwortlichen[35] zu benennen. Nach Artikel 23 Absatz 1 VDSG müssen zurzeit nur die Departemente und die Bundeskanzlei einen Berater für den Datenschutz bezeichnen. Für die Bundesorgane im Geltungsbereich des SDSG muss deshalb eine Sonderregelung eingeführt werden. Sie können allenfalls eine gemeinsame Datenschutzverantwortliche oder einen gemeinsamen Datenschutzverantwortlichen ernennen. In der Praxis hat Artikel 16 SDSG nur eine beschränkte Tragweite, da die meisten der betroffenen Behörden bereits heute über eine Datenschutzverantwortliche oder einen Datenschutzverantwortlichen verfügen.

Die Datenschutzverantwortliche oder der Datenschutzverantwortliche sorgt dafür, dass die Datenschutzvorschriften eingehalten werden, und berät in Datenschutzfragen. Das Bundesorgan ist jedoch allein dafür verantwortlich, dass die Personendaten vorschriftsgemäss bearbeitet werden.

In Absatz 2 werden die Voraussetzungen festgelegt, welche die Datenschutzverantwortliche oder der Datenschutzverantwortliche erfüllen muss. Nach Buchstabe a muss sie oder er über die erforderlichen Fachkenntnisse verfügen, um diese Aufgabe wahrzunehmen. Dabei ist für diese Tätigkeit Fachwissen sowohl im Bereich der Datenschutzgesetzgebung als auch über technische Standards zur Datensicherheit erforderlich. Um eine gewisse Unabhängigkeit zu gewährleisten, darf die oder der Datenschutzverantwortliche nach Buchstabe b keine Tätigkeiten übernehmen, die mit ihren bzw. seinen Aufgaben unvereinbar sind. Dies könnte beispielsweise der Fall sein, wenn sie oder er Funktionen im Bereich der Informationssystemverwaltung ausübt oder zu einer Dienststelle gehört, die selbst besonders schützenswerte Personendaten bearbeitet. Hingegen ist es z. B. denkbar, die Aufgabe der oder des Datenschutzverantwortlichen mit derjenigen der oder des Informationssicherheitsbeauftragten zu kumulieren.

Absatz 3 regelt die Aufgaben der oder des Datenschutzverantwortlichen. Diese Aufgaben entsprechen im Wesentlichen denjenigen nach Artikel 23 Absatz 1 VDSG.

---

[34] Siehe Erwägungsgrund 62 der Richtlinie (EU) 2016/680.

[35] Zur Terminologie: Im Gegensatz zum E-DSG wird im SDSG in der deutschen Sprachfassung – wie im geltenden Recht – der Ausdruck «Datenschutzverantwortliche» bzw. «Datenschutzverantwortlicher» verwendet, um der Parallelität zum DSG Rechnung zu tragen. Im Rahmen der Totalrevision des DSG sollte der Begriff aus Gründen der sprachlichen Klarheit allerdings durch den Ausdruck «Datenschutzberaterin» bzw. «Datenschutzberater» abgelöst werden.

2.4 Rechte der betroffenen Personen

Art. 17 Auskunftsrecht

Absatz 1 hält fest, dass sich das Auskunftsrecht der betroffenen Person nach Artikel 8 DSG richtet. Artikel 14 der Richtlinie (EU) 2016/680 sieht zudem vor, dass die betroffene Person auch das Recht hat, über die Dauer der Aufbewahrung ihrer Daten (Bst. d) sowie über ihre Rechte im Bereich des Datenschutzes (Bst. e und f) Auskunft zu erhalten. Diese beiden Auskunftsansprüche sind im DSG bis anhin nicht verankert, weshalb Artikel 17 SDSG Artikel 8 DSG ergänzt. Die neue Regelung hat zur Folge, dass das Bundesorgan der betroffenen Person auch diejenigen Informationen mitteilen muss, welche für sie erforderlich sind, um ihre Rechte, namentlich die in Artikel 19 SDSG vorgesehenen Ansprüche, geltend machen zu können. Ausserdem muss das Bundesorgan der betroffenen Person über die Aufbewahrungsdauer ihrer Daten Auskunft erteilen. Dadurch soll die betroffene Person insbesondere nachvollziehen können, ob das Bundesorgan ihre Daten entsprechend den Grundsätzen in Artikel 4 SDSG aufbewahrt.

Absatz 2 behält die Spezialbestimmungen in anderen Bundesgesetzen wie der StPO, dem IRSG oder dem BPI vor.

Art. 18 Einschränkung des Auskunftsrechts

Unter Vorbehalt von Spezialbestimmungen in anderen Bundesgesetzen richtet sich die Einschränkung des Auskunftsrechts nach Artikel 9 Absätze 1–3 und 5 DSG. Artikel 12 Absatz 4 Buchstabe b der Richtlinie (EU) 2016/680 sieht ausserdem vor, dass sich der für die Datenbearbeitung Verantwortliche unter anderem weigern kann, aufgrund eines Gesuchs der betroffenen Person (z. B. gestützt auf das Auskunftsrecht) tätig zu werden, wenn das betreffende Gesuch offenkundig unbegründet oder exzessiv ist, namentlich wenn die betroffene Person wiederholt Informationen verlangt.[36] In diesem Fall muss der Verantwortliche nachweisen, dass das Gesuch offenkundig unbegründet oder exzessiv ist. Dieser Einschränkungsgrund ist im DSG nicht ausdrücklich enthalten. Er wird deshalb in Artikel 18 SDSG eingeführt. Der Wortlaut ist beispielsweise an Artikel 108 des Bundesgesetzes vom 17. Juni 2005 über das Bundesgericht[37] angelehnt.

Die Ausnahme nach dem zweiten Satz von Absatz 1 ist eng auszulegen. Dies gilt in zweifacher Hinsicht. Einerseits darf das Bundesorgan nicht leichthin annehmen, ein Auskunftsgesuch sei offensichtlich unbegründet oder querulatorisch. Andererseits hat es selbst für den Fall, dass ein solches Gesuch vorliegt, die für die betroffene Person günstigste Lösung zu wählen. Es muss sich daher soweit als möglich damit begnügen, die Auskunft lediglich einzuschränken oder allenfalls aufzuschieben. Nur in den absolut eindeutigen, offensichtlichen Fällen kann es die Auskunft ganz verweigern. In jedem Fall hat es die betroffene Person über den Grund für die Verweigerung der Auskunft zu informieren (Art. 9 Abs. 5 DSG).

Das Auskunftsrecht kann ohne Nachweis eines Interesses und ohne eine Begründung geltend gemacht werden. Auch blosse Neugier reicht aus. Das Bundesorgan darf daher grundsätzlich keine Begründung des Auskunftsgesuchs fordern. Das Bundesgericht hat jedoch festgehalten, dass der Auskunftspflichtige eine Begründung für das Auskunftsbegehren verlangen kann, wenn im konkreten Fall eine rechtsmissbräuchliche Nutzung des Auskunftsrechts in Frage steht.[38] Als möglicherweise rechtsmissbräuchlich hat das Bundesgericht insbesondere die Verwendung des Auskunftsrechts zu datenschutzwidrigen Zwecken erachtet, beispielsweise um sich die Kosten einer Beweisbeschaffung zu sparen, oder um eine mögli-

---

[36] Siehe Erwägungsgrund 40 der Richtlinie (EU) 2016/680.

[37] SR **173.110**

[38] BGE **138** III 425 E. 5.4 f.; BGE **123** II 534 E. 2e.

che Gegenpartei auszuforschen.[39] Bringt die betroffene Person, welche Auskunft verlangt, anschliessend eine Begründung vor, die sich bereits ohne vertiefte Prüfung und ohne Zweifel als haltlos erweist, darf das Bundesorgan das Auskunftsrecht einschränken. Nur unter diesen Umständen kann ein offensichtlich unbegründetes Auskunftsgesuch vorliegen. Es muss mit anderen Worten offenkundig sein, dass das Auskunftsgesuch aus Gründen gestellt wurde, die nichts mit dem Datenschutz zu tun haben, oder dass dies in anderweitiger (z. B. betrügerischer) Absicht geschehen ist. Bestehen Zweifel, ob es sich um einen solchen Fall handelt, liegt kein offensichtlich unbegründetes Gesuch vor.

Querulatorisch sind Auskunftsgesuche, die beispielsweise ohne plausible Begründung häufig wiederholt werden, oder die sich an ein Bundesorgan richten, von dem die Gesuchstellerin oder der Gesuchsteller bereits weiss, dass es keine Daten über sie oder ihn bearbeitet. Auch von einem querulatorischen Gesuch darf das Bundesorgan nicht leichthin ausgehen.

Art. 19 Weitere Ansprüche und Verfahren

Artikel 19 SDSG räumt der betroffenen Person verschiedene Rechtsansprüche ein, um gegen eine widerrechtliche Datenbearbeitung vorzugehen. Die Bestimmung orientiert sich stark am geltenden Artikel 25 DSG, erfährt aber einige Änderungen, die nachfolgend erklärt werden. Um zu vermeiden, dass die Rechtsansprüche in zwei verschiedenen Gesetzen geregelt werden (DSG und SDSG), werden sie alle im SDSG aufgeführt. Damit ist die Rechtssicherheit besser gewährleistet.

Abs. 1: Unterlassungs-, Beseitigungs- und Feststellungsbegehren

Absatz 1 entspricht – abgesehen von geringfügigen sprachlichen Anpassungen – dem heutigen Artikel 25 Absatz 1 DSG.

Abs. 2: Weitere Begehren

Im geltenden Recht ergibt sich der Anspruch der betroffenen Person, die *Löschung* ihrer Daten zu verlangen, implizit aus Artikel 25 DSG. Um den Anforderungen von Artikel 16 Absatz 2 der Richtlinie (EU) 2016/680 besser Rechnung zu tragen, wird dieser Anspruch im SDSG nun ausdrücklich in Artikel 19 Absatz 2 genannt. Des Weiteren setzt Absatz 2 – wie heute Artikel 25 Absatz 3 DSG – das in Artikel 16 Absatz 1 der Richtlinie (EU) 2016/680 gewährleistete Recht auf *Berichtigung* um.

In Absatz 2 Buchstabe a wird im Vergleich zu Artikel 25 Absatz 3 Buchstabe a DSG der letzte Teilsatz betreffend die Sperrung der Bekanntgabe an Dritte gelöscht, weil ein solcher Widerspruch gegen die Datenbekanntgabe abschliessend durch Artikel 20 DSG geregelt ist.[40] Die Sperrung der Bekanntgabe nach Artikel 20 DSG ist nicht an die widerrechtliche Bearbeitung gebunden, was bei den Ansprüchen nach Artikel 19 SDSG der Fall ist.

Gemäss Absatz 2 Buchstabe b kann die betroffene Person vom verantwortlichen Bundesorgan verlangen, dass es seinen Entscheid, namentlich über die Berichtigung, Löschung oder Vernichtung, die Sperrung der Bekanntgabe nach Artikel 20 DSG (zumindest für den Fall der widerrechtlichen Bekanntgabe) oder den Bestreitungsvermerk nach Artikel 19 Absatz 4 SDSG veröffentlicht oder Dritten mitteilt. Diese Bestimmung entspricht im Wesentlichen dem geltenden Artikel 25 Absatz 3 Buchstabe b DSG.

---

[39] BGE **138** III 425 E. 5.5.

[40] 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.

Abs. 3: Einschränkung der Bearbeitung

In Absatz 3 wird eine neue Regelung eingeführt, um Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680 umzusetzen. Nach dieser Bestimmung kann das verantwortliche Bundesorgan in bestimmten Fällen die Datenbearbeitung einschränken, anstatt die umstrittenen Daten zu löschen.

Mit Absatz 3 wird somit eine Massnahme vorgesehen, die weniger radikal ist als die Löschung oder Vernichtung der umstrittenen Personendaten. Die Bestimmung ist in dem Sinne auszulegen, dass die Daten weiter bearbeitet werden dürfen, jedoch nur zu bestimmten Zwecken. Es geht nicht darum, jegliche Art der Datenbearbeitung auszuschliessen. Gemäss dem Erwägungsgrund 47 der Richtlinie (EU) 2016/680 ist die Einschränkung der Bearbeitung so zu verstehen, dass das Bundesorgan die betreffenden Daten nur zu dem Zweck bearbeiten darf, der ihrer Löschung entgegensteht. Absatz 3 sieht dafür vier Konstellationen vor.

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

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

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

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

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

Abs. 4: Bestreitungsvermerk

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

Abs. 5: Verfahren nach dem Verwaltungsverfahrensgesetz

Gemäss Absatz 5 richtet sich das Verfahren zur Geltendmachung der Ansprüche der betroffenen Person nach dem Verwaltungsverfahrensgesetz vom 20. Dezember 1968[41] (VwVG). Diese Regelung entspricht dem geltenden Artikel 25 Absatz 4 DSG.

Abs. 6: Vorbehalt der Spezialbestimmungen

Absatz 6 behält die Spezialbestimmungen zu den Rechtsansprüchen der betroffenen Person in anderen Bundesgesetzen vor, namentlich die neu eingeführten Bestimmungen im StGB, in der StPO oder im IRSG.

Art. 20 Verfahren im Falle der Bekanntgabe von amtlichen Dokumenten, die Personendaten enthalten

Bei Artikel 20 SDSG handelt es sich um eine Bestimmung zur Koordination des SDSG mit dem Bundesgesetz vom 17. Dezember 2004[42] über das Öffentlichkeitsprinzip der Verwaltung in Bezug auf das Verfahren. Er entspricht Artikel 25bis DSG, ausser dass er auf Artikel 19 SDSG verweist. Der Anwendungsbereich von Artikel 20 SDSG ist jedoch eingeschränkt, da das BGÖ gemäss dessen Artikel 3 Absatz 1 Buchstabe a nicht für den Zugang zu amtlichen Dokumenten betreffend Strafverfahren (Ziff. 2), Verfahren der internationalen Rechts- und Amtshilfe (Ziff. 3) sowie Verfahren der Staats- und Verwaltungsrechtspflege (Ziff. 5) gilt.

2.5 Aufsicht

In den Artikeln 21–25 SDSG werden die Artikel 45–47 der Richtlinie (EU) 2016/680 umgesetzt. Damit werden auch die Empfehlungen erfüllt, welche die Europäische Union bei der Schengen-Evaluierung des Jahres 2014 gegenüber der Schweiz abgegeben hatte und wonach der Beauftragte Verfügungskompetenzen erhalten sollte.

Art. 21 Beauftragter

Nach Absatz 1 ist der Beauftragte die Behörde, welche die Anwendung der bundesrechtlichen Datenschutzvorschriften überwacht. Er kann die Bundesorgane sowie die Auftragsbearbeiter im Geltungsbereich des SDSG beaufsichtigen.

Mit Absatz 2 werden jedoch verschiedene Behörden, beispielsweise die eidgenössischen Gerichte (Bst. a), von der Aufsicht des Beauftragten ausgenommen. Diese Ausnahmen liegen im Wesentlichen darin begründet, dass die Unterstellung der genannten Behörden unter die Aufsicht des Beauftragten die Gewaltenteilung und die Unabhängigkeit der Justiz beeinträchtigen würde. Sie entsprechen den Anforderungen nach Artikel 45 Absatz 2 der Richtlinie (EU) 2016/680.

Soweit sie Personendaten im Rahmen von Strafverfahren bearbeitet, ist nach Buchstabe b auch die Bundesanwaltschaft von der Aufsicht durch den Beauftragten ausgenommen.[43]

---

41 SR **172.021**

42 SR **152.3**

43 Vgl. Erwägungsgrund 80 der Richtlinie (EU) 2016/680 sowie Artikel 18 dieser Richtlinie.

Gemäss Buchstabe c sind schliesslich Bundesbehörden von der Aufsicht des Beauftragten ausgenommen, soweit sie Personendaten im Rahmen von Verfahren der internationalen Rechtshilfe in Strafsachen bearbeiten. Diese Ausnahme betrifft hauptsächlich die Bundesanwaltschaft und das Bundesamt für Justiz. Nach der Erklärung des Bundesrates zu Artikel 1 des Europäischen Übereinkommens vom 20. April 1959[44] über die Rechtshilfe in Strafsachen ist das Bundesamt für Justiz als schweizerische Justizbehörde im Sinne des Übereinkommens zu betrachten. Die Ausnahme ist allerdings von beschränkter Tragweite. Denn der Beauftragte kann die Rechtmässigkeit einer Datenbearbeitung überprüfen, wenn eine betroffene Person ihre Rechte nach Artikel 11*c* IRSG geltend macht.

Art. 22 Untersuchung

Mit dieser Bestimmung wird Artikel 46 Absatz 1 Buchstabe i der Richtlinie (EU) 2016/680 umgesetzt.

Abs. 1: Eröffnung der Untersuchung

Gemäss Absatz 1 eröffnet der Beauftragte von Amtes wegen oder auf Anzeige hin eine Untersuchung, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Wie die Richtlinie (EU) 2016/680 dies vorsieht, kann die Untersuchung gegen das verantwortliche Bundesorgan oder den Auftragsbearbeiter eröffnet werden. Die Anzeige kann durch einen Dritten oder durch die betroffene Person erfolgen. Unter Vorbehalt einer Spezialbestimmung[45] hat die Person, die Anzeige erstattet, im Verfahren jedoch keine Parteistellung (siehe den Vorbehalt nach Art. 25 Abs. 2 SDSG). Falls die betroffene Person Anzeige erstattet hat, muss der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung informieren (Abs. 4). Die betroffene Person muss ihre Rechte mit den anwendbaren Rechtsmitteln geltend machen, d. h. sie kann bei einem Zivilgericht Klage erheben, wenn es um den Auftragsbearbeiter geht, oder sie kann gegen den Entscheid des verantwortlichen Bundesorgans Beschwerde führen. Dies entspricht dem geltenden Recht.

Wie im Erwägungsgrund 82 der Richtlinie (EU) 2016/680 dargelegt wird, dürfen die Befugnisse des Beauftragten die speziellen Verfahrensvorschriften wie diejenigen für das Strafverfahren nicht berühren. Bei seiner Untersuchung beschränkt er sich somit darauf, zu prüfen, ob die Bearbeitung in Bezug auf die datenschutzrechtlichen Anforderungen rechtmässig ist. Im Falle eines Fehlers bei der Datenbearbeitung kann er gegenüber dem betreffenden Bundesorgan oder dem Auftragsbearbeiter Verwaltungsmassnahmen ergreifen (Art. 24 SDSG). Dies könnte beispielsweise der Fall sein, wenn die Sicherheit der Daten nicht gewährleistet ist oder wenn unberechtigte Dritte Zugriff auf die Daten haben.

Abs. 2: Verzicht auf die Eröffnung einer Untersuchung

Der Beauftragte kann von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist. Absatz 2 kann auch zur Anwendung gelangen, wenn der Beauftragte der Auffassung ist, dass die Beratung des Bundesorgans oder des Auftragsbearbeiters ausreicht, um eine an sich kaum problematische Situation zu beseitigen.

Abs. 3: Mitwirkungspflichten

Absatz 3 regelt die Mitwirkungspflichten des Bundesorgans und des Auftragsbearbeiters, indem die Regelung nach den Artikeln 27 Absatz 3 und 29 Absatz 2 DSG übernommen wird. Die Verfahrenspartei hat dem Beauftragten sämtliche Auskünfte zu erteilen und alle Unterla-

---

[44] SR **0.351.1**

[45] Siehe Art. 349*h* Abs. 3 StGB.

gen zur Verfügung zu stellen, welche dieser für die Untersuchung benötigt. In Absatz 3 zweiter Satz ist festgehalten, dass sich das Auskunftsverweigerungsrecht nach den Artikeln 16 und 17 VwVG richtet. Artikel 16 Absatz 1 VwVG verweist auf Artikel 42 Absätze 1 und 3 des Bundesgesetzes vom 4. Dezember 1947[46] über den Bundeszivilprozess. Nach dieser Bestimmung können die befragten Personen das Zeugnis verweigern, wenn die Beantwortung der Frage sie der Gefahr einer strafgerichtlichen Verfolgung aussetzen kann.

Art. 23 Befugnisse

Diese Bestimmung erfüllt die Anforderungen von Artikel 47 Absatz 1 der Richtlinie (EU) 2016/680, wonach die Schengen-Staaten wirksame Untersuchungsbefugnisse für die Aufsichtsbehörde vorzusehen haben, namentlich die Befugnis, von dem für die Datenbearbeitung Verantwortlichen und dem Auftragsbearbeiter Zugang zu allen Daten, die bearbeitet werden, und zu allen für die Erfüllung ihrer Aufgaben notwendigen Informationen zu erhalten.

Abs. 1: Untersuchungsmassnahmen

Die Massnahmen nach Absatz 1 dürfen nur angeordnet werden, wenn eine Untersuchung eröffnet worden ist und soweit das Bundesorgan oder der Auftragsbearbeiter seinen Mitwirkungspflichten nicht nachkommt. Der Beauftragte kann die Massnahmen nach den Buchstaben a–d mit anderen Worten nur anordnen, wenn er vergeblich versucht hat, die Mitwirkung des verantwortlichen Bundesorgans oder des Auftragsbearbeiters einzuholen.

Der Katalog der Massnahmen nach Absatz 1 gleicht jenem nach Artikel 12 VwVG. Es handelt sich um eine nicht abschliessende Liste. Der Beauftragte ist unter anderem befugt, Zugang zu allen Auskünften, Unterlagen, Bearbeitungsverzeichnissen und Personendaten zu verlangen, die für die Untersuchung erforderlich sind (Bst. a), oder Zugang zu Räumlichkeiten und Anlagen zu verlangen (Bst. b). Wie alle Bundesbehörden muss er die geltenden Rechtsvorschriften beachten, namentlich jene zum Datenschutz und zur Wahrung von Fabrikations- und Geschäftsgeheimnissen. Er untersteht ausserdem dem Amtsgeheimnis nach Artikel 22 des Bundespersonalgesetzes vom 24. März 2000[47] (BPG). Folglich ist die vertrauliche Behandlung der Personendaten, zu denen er in Ausübung seiner Aufsichtsaufgaben Zugang erhält, gewährleistet, namentlich wenn er die Person, die Anzeige erstattet hat, über das Ergebnis einer allfälligen Untersuchung informiert (Art. 22 Abs. 4 SDSG) oder wenn er seinen Tätigkeitsbericht nach Artikel 30 DSG veröffentlicht.

Abs. 2: Vorsorgliche Massnahmen

Absatz 2 verleiht dem Beauftragten die Befugnis, für die Dauer der Untersuchung vorsorgliche Massnahmen anzuordnen. 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 seinen Untersuchungen feststellt, dass den betroffenen Personen ein nicht leicht wiedergutzumachender Nachteil droht. Da Artikel 24 SDSG dem Beauftragten Verfügungskompetenzen erteilt, braucht es das Bundesverwaltungsgericht für die Anordnung vorsorglicher Massnahmen nicht mehr. Das Verfahren für Beschwerden gegen vorsorgliche Massnahmen richtet sich nach Artikel 44 ff. VwVG. Die aufschiebende Wirkung der Beschwerde wird durch Artikel 55 VwVG geregelt.

[46] SR **273**

[47] SR **172.220.1**

Art. 24 Verwaltungsmassnahmen

Artikel 24 SDSG setzt Artikel 47 Absatz 2 der Richtlinie (EU) 2016/680 um.

Absatz 1 lässt dem Beauftragten einen grossen Handlungsspielraum. Denn es handelt sich um eine Kann-Bestimmung und er ist nicht verpflichtet, Verwaltungsmassnahmen zu ergreifen.

Artikel 24 umfasst eine Reihe von Massnahmen bei Datenbearbeitungen, die gegen die Datenschutzvorschriften verstossen. Die Massnahmen reichen von einer einfachen Verwarnung (Abs. 3) bis zur Verfügung, Personendaten zu vernichten (Abs. 1).

Nach Absatz 2 kann der Beauftragte des Weiteren die Bekanntgabe von Personendaten aufschieben oder untersagen, wenn sie gegen die anwendbaren gesetzlichen Bestimmungen betreffend die Bekanntgabe von Personendaten an einen Drittstaat oder an ein internationales Organ, d. h. gegen die Artikel 349*c*–349*e* StGB verstösst. Dabei ist darauf hinzuweisen, dass die Bekanntgabe von Daten an Schengen-Staaten in Absatz 2 nicht erwähnt wird. Denn diese unterliegt denselben Bedingungen wie die Bekanntgabe von Daten an schweizerische Strafbehörden (siehe Art. 8 Abs. 1 SDSG).

Grundsatz dieser Regelung ist die Wahrung der Verhältnismässigkeit. So kann der Beauftragte, statt den Abbruch der Datenbearbeitung anzuordnen, eine vorschriftsgemässe Datenbearbeitung anordnen und die Massnahme nur auf den problematischen Teil der Bearbeitung beschränken.

Unter Vorbehalt der Ausnahme nach Artikel 25 Absatz 2 SDSG eröffnet der Beauftragte seine Verfügung ausschliesslich dem Bundesorgan oder dem Auftragsbearbeiter, das oder der Partei des Untersuchungsverfahrens ist. Die angeordnete Massnahme ist genau zu begründen.

Art. 25 Verfahren

Nach Absatz 1 unterstehen das Untersuchungsverfahren sowie die Verfügungen nach den Artikeln 23 und 24 SDSG dem Verwaltungsverfahrensgesetz. Das Bundesorgan oder der Auftragsbearbeiter, das oder der in der Untersuchung Partei ist, hat insbesondere Anspruch auf Gewährung des rechtlichen Gehörs (Art. 29 ff. VwVG).

Absatz 2 präzisiert, dass nur das Bundesorgan oder der Auftragsbearbeiter, gegen das bzw. den eine Untersuchung eröffnet wurde, Verfahrenspartei sein kann. Grundsätzlich können lediglich diese gegen Verfügungen des Beauftragten Beschwerde erheben. Die betroffene Person hat im Verfahren auch dann keine Parteistellung, wenn der Beauftragte die Untersuchung auf ihre Anzeige hin eröffnet hat. Sie muss also gegen das verantwortliche Bundesorgan vorgehen (Art. 19 SDSG), indem sie dessen Entscheid bei der zuständigen Beschwerdeinstanz anficht. Dies bleibt unverändert zum geltenden Recht. Absatz 2 behält jedoch Artikel 349*h* StGB vor, wonach die betroffene Person unter bestimmten Voraussetzungen vom Beauftragten die Eröffnung einer Untersuchung verlangen und gegebenenfalls gegen den Entscheid des Beauftragten als Partei Beschwerde erheben kann.

Nach Absatz 3 kann der Beauftragte Beschwerdeentscheide des Bundesverwaltungsgerichts beim Bundesgericht anfechten, wie er dies bereits aktuell gemäss Artikel 27 Absatz 6 und Artikel 29 Absatz 4 DSG tun kann.

2.6 Amtshilfe zwischen dem Beauftragten und ausländischen Behörden

Art. 26

Artikel 26 SDSG regelt die Amtshilfe zwischen dem Beauftragten und den Datenschutzbehörden der Schengen-Staaten. Diese neue Bestimmung überträgt Artikel 50 der Richtlinie (EU) 2016/680 ins schweizerische Recht, denn der derzeit geltende Artikel 31 Absatz 1 Buchstabe c DSG beschränkt sich darauf, den Beauftragten zur Zusammenarbeit mit ausländischen Datenschutzbehörden zu verpflichten.

Abs. 1: Voraussetzungen

Gemäss Absatz 1 kann der Beauftragte unter bestimmten Voraussetzungen (Bst. a–e) mit den für den Datenschutz zuständigen Behörden der Schengen-Staaten für die Erfüllung ihrer jeweiligen gesetzlich vorgesehenen Aufgaben im Bereich des Datenschutzes Informationen oder Personendaten austauschen.

Nach der ersten Voraussetzung (Bst. a) muss zwischen der Schweiz und dem Schengen-Staat die Gegenseitigkeit der Amtshilfe im Datenschutzbereich sichergestellt sein. Zweitens dürfen die ausgetauschten Informationen und Personendaten nach dem Spezialitätsgrundsatz nur für das fragliche Datenschutzverfahren verwendet werden, das dem Amtshilfeersuchen zugrunde liegt (Bst. b). Wenn die Daten anschliessend in einem Strafverfahren verwendet werden sollen, gelten die Grundsätze der internationalen Rechtshilfe in Strafsachen. Die dritte und die vierte Voraussetzung gewährleisten die Wahrung der Berufsgeheimnisse sowie der Geschäfts- und Fabrikationsgeheimnisse (Bst. c) und verbieten, dass die Informationen und Personendaten ohne vorgängige Genehmigung der Behörde, die sie übermittelt hat, bekanntgegeben werden (Bst. d). Schliesslich muss die empfangende Behörde die Auflagen und Einschränkungen der Behörde einhalten, die ihr die Informationen und Personendaten übermittelt hat (Bst. e).

Abs. 2: Bekanntgabe von Personendaten

Absatz 2 Buchstaben a–g bestimmt, welche Angaben der Beauftragte der Behörde eines Schengen-Staates bekanntgeben darf, um sein Amtshilfegesuch zu begründen oder dem Ersuchen einer Behörde eines Schengen-Staates Folge zu leisten. Die Identität der betroffenen Personen darf nur weitergeleitet werden, wenn dies für die Erfüllung der gesetzlichen Aufgaben des Beauftragten oder der Behörde des Schengen-Staates unentbehrlich ist (Abs. 2 Bst. c).

Abs. 3: Stellungnahme

Bevor der Beauftragte in einem Amtshilfeverfahren einer für den Datenschutz zuständigen Behörde eines Schengen-Staates Informationen bekanntgibt, die Berufs-, Geschäfts- oder Fabrikationsgeheimnisse enthalten können, informiert er die betroffenen Personen und lädt sie zur Stellungnahme ein. Von dieser Pflicht ist er jedoch entbunden, wenn die Information nicht möglich ist oder einen unverhältnismässigen Aufwand erfordert.

2.7 Übergangsbestimmung betreffend laufende Verfahren

Art. 27

Zur Gewährleistung der Rechtssicherheit und Einhaltung des Grundsatzes von Treu und Glauben schreibt diese Bestimmung vor, dass Untersuchungen des Beauftragten, die im Zeitpunkt des Inkrafttretens des SDSG hängig sind, sowie hängige Beschwerden gegen erstinstanzliche Entscheide dem bisherigen Recht unterstehen. Dies betrifft sowohl die materiel-

len Datenschutzvorschriften als auch die Befugnisse des Beauftragten und die weiteren anwendbaren Verfahrensvorschriften.

3 Erläuterungen zu den Änderungen des DSG

Art. 26 Abs. 3 erster Satz

Absatz 3 erster Satz konkretisiert die Unabhängigkeit des Beauftragten mit der Präzisierung, dass er keine Weisungen einer Behörde oder eines Dritten einholen oder erhalten darf. Diese Änderung berücksichtigt die Anforderungen von Artikel 42 Absätze 1 und 2 der Richtlinie (EU) 2016/680.

Art. 26a Abs. 1 und 1bis

Gegenwärtig kann 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. Letztere Bestimmung sieht vor, dass die Schengen-Staaten regeln müssen, ob und wenn ja wie oft das Mitglied oder die Mitglieder der Aufsichtsbehörde wiederernannt werden können. Demgemäss haben die Schengen-Staaten also die Wahl, ob und wie oft eine Wiederernennung der Aufsichtsbehörde möglich ist.

Entsprechend dem Handlungsspielraum, den Artikel 44 der Richtlinie (EU) 2016/680 gewährt, kann der Beauftragte zwei Mal wiederernannt werden. Dieser kann daher für höchstens zwölf Jahre im Amt bleiben. Durch diese Massnahme soll die Unabhängigkeit des Beauftragten als Behörde gestärkt werden. Er soll nicht aus Furcht, nicht wiedergewählt zu werden, in der Erfüllung seines gesetzlichen Auftrags zurückgehalten werden. Wenn der Beauftragte während der Amtsdauer das Pensionsalter erreicht, endet das Arbeitsverhältnis automatisch bei Erreichen des Alters nach Artikel 21 des Bundesgesetzes vom 20. Dezember 1946[48] über die Alters- und Hinterlassenenversicherung (AHVG) (Art. 10 Abs. 1 BPG in Verbindung mit Art. 14 Abs. 1 BPG).

Absatz 1bis entspricht – unter Vorbehalt gewisser redaktioneller Anpassungen – dem bisherigen Absatz 1 von Artikel 26*a* DSG.

Art. 26b Nebenbeschäftigung

In Artikel 26*b* werden die Voraussetzungen für die Ausübung einer Nebenbeschäftigung durch den Beauftragten verschärft. Mit dieser Bestimmung werden die Anforderungen von Artikel 42 Absatz 3 der Richtlinie (EU) 2016/680 umgesetzt. Die Bestimmung gilt nur für den Beauftragten. Dessen Stellvertreterin oder Stellvertreter sowie das Sekretariat unterstehen dem BPG.

Nach Artikel 26*b* DSG ist heute lediglich vorgesehen, dass der Bundesrat dem Beauftragten gestatten kann, eine andere Beschäftigung auszuüben, wenn dadurch dessen Unabhängigkeit und Ansehen nicht beeinträchtigt werden. Artikel 26*b* Absatz 1 erster Satz SDSG hält hingegen den Grundsatz fest, wonach der Beauftragte keine zusätzliche Erwerbstätigkeit ausüben darf. Dies gilt unabhängig davon, ob eine solche Tätigkeit vergütet würde oder nicht. Diese Bestimmung weicht von Artikel 41 Absatz 1 zweiter Satz des E-DSG des Bundesrates ab.

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

---

[48] SR **831.10**

Art. 31 Abs. 1 Bst. h

Um den Anforderungen der Richtlinie (EU) 2016/680 (Art. 46 Abs. 1 Bst. b) Rechnung zu tragen, wird der Katalog der Aufgaben des Beauftragten um eine neue Aufgabe erweitert: Er sensibilisiert die Bevölkerung für den Datenschutz.

4 Erläuterungen zur Änderung der weiteren Erlasse zum Datenschutz

Die Änderungen der weiteren Bundesgesetze zur Umsetzung der Anforderungen der Richtlinie (EU) 2016/680 werden in der Botschaft des Bundesrates vom 15. September 2017[49] erläutert.

[49] BBl **2017** 6941, 7152