Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht

31. August 2022

Verordnung über den Datenschutz (Datenschutzverordnung, DSV)

Erläuternder Bericht

BJ-D-DB3D3401/217

Inhaltsverzeichnis

1 Ausgangslage

1.1 Kontext

Aufgrund einer Evaluation des Bundesgesetzes vom 19. Juni 1992[1] über den Datenschutz (DSG) und mit Blick auf die technologische Entwicklung und das weiterentwickelte EU-Recht beschloss der Bundesrat, das Bundesgesetz über den Datenschutz zu revidieren. Am 15. September 2017 verabschiedete er die Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz[2]. Die Vorlage umfasst zum einen eine Totalrevision des DSG (nDSG), zum andern eine Teilrevision weiterer Bundesgesetze, womit insbesondere auch die Richtlinie (EU) 2016/680[3] umgesetzt werden soll. Das Parlament hat die Vorlage des Bundesrates in zwei Etappen aufgeteilt. In der ersten Etappe wurde nur die Schengen-relevante Richtlinie (EU) 2016/680 zum Datenschutz in Strafsachen umgesetzt. Das Bundesgesetz vom 28. September 2018[4] über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (SDSG) ist am 1. März 2019 in Kraft getreten. In einer zweiten Etappe hat das Parlament das neue Datenschutzgesetz (nDSG) beraten und am 25. September 2020 verabschiedet[5].

Aufgrund der Totalrevision des DSG müssen auch die dazugehörigen Verordnungen, namentlich die Verordnung zum Bundesgesetz über den Datenschutz (VDSG)[6] und die Verordnung über die Datenschutzzertifizierungen (VDSZ)[7], angepasst werden.

1.2 Grundzüge des nDSG

Das nDSG regelt die Bearbeitung von Personendaten natürlicher Personen durch private Personen und durch Bundesorgane (Art. 2 Abs. 1). Nicht anwendbar ist es indessen auf Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet (Art. 2 Abs. 2 Bst. a). Ausgenommen sind auch Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden (Art. 2 Abs. 2 Bst. b), sowie Personendaten, die von institutionell Begünstigten, die in der Schweiz Immunität von der Gerichtsbarkeit geniessen, bearbeitet werden (Art. 2 Abs. 2 Bst. c). Das anwendbare Verfahrensrecht regelt die Bearbeitung von Personendaten und die Rechte der betroffenen Personen in Gerichtsverfahren und in Verfahren nach bundesrechtlichen Verfahrensordnungen. Auf erstinstanzliche Verwaltungsverfahren sind dagegen die Bestimmungen des nDSG anwendbar (Art. 2 Abs. 3). Die öffentlichen Register des Privatrechtsverkehrs werden vorwiegend durch die Spezialbestimmungen des anwendbaren Bundesrechts geregelt (Art. 2 Abs. 4). Das Parlament ergänzte einen Artikel zum räumlichen Geltungsbereich des nDSG (Art. 3). Dieser präzisiert, dass das Gesetz auch für im Ausland veranlasste Sachverhalte gilt, wenn sie sich in der Schweiz auswirken. Zudem wird darin auf

---

1 SR **235.1**

2 BBl **2017** 6941

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

4 SR **235.3**

5 BBl **2020** 7639

6 SR **235.11**

7 SR **235.13**

das Bundesgesetz vom 18. Dezember 1987[8] über das Internationale Privatrecht (IPRG) verwiesen. Artikel 4 umschreibt die Funktion des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Das zweite Kapitel enthält allgemeine Bestimmungen zur Bearbeitung von Personendaten.

Artikel 5 enthält einen Begriffskatalog. Hervorzuheben ist, dass im neuen Gesetz der Begriff «Inhaber der Datensammlung» durch «Verantwortlicher» ersetzt wird (Art. 5 Bst. j nDSG). Der Begriff «Profiling mit hohem Risiko» wurde später von den eidgenössischen Räten eingeführt (Art. 5 Bst. g).

Artikel 6 legt einige allgemeine Grundsätze fest. Personendaten müssen rechtmässig bearbeitet werden (Art. 6 Abs. 1). Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein (Art. 6 Abs. 2). Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden (Art. 6 Abs. 3). Die Daten müssen vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 6 Abs. 4). Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern (Art. 6 Abs. 5). Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, Personendaten durch Technik und datenschutzfreundliche Voreinstellungen zu schützen («privacy by design and by default»; Art. 7) und die Datensicherheit zu gewährleisten (Art. 8). Aufgrund von Artikel 10 können Verantwortliche eine Datenschutzberaterin oder einen Datenschutzberater ernennen. Überdies müssen sie ein Verzeichnis der Bearbeitungstätigkeiten erstellen (Art. 12).

Artikel 9 regelt die Datenbearbeitung durch Auftragsbearbeiter. Das nDSG kodifiziert das Instrument der Verhaltenskodizes (Art. 11).

Im 2. Kapitel hat das Parlament einen zusätzlichen Abschnitt eingefügt. Er bezieht sich auf die Datenbearbeitung durch private Verantwortliche mit Sitz oder Wohnsitz im Ausland. In Artikel 14 wird der Begriff «Vertretung» eingeführt. Die Pflichten der Vertretung sind in Artikel 15 festgelegt.

Der 3. Abschnitt des 2. Kapitels behandelt die Bekanntgabe von Personendaten ins Ausland. Personendaten dürfen nur ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass der betreffende Staat oder das betreffende internationale Organ einen angemessenen Schutz bietet (Art. 16). Artikel 17 sieht allerdings verschiedene Ausnahmen vor.

Das 3. Kapitel regelt die Pflichten des Verantwortlichen. Es präzisiert die Pflicht, bei der Beschaffung von Personendaten die betroffenen Personen zu informieren (Art. 19 und 20). In Artikel 21 wird eine neue Informationspflicht bei automatisierten Einzelentscheiden eingeführt, in Artikel 22 die Pflicht, eine Datenschutz-Folgenabschätzung zu erstellen. Der Verantwortliche muss zudem vor der Datenbearbeitung die Stellungnahme des EDÖB einholen, wenn die Datenschutz-Folgenabschätzung ergibt, dass die geplante Bearbeitung trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat (Art. 23). Ausserdem muss der Verantwortliche dem EDÖB eine Verletzung der Datensicherheit melden, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt (Art. 24).

[8] SR **291**

Die Rechte der betroffenen Person sind im 4. Kapitel festgelegt. Das Auskunftsrecht und dessen Einschränkungen sind in den Artikeln 25–27 geregelt. Das Recht auf Datenportabilität und dessen Einschränkungen wurden vom Parlament eingeführt (Art. 28 und 29).

Das 5. Kapitel enthält eine Reihe von Bestimmungen zur Datenbearbeitung durch Private. So dürfen private Personen, die Personendaten bearbeiten, die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen (Art. 30 Abs. 1). Insbesondere dürfen sie Personendaten nicht entgegen den Grundsätzen nach den Artikeln 6 und 8 nDSG oder entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeiten, sofern nicht ein Rechtfertigungsgrund vorliegt (Art. 30 Abs. 2 Bst. a und b sowie Art. 31). Schliesslich regelt dieses Kapitel auch die zivilrechtlichen Ansprüche, die Geschädigte geltend machen können (Art. 32).

Ein sechstes Kapitel (Art. 33–42) regelt die Datenbearbeitung durch Bundesorgane. Diese dürfen Personendaten grundsätzlich nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Art. 34 Abs. 1). Artikel 41 regelt die Rechtsansprüche, die betroffene Personen gegenüber einem für die Bearbeitung von Personendaten verantwortlichen Bundesorgan geltend machen können.

Organisation und Kompetenzen des EDÖB sind im 7. Kapitel festgelegt. Die Leiterin oder der Leiter des EDÖB (die oder der Beauftragte) wird von der Bundesversammlung gewählt (Art. 43 Abs. 1). Dieses neue Verfahren haben die eidgenössischen Räte eingeführt. Amtsdauer, Wiederwahl und Beendigung der Amtsdauer sind in Artikel 44 geregelt, die Ausübung von Nebenbeschäftigungen in Artikel 47. Bestimmungen zum Budget des EDÖB (Art. 45) und zu den Unvereinbarkeiten mit dem Amt der oder des Beauftragten (Art. 46) wurden vom Parlament eingefügt. In Artikel 48, der letzten Bestimmung dieses 1. Abschnitts über die Organisation des EDÖB, geht es um die Selbstkontrolle des EDÖB. Der 2. Abschnitt regelt die Untersuchungen, die der EDÖB führen kann. Vorgesehen ist, dass der EDÖB von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnet, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte (Art. 49 Abs. 1). Der EDÖB hat bestimmte Befugnisse (Art. 50) und kann Verwaltungsmassnahmen ergreifen (Art. 51). Der 3. Abschnitt enthält Bestimmungen zur Amtshilfe zwischen dem EDÖB und anderen schweizerischen (Art. 54) oder ausländischen Behörden (Art. 55). Das nDSG weist dem EDÖB weitere Aufgaben zu (Art. 56–58), insbesondere auch das Führen eines Registers der Bearbeitungstätigkeiten der Bundesorgane (Art. 56). Für einige Dienstleistungen erhebt der EDÖB von privaten Personen Gebühren (Art. 59).

Das nDSG enthält einen Katalog von Strafbestimmungen, die bei der Verletzung verschiedener gesetzlicher Pflichten anwendbar sind (Kap. 8, Art. 60–66), sowie eine Reihe von Schlussbestimmungen (Kap. 10, Art. 68–74), darunter insbesondere auch die Übergangsbestimmung betreffend Daten juristischer Personen (Art. 71), die für die Anpassung der sektoriellen Verordnungen wichtig ist (vgl. Anhang 2 DSV).

Die Totalrevision des DSG zieht die Änderung zahlreicher sektorieller Gesetze nach sich. Aufgrund der Revision der VDSG müssen auch mehrere Verordnungen geändert werden.

1.3 Verfassungsmässigkeit und Vereinbarkeit mit internationalen Verpflichtungen

Die Verordnung zum Bundesgesetz über den Datenschutz ist eine Ausführungsverordnung zum Datenschutzgesetz, welches am 25. September 2020 vom Parlament revidiert wurde. In diesem Sinn entspricht sie dem Gesetz und es kann in Bezug auf die rechtlichen Aspekte auf

die Erläuterungen in der Botschaft (siehe BBl *2017* 6941, insbesondere 7184 ff.) verwiesen werden.

2 Grundzüge der Vorlage

Nachfolgend werden die zentralen Neuerungen der Totalrevision der VDSG skizziert. Die VDSG wird neu Verordnung über den Datenschutz (Datenschutzverordnung, DSV) genannt.

2.1 Datensicherheit

Artikel 8 Absatz 3 nDSG verpflichtet den Bundesrat, Mindestanforderungen an die Datensicherheit zu definieren. Die neuen Regelungen knüpfen an den geltenden Standard der Datensicherheit von Artikel 8 ff. VDSG an. Die Vorschriften wurden aber überarbeitet und ergänzt, um sie auf den heutigen Stand der Technik abzustimmen und um den Vorgaben der Schengen-relevanten Richtlinie (EU) 2016/680 zu genügen. Es wurde aber auch Wert auf die Kompatibilität mit der DSGVO gelegt, damit Schweizer Unternehmen, die in der EU tätig sind und eine gemäss der DSGVO konforme Datensicherheit gewährleisten, auch in der Schweiz davon ausgehen können, dass sie die Mindestanforderungen erfüllen.

Wie bereits in Artikel 8 Absatz 1 nDSG angelegt, der von einer dem Risiko angemessenen Datensicherheit spricht, gibt die Verordnung nicht starre Mindestanforderungen vor, die für alle gleichermassen gelten, da eine solche Regelung nicht praktikabel wäre. Stattdessen wird auch hier der risikobasierte Ansatz verfolgt: Der Verantwortliche und der Auftragsbearbeiter müssen den Schutzbedarf beurteilen und festlegen, welche Massnahmen angesichts des Risikos zu ergreifen sind. Die Verordnung hält fest, welche Kriterien dabei zu berücksichtigen sind, und gibt Leitlinien vor, wie die Massnahmen auszugestalten sind (Art. 1, 2 und 3 DSV).

Werden besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder wird ein Profiling mit hohem Risiko durchgeführt und können die präventiven Massnahmen den Datenschutz nicht gewährleisten, so müssen der private Verantwortliche und sein privater Auftragsbearbeiter zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren. Eine Protokollierung muss insbesondere dann erfolgen, wenn sonst nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden. Das verantwortliche Bundesorgan und sein Auftragsbearbeiter müssen ihrerseits bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren. Für Datenbearbeitungen, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, wird eine Übergangsfrist von drei Jahren ab Inkrafttreten der Verordnung oder spätestens nach Ende des Lebenszyklus des Systems vorgesehen. Die Dauer für die Aufbewahrung der Protokolle beträgt mindestens ein Jahr (Art. 4 DSV).

Die Verantwortlichen müssen weiterhin ein Bearbeitungsreglement erstellen (Art. 5 f. DSV).

2.2 Bekanntgabe von Personendaten ins Ausland

Der Abschnitt zur Bekanntgabe von Personendaten ins Ausland wurde von Grund auf geändert, da nach dem nDSG nun der Bundesrat festlegt, welche Staaten oder internationalen Organe einen angemessenen Datenschutz gewährleisten. Daher regelt die Verordnung neu die Kriterien, welche der Bundesrat bei seiner Beurteilung berücksichtigt (Art. 8 DSV). Im Anhang 1 sind dann tabellarisch diejenigen Staaten und internationalen Organe aufgeführt, welche über ein angemessenes Datenschutzniveau verfügen. Die Angemessenheit des Datenschutzes wird nach dem Inkrafttreten der Verordnung periodisch neu beurteilt (Art. 8 Abs. 4 DSV).

Des Weiteren werden die in Artikel 16 Absatz 2 nDSG genannten weiteren Möglichkeiten zur Gewährleistung eines geeigneten Datenschutzes (z. B. Standarddatenschutzklauseln) in der Verordnung inhaltlich konkretisiert (Art. 9 ff. DSV).

Schliesslich wurde von der Delegation in Artikel 16 Absatz 3 nDSG, wonach andere geeignete Garantien vorgesehen werden können, Gebrauch gemacht. So dürfen ebenfalls Personendaten bekanntgegeben werden, wenn das angemessene Datenschutzniveau durch einen Verhaltenskodex oder eine Zertifizierung gewährleistet wird (Art. 12 DSV).

2.3 Auskunftsrecht

Wie nach heutigem Recht, muss das Auskunftsbegehren grundsätzlich in schriftlicher oder elektronischer Form gestellt werden. Das Auskunftsrecht wird für den Gesuchsteller zukünftig aber insofern etwas niederschwelliger ausgestaltet, indem das Auskunftsbegehren mit dem Einverständnis des Verantwortlichen auch in mündlicher Form gestellt werden kann.

Weitere Ausführungsbestimmungen zum Auskunftsrecht wurden teilweise aus dem alten Recht übernommen. So wurde die Bestimmung zur Frist für die Auskunftserteilung nur terminologisch und systematisch angepasst (Art. 18 DSV). Auch die Regelung zu den Ausnahmen von der Kostenlosigkeit des Auskunftsrechts (Art. 19 DSV) bleibt mehrheitlich dieselbe, abgesehen davon, dass die Ausnahme des fehlenden schutzwürdigen Interesses gestrichen wurde, da diese gemäss Artikel 26 Absatz 1 Buchstabe c nDSG nun sogar einen Grund zur Verweigerung der Auskunft darstellt.

Nicht in die DSV wurde hingegen die Auskunft über Daten verstorbener Personen übernommen, da deren Regelung in der Verordnung nicht stufengerecht war und ein entsprechender Gesetzesartikel im nDSG vom Parlament abgelehnt wurde.

Mit der Revision wurde auf Gesetzesstufe neu ein Recht auf Datenherausgabe und -übertragung eingeführt. Dabei wurden neue Bestimmungen geschaffen (Art. 20 f. DSV). Trotzdem sollen die meisten Ausführungsbestimmungen des Auskunftsrechts sinngemäss auf dieses Recht Anwendung finden (Art. 22 DSV).

2.4 Datenschutzberaterin bzw. Datenschutzberater

Die bisherigen Bestimmungen zum Datenschutzverantwortlichen (Art. 12*a* und 12*b* VDSG) sowie zum Berater für den Datenschutz in den Departementen und der Bundeskanzlei (Art. 23 VDSG) werden durch diejenigen der Datenschutzberaterin bzw. des Datenschutzberaters ersetzt. Dabei gibt es jeweils eine separate Norm für den privaten Verantwortlichen (Art. 23 DSV) und die Bundesorgane (Art. 25 ff. DSV).

Da die Anforderungen an die Beraterin bzw. den Berater und deren Hauptaufgaben beim privaten Verantwortlichen bereits in Artikel 10 nDSG geregelt werden, beschränkt sich die dazugehörige Verordnungsbestimmung (Art. 23 DSV) hauptsächlich auf die Konkretisierung der Anforderungen, die ein Verantwortlicher erfüllen muss, wenn er eine Datenschutzberaterin oder einen Datenschutzberater einsetzt.

Hingegen wird die Regelung der Beraterin bzw. des Beraters der Bundesorgane dem Bundesrat überlassen. Dabei sollen neu nicht nur die einzelnen Departemente und die Bundeskanzlei, sondern grundsätzlich jedes Bundesorgan eine Beraterin oder einen Berater bezeichnen. Damit aber insbesondere bei kleineren Bundesorganen und solchen mit spezieller Organisationsstruktur keine sinnvollen und ressourceneinsparenden Synergien verloren gehen, können mehrere Bundesorgane gemeinsam eine Datenschutzberaterin oder einen Daten-

schutzberater bezeichnen. Die Anforderungen an sie oder ihn wurden, soweit auf Bundesorgane sinnvoll anwendbar, gleich geregelt wie beim privaten Verantwortlichen und auch die Aufgaben sind im Wesentlichen dieselben.

2.5 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten

Um KMU, die nicht risikobehaftete Datenbearbeitungen vornehmen, administrativ zu entlasten, wurde dem Bundesrat in Artikel 12 Absatz 5 nDSG delegiert, Ausnahmen von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten für Unternehmen mit weniger als 250 Mitarbeitenden vorzusehen. Die Verordnung knüpft die Ausnahme an einen Negativkatalog, welcher die risikobehafteten Datenbearbeitungen (bspw. die Bearbeitung besonders schützenswerter Personendaten in grossem Umfang) aufzählt (Art. 24 DSV). Der Katalog orientiert sich dabei teilweise an der Umschreibung des Begriffs des hohen Risikos bei der Datenschutz-Folgenabschätzung in Artikel 22 Absatz 2 nDSG.

2.6 EDÖB

Auch wenn sich beim EDÖB aus dem nDSG mehrere grundlegende Änderungen ergeben, konnten die Bestimmungen zum Sitz sowie zur Beziehung und Kommunikation mit anderen Behörden mit geringfügigen Anpassungen übernommen werden (vgl. Art. 36–38 DSV). Aufgrund des geänderten Wahlverfahrens, wonach die Leiterin oder der Leiter des EDÖB (die oder der Beauftragte) inskünftig durch die Vereinigte Bundesversammlung gewählt wird (Art. 43 Abs. 1 nDSG), hat die SPK-N im Rahmen der Initiative 21.443 am 27. Januar 2022 einen Entwurf für eine Verordnung der Bundesversammlung verabschiedet, der die Ausführungsbestimmungen zum Arbeitsverhältnis der oder des Beauftragten enthält. Ausserdem sind in diesem Zusammenhang einzelne Änderungen des nDSG vorgesehen. Das Parlament hat die Vorlagen in der Schlussabstimmung vom 17. Juni 2022 angenommen. Das Arbeitsverhältnis des ständigen Sekretariats des EDÖB wird dagegen weiterhin in der DSV geregelt und soll sich wie bisher nach dem Bundespersonalgesetz vom 24. März 2000[9] (BPG) und nach dessen Vollzugsbestimmungen bestimmen (Art. 36 Abs. 2 DSV).

Ausführlicher geregelt wird neu die gesetzliche Grundlage für die Datenbearbeitungen des EDÖB (Art. 39 DSV), die bis anhin nur in allgemeiner Weise in Zusammenhang mit dem Geschäftsverwaltungssystem vorlag. Weiter schreibt Artikel 48 nDSG vor, dass der EDÖB eine Selbstkontrolle einrichten muss, damit die Einhaltung der Datenschutzvorschriften innerhalb der Behörde gewährleistet ist. In der Verordnung werden diese Kontrollmassnahmen definiert (Art. 40 DSV): So hat der EDÖB ein Bearbeitungsreglement für sämtliche seiner automatisierten Bearbeitungen zu erstellen.

3 Auswirkungen

3.1 Finanzielle und personelle Auswirkungen auf den Bund und die Kantone

Eigenständige Auswirkungen auf den Bund aus der DSV ergeben sich nur im Rahmen der Delegationsnormen des nDSG und der Vollzugskompetenz des Bundesrates:

- Bei den Verantwortlichen resultiert aus den angepassten Mindestanforderungen an die Datensicherheit ein Umsetzungsaufwand. Für private Personen ist dieser Aufwand aber generell als eher gering einzustufen, da die Regelung grundsätzlich aus dem bisherigen Recht übernommen und nur punktuell angepasst worden ist. Für Bundesorgane entstehen insbesondere aus der Erweiterung der Protokollierungspflicht zusätzliche Kosten, da hierfür

[9] SR **172.220.1**

einmalige Systemanpassungen vorgenommen werden müssen und dafür mehr Speicherplatz benötigt wird. Die Ausweitung der Protokollierungspflicht ist als eine Weiterentwicklung der Massnahmen anzusehen, die der Bundesrat im Jahr 2009 beschlossen hat (vgl. Bundesratsbeschluss vom 16. Dezember 2009 betreffend Massnahmen zur Erhöhung der Informationssicherheit in der Bundesverwaltung). Die damit verbundenen Kosten können aktuell nicht abschliessend abgeschätzt werden und werden von den betroffenen Verwaltungseinheiten in Budget und Voranschlag eingeplant werden müssen. Um dem Mehraufwand Rechnung zu tragen, wird für die Umsetzung der Protokollierung für Datenbearbeitungen, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, eine Übergangsfrist von drei Jahren vorgesehen. Im Übrigen werden die Protokolle nun während einer Frist von mindestens einem Jahr aufbewahrt und nicht während zwei Jahren, wie dies noch im Vernehmlassungsentwurf vorgesehen war.

- Zu einem gewissen Mehraufwand kann auch der Umstand führen, dass neu grundsätzlich jedes Bundesorgan eine Datenschutzberaterin oder einen Datenschutzberater ernennen muss. Allerdings entspricht dies einer bereits heute schon weitgehend gelebten Praxis, da eine Vielzahl der Bundesämter über Datenschutzberatende verfügt, was den Aufwand begrenzt. Unter Umständen müssen gewisse Bundesorgane ihren Datenschutzberatenden inskünftig allerdings mehr Ressourcen zur Verfügung stellen, da deren Anforderungs- und Aufgabenprofil umfassender geregelt ist als im geltenden Recht. Der Mehraufwand kann variieren, je nach Grösse eines Bundesorgans und dessen Aufgaben. Im Gegenzug kann eine Stärkung der Datenschutzberatenden zu einer gewissen Entlastung des EDÖB beitragen.

Beim Bund ergeben sich insbesondere finanzielle und personelle Auswirkungen auf den EDÖB, da dieser durch das nDSG mehrere neue Aufgaben wahrzunehmen hat, sowie in etwas geringerem Ausmass auf das BJ, welches insbesondere mit der Prüfung des Datenschutzniveaus von anderen Staaten und internationalen Organen eine zusätzliche Aufgabe erhält. Die Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl *2017* 6941, 7171 ff.) sieht daher auch zusätzliche Ressourcen für den EDÖB und das BJ vor.

Die Kantone und Gemeinden sind von der Vorlage nicht betroffen. Vom Geltungsbereich des nDSG und somit auch der DSV sind nur private Personen und Bundesorgane erfasst (Art. 2 Abs. 1 nDSG).

3.2 Auswirkungen auf die Volkswirtschaft

Auswirkungen auf Unternehmen ergeben sich hauptsächlich aus der Totalrevision des DSG. Diese Auswirkungen wurden in der zum DSG durchgeführten Regulierungsfolgenabschätzung[10] berücksichtigt und dargelegt. Eigenständige Auswirkungen durch die DSV, welche in der RFA zum DSG noch nicht untersucht wurden, sind primär bei der Datensicherheit zu erwarten (Voraussichtlich sind diese Auswirkungen insgesamt von begrenzter Relevanz, da die konkreten Vorgaben für die Unternehmen im Vergleich zum geltenden Recht nur leicht angepasst werden. Ausserdem tragen diese Massnahmen teilweise zur Stärkung der Cybersicherheit bei, was zum Vorteil der Unternehmen ist. Es ist von einem gewissen Umsetzungsaufwand auszugehen. Dabei ist zu berücksichtigen, dass sich der Aufwand nach den Risiken, welche die Datenbearbeitungen eines Unternehmens mit sich bringen, richtet. Unternehmen mit einer geringeren datenschutzrechtlichen Exponierung müssen weniger Massnahmen

[10] Regulierungsfolgenabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG) vom 11. Juli 2016 (abrufbar unter: http://www.seco.admin.ch/ > SECO - Staatssekretariat für Wirtschaft > Publikationen & Dienstleistungen > Publikationen > Regulierung > Regulierungsfolgenabschätzung > Vertiefte RFA > Datenschutzgesetz (DSG) (2016)).

treffen als Unternehmen mit grosser datenschutzrechtlicher Exponierung. Dieser Regelungsansatz belässt den Unternehmen gewisse Handlungsspielräume.

Weiter ist die Verabschiedung der Totalrevision der DSV auch mit Blick auf die Gesamtwirtschaft von Bedeutung, denn das Inkrafttreten des neuen Datenschutzrechts ist wichtig mit Blick auf die derzeit laufende Evaluation der Schweiz durch die Europäische Kommission. Die Beibehaltung des Angemessenheitsbeschlusses der EU ist für den Wirtschaftsstandort und die Wettbewerbsfähigkeit der Schweiz zentral. Denn nur, wenn die Schweiz von der EU weiterhin als Drittstaat mit angemessenem Datenschutz anerkannt wird, können Personendaten ohne zusätzliche Hindernisse aus den EU-Mitgliedstaaten in die Schweiz bekannt gegeben werden. Ohne den Angemessenheitsbeschluss der EU (und ohne den freien Datenverkehr) wären beträchtliche Wettbewerbsnachteile für die Schweiz zu erwarten. Auch die Anpassung des schweizerischen Datenschutzrechts an das revidierte Übereinkommen SEV 108 des Europarates hat für den internationalen Marktzugang eine wichtige Bedeutung. Das Interesse aussereuropäischer Staaten an einem Beitritt zum revidierten Übereinkommen SEV 108 nimmt zu, was den Datenaustausch mit diesen Ländern inskünftig ebenfalls erleichtern könnte.

Schliesslich fördert der sichere Umgang mit Personendaten das Vertrauen in digitale Technologien und ihre Anbieter. Mit einem verbesserten Datenschutz lässt sich also auch die Digitalisierung stärken.

4 Anpassungen aufgrund der Vernehmlassung

Die Verordnung enthält im Vergleich zum Vernehmlassungsentwurf inhaltliche und systematische Anpassungen. Die wichtigsten Änderungen werden im Folgenden dargestellt.

4.1 Datensicherheit

Der Abschnitt zur Datensicherheit wurde überarbeitet, um der in der Vernehmlassung geäusserten Kritik Rechnung zu tragen.

Auslegungsbedürftige Begriffe (z. B. «angemessene Abstände») wurden gestrichen. Ausserdem werden die Ziele neu in einem eigenen Artikel (Art. 2 DSV) geregelt, der sich an der Regelung im Informationssicherheitsgesetz[11] orientiert. Artikel 3 regelt die technischen und organisatorischen Massnahmen.

Die Bestimmungen zur Protokollierung und zum Bearbeitungsreglement (Art. 4–6 DSV) erhalten so weit wie möglich die Regelung der geltenden VDSG aufrecht. So wird der Verweis auf die Datenschutz-Folgenabschätzung aus den Voraussetzungen für die Protokollierungspflicht gestrichen. Der Vorschlag, die Dauer für die Aufbewahrung der Protokolle auf zwei Jahre zu erhöhen, wird nicht aufrechterhalten. Da die Dauer von einem Jahr gemäss der geltenden VDSG sowohl ein Minimum als auch ein Maximum darstellt, wurde der Ausdruck «mindestens» eingefügt, damit die privaten Personen die Protokolle auch während mehr als einem Jahr aufbewahren können. Bei den Bundesorganen bleiben die spezialgesetzlichen Vorschriften vorbehalten.

4.2 Bearbeitung durch Auftragsbearbeiter

Der bisherige Inhalt von Artikel 6 E-VDSG wurde gestrichen. Stattdessen wird in Artikel 7 DSV einzig die Art der vorgängigen Genehmigung, mit welcher ein Verantwortlicher einen

[11] ISG, BBl **2017** 3097.

Auftragsbearbeiter zur Übertragung der Datenbearbeitung auf einen Dritten ermächtigen kann, geregelt. Diese Bestimmung orientiert sich an Artikel 22 Absatz 2 der Richtlinie (EU) 2016/680 bzw. Artikel 28 Abs. 2 DSGVO. Sie nimmt aus Gründen der Rechtssicherheit auf, was der Bundesrat bereits in der Botschaft zur Totalrevision des Datenschutzgesetzes zur Genehmigung der Subauftragsbearbeitung ausgeführt hat (vgl. BBl *2017* 6941, 7032).

Die Streichung von Artikel 6 Absätze 1 und 2 E-VDSG erfolgt, weil diese Normen bereits durch Art. 9 Abs. 1 Bst. a nDSG sowie die Bestimmungen zur Datenbekanntgabe ins Ausland (Art. 16 f. nDSG; Art. 8 ff. DSV) abgedeckt sind. Auch ein Verantwortlicher, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich.

Eine ausdrückliche Regelung der Schriftform der vorgängigen Genehmigung der Subauftragsbearbeitung durch Bundesorgane, wie sie Artikel 6 Absatz 3 E-VDSG vorgesehen hat, scheint ausserdem nicht erforderlich. Es ist davon auszugehen, dass diese bereits mit Blick auf die Rechtssicherheit zu wählen ist. Ausserdem sind auch die gegebenenfalls einschlägigen beschaffungsrechtlichen Formvorgaben zu beachten.

Artikel 7 E-VDSG wurde ganz gestrichen. Dies ist damit zu begründen, dass bereits Artikel 26 Absatz 2 Buchstabe a DSV (ehem. Art. 28 Abs. 2 Bst. a und b E-VDSG) die Mitwirkung der Datenschutzberaterin bzw. des Datenschutzberaters regelt.

4.3 Bekanntgabe von Personendaten ins Ausland

Die Vernehmlassung hat gezeigt, dass ein Bedarf an erhöhter Transparenz und Klarheit besteht.

Gemäss Artikel 8 Absatz 5 DSV müssen die Beurteilungen des Bundesrates nunmehr veröffentlicht werden. Eine Übergangsbestimmung regelt die Modalitäten (Art. 46 Abs. 2 DSV). Darüber hinaus wurde der Grundsatz der Transparenz ausdrücklich in Artikel 9 Absatz 1 Buchstabe a DSV aufgenommen.

Schliesslich wird auch präzisiert, dass der EDÖB innerhalb von neunzig Tagen zu den Standarddatenschutzklauseln und verbindlichen unternehmensinternen Datenschutzvorschriften, die ihm unterbreitet werden, Stellung nimmt (Art. 10 Abs. 2 und Art. 11 Abs. 3 DSV).

4.4 Pflichten des Verantwortlichen

Aus Artikel 13 Absatz 1 DSV (ehem. Art. 13 Abs. 1 E-VDSG) wurde der Auftragsbearbeiter gestrichen, da sich auch die Rechtsgrundlage in Artikel 19 nDSG nur an den Verantwortlichen richtet. Die Verantwortung für die Auskunft bleibt beim Verantwortlichen. Weiter wurde Absatz 1 im Sinne der DSGVO umformuliert. Zudem wurde Absatz 2 der Bestimmung gestrichen. Die Vernehmlassung hat gezeigt, dass die Verwendung von Piktogrammen in der verlangten Form von der Wirtschaft nicht umgesetzt werden könnte. Insbesondere die Voraussetzung der Maschinenlesbarkeit wurde stark kritisiert.

Artikel 15 E-VDSG wird neu nur noch für Bundesorgane gelten und daher in das Kapitel betreffend die Datenbearbeitungen durch Bundesorgane verschoben (neu Art. 30 DSV). Die Bestimmung wird für Bundesorgane beibehalten, da sie von Art. 7 Abs. 2 der Richtlinie (EU) 2016/680 gefordert wird.

Artikel 16 E-VDSG wurde gestrichen, da dieser Artikel nach der Vernehmlassung zum nDSG entfernt worden war und deshalb nicht im Gesetzesentwurf war, der dem Parlament unterbreitet wurde. In diesem Sinne war es nicht kohärent, ihn im Verordnungsentwurf aufzuführen.

Artikel 17 E-VDSG wurde gestrichen, da Ziel und Zweck der Bestimmung insbesondere durch Artikel 21 Absatz 2 nDSG bereits abgedeckt sind.

Artikel 14 DSV (ehem. Art. 18 E-VDSG) regelt nur noch die Aufbewahrung der Datenschutz-Folgenabschätzung und macht keine Aussage mehr zu deren Form. Wie bei anderen im nDSG und der DSV geregelten Instrumenten liegt es im Ermessen der Verantwortlichen in welcher Form sie diese speichern möchten. Sicherlich muss diese bei einer Prüfung durch den EDÖB oder bei einer Verletzung in einem gängigen Format lesbar sein.

Bei Artikel 15 E-VDSG wurde Absatz 2 an die Vorgabe von Artikel 24 Absatz 1 nDSG angeglichen, so dass auch die Nachmeldung «so rasch als möglich» erfolgen muss. Absatz 4 wurde aufgrund der Änderung in Artikel 26 und 27 DSV, wonach der Miteinbezug der Datenschutzberaterin bzw. des Datenschutzberaters in die Meldung der Verletzung der Datensicherheit neu als Pflicht des Bundesorgans ausgestaltet ist, gestrichen.

4.5 Rechte der betroffenen Person

Im ersten Abschnitt wurde Artikel 20 Absatz 4 E-VDSG (neu Art. 16 Abs. 5 DSV) dahingehend geändert, dass die bereits in Artikel 1 Absatz 2 Buchstaben a und b VDSG vorgesehenen Anforderungen, um die Sicherheit der übermittelten Informationen zu gewährleisten, nur teilweise übernommen werden. Die nach Buchstabe b vorgesehene Pflicht des Verantwortlichen, sicherzustellen, dass die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter geschützt werden, ergibt sich bereits genügend konkret aus Artikel 8 nDSG. Buchstabe b wurde deshalb gestrichen. Es wurde hingegen ausdrücklich beibehalten, dass der Verantwortliche angemessene Massnahmen treffen muss, um die betroffene Person zu identifizieren. Dies insbesondere, da eine Mitwirkungspflicht der betroffenen Person statuiert wird.

Artikel 20 Absatz 5 E-VDSG wurde gestrichen, da die Problematik bereits genügend durch Artikel 26 Absatz 4 nDSG gedeckt ist. Artikel 26 Absatz 4 nDSG sieht bereits vor, dass der Verantwortliche angeben muss, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt. Dies genügt für eine gerichtliche Geltendmachung. Die Verantwortlichen haben somit keine Aufbewahrungspflicht mehr. Eine Aufbewahrung durch den Verantwortlichen bietet sich jedoch aus Beweisgründen an.

Artikel 21 E-VDSG (neu Art. 17 DSV) wurde angepasst, um klar als Koordinationsnorm ersichtlich zu sein. Absatz 2 wurde dergestalt abgeändert, dass der Auftragsbearbeiter den Verantwortlichen bei der Erteilung der Auskunft unterstützt.

Artikel 23 E-VDSG (neu Art. 19 DSV) zu den Ausnahmen von der Kostenlosigkeit wurde ebenfalls überarbeitet. Absatz 3 sieht nun vor, dass das Gesuch als zurückgezogen gilt, wenn die betroffene Person ihr Begehren nach Mitteilung der Kostenbeteiligung nicht innert zehn Tagen bestätigt. Die Frist nach Artikel 18 DSV (ehem. Art. 22 E-VDSG) beginnt dementsprechend erst nach dieser Bedenkzeit zu laufen.

Der 2. Abschnitt zum Recht auf Datenherausgabe oder -übertragung wurde nochmals grundsätzlich überarbeitet. Es wurden folgende Artikel geschaffen: Artikel 20 DSV behandelt den Umfang des Anspruchs, Artikel 21 DSV die technischen Anforderungen an die Umsetzung

und Artikel 22 DSV (ehem. Art. 24 E-VDSG) führt unter Frist, Modalitäten und Zuständigkeit aus, inwiefern die Bestimmungen zum Auskunftsrecht auf das Recht auf Datenherausgabe oder -übertragung anwendbar sind.

4.6 Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Absatz 1 von Artikel 25 E-VDSG (neu Art. 23 DSV) «Datenschutzberaterin oder Datenschutzberater» wurde gestrichen, da die privaten Verantwortlichen nicht verpflichtet sind, Datenschutzberatende zu ernennen. Im verbleibenden Text wurde mit Buchstabe c die Möglichkeit eingeführt, dass die Datenschutzberatenden in wichtigen Fällen das oberste Leitungs- oder Verwaltungsorgan informieren können.

4.7 Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane

In Artikel 26 DSV (ehem. Art. 28 E-VDSG) wird in Absatz 2 klargestellt, dass die Datenschutzbeauftragten bei der Anwendung der Datenschutzvorschriften mitwirken. Wobei die Vorgaben in Ziff. 1 und 2 hier ausschliesslich als Beispiele dafür dienen.

Die Aufgabe der Datenschutzberaterin bzw. des Datenschutzberaters, Meldungen von Verletzungen der Datensicherheit dem EDÖB zu melden (Artikel 28 Absatz 2 Buchstabe c E-VDSG), wird neu als Pflicht des Bundesorgans ausgestaltet. Sie ist daher neu in Artikel 27 DSV geregelt.

Artikel 31 E-VDSG zur Information an die Datenschutzberaterin oder den Datenschutzberater wird gestrichen. Mit der Bestimmung wurde Artikel 20 Absatz 2 VDSG teilweise übernommen. Die Information der Datenschutzberaterin oder des Datenschutzberaters ergibt sich jedoch aus ihren bzw. seinen allgemeinen Beratungs-, Unterstützungs- und Kontrollaufgaben.

5 Erläuterungen zur DSV

5.1 1. Kapitel: Allgemeine Bestimmungen

5.1.1 1. Abschnitt: Datensicherheit

Die Leitplanken zur Gewährleistung der Datensicherheit werden bereits im Gesetz normiert. Gemäss Artikel 8 Absatz 1 nDSG sind der Verantwortliche und der Auftragsbearbeiter verpflichtet, durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten. Gemäss Absatz 2 müssen diese Massnahmen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden. In Absatz 3 wird der Bundesrat dazu beauftragt, die Mindestanforderungen an die Datensicherheit auf Verordnungsstufe zu präzisieren.

Mit den Bestimmungen zur Datensicherheit erfüllt der Bundesrat den gesetzlichen Auftrag gemäss Artikel 8 Absatz 3 nDSG. An diese Mindestanforderungen knüpft zudem die Strafnorm in Artikel 61 Buchstabe c nDSG an. Der Grad an Sicherheit, der eingehalten werden muss, damit die Strafnorm nicht verletzt wird, bestimmt sich dabei nach den Grundsätzen und Kriterien des vorliegenden Abschnittes. Die Strafbarkeit besteht gemäss Artikel 61 Buchstabe c nDSG nur im Fall einer vorsätzlichen Begehung. Dies setzt voraus, dass der Verantwortliche die Mindestanforderungen an die Datensicherheit wissentlich und willentlich nicht einhält. So würde sich beispielsweise derjenige strafbar machen, der es unterlässt, eine Anti-Viren-Software zu installieren, obwohl er weiss (oder zumindest in Kauf nimmt), dass er damit ungenügende Massnahmen zur Einhaltung der Mindestanforderungen an die Datensicherheit trifft.

Da bereits im Gesetz der Ansatz einer risikobasierten Datensicherheit verfolgt wird und sich keine allgemeingültigen Mindestanforderungen für jegliche Branchen festlegen lassen,

wurde in der DSV auf ein starres Regime von Mindestanforderungen verzichtet. Der Ansatz der DSV beruht vielmehr darauf, dass es in erster Linie in der Verantwortung des Verantwortlichen liegt, die im Einzelfall notwendigen Massnahmen zu bestimmen und zu ergreifen. Diese sind stark einzelfallbezogen und abhängig vom jeweiligen Risiko zu bestimmen. So stellen sich etwa in einem Spital, wo regelmässig besonders schützenswerte Personendaten bearbeitet werden, in aller Regel erhöhte Anforderungen im Vergleich zur Bearbeitung von Kunden- oder Lieferantendaten in einer Bäckerei oder Metzgerei. Die DSV beinhaltet daher insbesondere die Leitlinien für die Bestimmung der zu ergreifenden Massnahmen (Art. 1, 2 und 3 DSV). Dadurch kann die angesichts der Vielfalt möglicher Fallkonstellationen notwendige Flexibilität gewährleistet werden und eine Überregulierung, insbesondere für Betriebe mit geringfügiger und wenig risikoreicher Datenbearbeitung, verhindert werden.

Anders als die DSGVO kennt das Schweizer Recht keine allgemeine Rechenschaftspflicht («accountability»). Allerdings enthält das Schweizer Recht bereits im geltenden Recht Massnahmen, mit denen die Rechenschaftspflicht oder Pflicht zur «accountability» erfüllt werden kann: die Protokollierung (Art. 4) und das Bearbeitungsreglement (Art. 5, 6). Beide Massnahmen werden in der DSV übernommen. Sie sind ausschlaggebend dafür, dass das Schweizer Recht ein im Vergleich zum EU-Recht angemessenes Schutzniveau gewährleisten kann. Darüber hinaus verlangt die Richtlinie (EU) 2016/680 die Protokollierung. Beide Massnahmen stellen Mindestanforderungen an die Datensicherheit im Sinne von Artikel 8 Absatz 3 nDSG dar. Der Bundesrat verfolgt auch hier einen risikobasierten Ansatz: Je höher die Gefährdung für die Persönlichkeitsrechte und die Grundrechte des Einzelnen, desto höher die Anforderungen.

Die Mindestanforderungen der Datensicherheit sind gemäss geltendem Recht in Artikel 8–12 und Artikel 20–21 VDSG geregelt. Der Bundesrat hat entschieden, am geltenden Standard der Datensicherheit anzuknüpfen. Die materiell-rechtlichen Vorgaben werden daher im Grundsatz so übernommen. Anpassungen werden nur vorgenommen, wo dies aufgrund der Digitalisierung bzw. des technischen Fortschritts, der Vorgaben im revidierten Gesetz oder der für die Schweiz massgeblichen Richtlinie (EU) 2016/680, namentlich deren Artikel 25 und 29, angezeigt scheint. Zudem hat sich der Bundesrat auch an der Verordnung (EU) 2016/679 orientiert, damit Schweizer Unternehmen, die in der EU tätig sind und eine gemäss der DSGVO konforme Datensicherheit gewährleisten, auch in der Schweiz davon ausgehen können, dass sie die Mindestanforderungen erfüllen.

In systematischer Hinsicht wird die Datensicherheit neu in einem eigens dafür vorgesehenen Abschnitt normiert. In der aktuellen VDSG wird die Datensicherheit für Private und Bundesorgane getrennt geregelt, aus Gründen der Übersichtlichkeit und der besseren Lesbarkeit werden die Bestimmungen neu zusammengeführt. Wo unterschiedliche Vorgaben für Private und Bundesorgane gelten, werden diese in getrennten Artikeln oder Absätzen geregelt.

Art. 1 Grundsätze

Artikel 1 DSV regelt die Grundsätze, die bei der Bestimmung der Massnahmen zu beachten sind. Er übernimmt im Wesentlichen das Regelungskonzept von Artikel 8 Absätze 2 und 3 VDSG, wobei bestimmte Aspekte präziser geregelt werden. Artikel 8 Absatz 1 VDSG wurde hingegen gestrichen, da die Ziele zur Gewährleistung der Datensicherheit neu auf Gesetzesebene angesiedelt sind. Artikel 8 Absatz 2 nDSG legt namentlich fest, dass die Massnahmen der Datensicherheit es ermöglichen müssen, Verletzungen der Datensicherheit zu vermeiden. Eine Verletzung der Datensicherheit liegt gemäss Artikel 5 Buchstabe h nDSG vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Daraus

lassen sich die herkömmlichen IT-Schutzziele der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit ableiten.

Gemäss Artikel 8 Absatz 1 nDSG müssen der Verantwortliche und der Auftragsbearbeiter eine dem Risiko angemessene Datensicherheit gewährleisten. In Artikel 1 DSV wird dieses Schutzziel in einem neuen Absatz 1 aufgenommen. Ausserdem werden verschiedene Kriterien zur Beurteilung des Schutzbedarfs (Abs. 2) sowie zur Beurteilung des Risikos für die Persönlichkeit oder die Grundrechte der betroffenen Person (Abs. 3) festgelegt. In Absatz 4 wird präzisiert, dass bei der Festlegung der technischen und organisatorischen Massnahmen, die zur Gewährleistung einer angemessenen Datensicherheit erforderlich sind, weitere Kriterien berücksichtigt werden können (Abs. 4). Die Liste der Kriterien lehnt sich an das geltende Recht an.

Artikel 1 Absatz 2 DSV übernimmt Artikel 8 Absatz 2 Buchstaben a und b VDSG in inhaltlicher Hinsicht und ergänzt diesen, um die Schutzbedarfsanalyse zu regeln. Der Schutzbedarf wird auf der Grundlage der Art der bearbeiteten Daten sowie des Zwecks, der Art, des Umfangs und der Umstände der Datenbearbeitung beurteilt. Dabei geht es insbesondere um das Schutzniveau, das angesichts des Risikos für die Persönlichkeits- und Grundrechte der betroffenen Personen gewährleistet werden muss. Je höher der Schutzbedarf, desto strenger sind die Anforderungen an die Massnahmen. Bei der Beurteilung des Schutzbedarfs sollten die folgenden Kriterien berücksichtigt werden:

- Die Art der bearbeiteten Daten (Bst. a): Es ist beispielsweise entscheidend, ob besonders schützenswerte Personendaten (Art. 5 Bst. c nDSG) bearbeitet werden.
- Zweck, Art, Umfang und Umstände der Datenbearbeitung (Bst. b): Der Zweck bezieht sich auf den Zweck der Bearbeitung und insbesondere auf die Prüfung, ob der Bearbeitungszweck ein erhöhtes Risiko für die Persönlichkeitsrechte und die Grundrechte mit sich bringt; bei der Art der Bearbeitung ist von Interesse, wie die Daten bearbeitet werden. Der Schutzbedarf kann beispielsweise bei einer vollständig automatisierten Entscheidung (Einsatz künstlicher Intelligenz) höher sein; der Umfang der Bearbeitung steht insbesondere im Zusammenhang mit der Anzahl der von der Bearbeitung betroffenen Personen (z. B. wenn umfangreich Daten bearbeitet werden oder systematisch umfangreiche öffentliche Bereiche überwacht werden). Bei der Nutzung einer Cloud kann der Schutzbedarf höher sein als wenn Daten auf einem internen Server ohne externe Zugriffsmöglichkeit gespeichert sind. Buchstabe b wurde entsprechend Artikel 22 Absatz 2 nDSG mit dem Ausdruck der «Umstände» der Datenbearbeitung ergänzt. Dabei handelt es sich um Aspekte, die im Einzelfall von besonderer Bedeutung sein können, weil sie Auswirkungen auf die anderen Kriterien haben. So können Kriterien einbezogen werden, die nicht in die Definition der bereits erwähnten Kriterien passen würden.

In Artikel 1 Absatz 3 DSV wird Artikel 8 Absatz 2 Buchstabe c VDSG aufgenommen und präzisiert. Mit der Bestimmung wird die Beurteilung des Risikos einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person eingeführt. Wie im vorherigen Absatz wird eine Reihe von Kriterien festgelegt. Der Absatz wird umformuliert, damit deutlich wird, dass die Ursachen des Risikos (Bst. a), die hauptsächlichen Gefahren (Bst. b), die zur Verringerung des Risikos ergriffenen oder vorgesehenen Massnahmen (Bst. c) sowie die Wahrscheinlichkeit und Schwere einer Verletzung der Datensicherheit (Bst. d) entscheidend sind. Dabei handelt es sich um eine Beurteilung gemäss einem Kaskadensystem: Das Ergebnis der Beurteilung nach einem Kriterium ist massgebend für die weitere Risikobeurteilung. Zu den einzelnen Punkten finden sich hier nähere Ausführungen:

- Die Ursachen des Risikos (Bst. a): Es muss festgestellt werden können, welche Personen (z. B. eine IT-Verantwortliche, ein Nutzer, eine Konkurrentin) oder Ereignisse (z. B. Feuer, Computervirus) dem Risiko zugrunde liegen könnten.
- Die hauptsächlichen Gefahren (Bst. b): Anhand dieses Kriteriums können Bedrohungen eruiert werden, die zu Verletzungen der Datensicherheit führen könnten (verlorene, beschädigte, veränderte, unsachgemäss oder betrügerisch verwendete Daten usw.).
- Die getroffenen oder ergriffenen Massnahmen, um das Risiko zu verringern (Bst. c): Die verschiedenen technischen und organisatorischen Massnahmen, die zur Verringerung des Risikos vorgesehen oder ergriffen werden können, werden in Artikel 3 DSV präzisiert.
- Die Wahrscheinlichkeit und Schwere einer Verletzung der Datensicherheit trotz der ergriffenen oder vorgesehenen Massnahmen (Bst. d): Die potenziellen Auswirkungen auf die betroffenen Personen müssen ermittelt werden, wenn beispielsweise Personen unrechtmässig auf Daten zugreifen (und sie weitergeben), sie ändern (was zu falschen Informationen über die betroffene Person führt) oder löschen (wodurch sie Gefahr laufen, notwendige Daten zu verlieren; hier ist z. B. an ein Patientendossier zu denken, in dem einige Daten vernichtet wurden, wodurch eine angemessene medizinische Behandlung verhindert wird). Dabei gilt: Je wahrscheinlicher der Eintritt einer Verletzung der Datensicherheit und je grösser die Auswirkungen für die betroffenen Personen, desto höher die Anforderungen an die Massnahmen. An dieser Stelle sei darauf hingewiesen, dass nicht jede Verletzung der Datensicherheit im Sinne von Artikel 5 Buchstabe h nDSG auch eine Verletzung der Mindestanforderungen im Sinne von Artikel 8 Absatz 3 nDSG und somit eine Verletzung der Sorgfaltspflichten gemäss Artikel 61 Buchstabe c nDSG darstellt. Eine absolute Sicherheit kann und soll nicht verlangt werden. So ist insbesondere vorstellbar, dass der Verantwortliche alle angemessenen Massnahmen getroffen hat, eine Verletzung der Datensicherheit aber dennoch eintritt, namentlich, weil sich das Restrisiko realisiert hat. Dieses kann dem Verantwortlichen nicht angelastet werden. Es ist im Rahmen der Mindestanforderungen vielmehr zu prüfen, ob der Verantwortliche und der Auftragsbearbeiter angesichts der konkreten Sachlage die angemessenen Massnahmen zur Gewährleitung der Datensicherheit getroffen haben, und zwar unabhängig davon, ob eine Verletzung der Datensicherheit eintritt.

In Anlehnung an Artikel 8 Absatz 2 Buchstabe d VDSG werden in Artikel 1 Absatz 4 DSV noch weitere Kriterien eingeführt, die bei der Festlegung der technischen und organisatorischen Massnahmen zur Gewährleistung der angemessenen Datensicherheit berücksichtigt werden können. Der Ausdruck «Festlegung» umfasst die «Beurteilung» und den «Entscheids» (in der französischen Fassung wird der Begriff «détermination» verwendet). Die Kriterien lauten wie folgt: der Stand der Technik (Bst. a) und die Implementierungskosten (Bst. b). Diese Kriterien geben nur indirekt Aufschluss darüber, ob Massnahmen ergriffen werden müssen und ob die zu ergreifenden Massnahmen angemessen sind.

- Stand der Technik (Bst. a): Die Massnahmen sind unter Berücksichtigung des Stands der Technik (technischer und wissenschaftlicher Kenntnisstand) zu bestimmen und ggf. anzupassen. Der Stand der Technik meint die Berücksichtigung des gegenwärtigen Standes. Es ist also ausreichend, Massnahmen zu treffen, die bereits zur Verfügung stehen und sich entsprechend bewährt haben. Hingegen kann nicht verlangt werden, dass brandneue unerforschte Techniken oder solche die sich noch im Entwicklungsprozess befinden, eingesetzt werden.
- Implementierungskosten (Bst. b): Der Begriff «Kosten» ist im weiten Sinn zu verstehen. Er ist nicht auf die finanziellen Kosten beschränkt, sondern umfasst auch die erforderlichen personellen und zeitlichen Ressourcen. Diese Terminologie entspricht der des europäischen Rechts (Richtlinie [EU] 2016/680 und DSGVO). Die Implementierungskosten sind – wie aus dem «Kommentar des Bundesamts für Justiz zur Vollzugsverordnung vom 14. Juni 1993 (Stand am 1. Januar 2008) zum Bundesgesetz über den Datenschutz (VDSG, SR

235.11)» (Ziff. 6.1.1)[12] hervorgeht – auch gemäss geltendem Recht ein Kriterium bei Beurteilung der Angemessenheit der Massnahmen. In erster Linie ist allerdings darauf abzustellen, welche technischen und organisatorischen Massnahmen angesichts der Kriterien in Buchstaben a–c erforderlich sind. Verantwortliche und Auftragsbearbeiter können sich insbesondere nicht mit der Begründung von der Pflicht einer angemessenen Datensicherheit befreien, dass damit übermässige Kosten verbunden sind; vielmehr müssen sie jedenfalls in der Lage sein, eine angemessene Datensicherheit zu gewährleisten. Es kann auch nicht argumentiert werden, dass sich bei fehlendem Konzept bei der Entwicklung die Implementierungskosten zur Umsetzung der Datensicherheit nach Inbetriebnahme als zu hoch erweisen. Bei Legacy Applikationen (Altanwendungen) muss vielmehr die geplante Zeit bis hin zur Ablösung einbezogen werden (Lifecycle). Das Kriterium der Kosten kann jedoch bedeuten, dass bei mehreren zur Verfügung stehenden Massnahmen zur Gewährleistung eines stets angemessenen Datenschutzniveaus die kostengünstigere Variante bevorzugt werden darf.[13]

Zur Gewährleistung der Datensicherheit kommen unterschiedliche Massnahmen in Betracht. Vorliegend seien beispielshaft drei Massnahmen erwähnt:

- die Anonymisierung, Pseudonymisierung und Verschlüsselung von Personendaten: Die Anonymisierung trägt insbesondere dazu bei, dass allfällig negative Auswirkungen für die betroffenen Personen reduziert werden, die sich beispielsweise durch eine unbefugte Offenlegung von Personendaten ergeben können. Liegt eine Anonymisierung vor, so kommt das DSG gemäss dessen Anwendungsbereich gar nicht zur Anwendung.
- Verfahren zur Identifikation, Bewertung und Evaluierung der Risiken und Überprüfung der Angemessenheit der getroffenen Massnahmen: Ab einem gewissen Risiko wird es in vielen Fällen sinnvoll beziehungsweise sogar notwendig sein, dass standardisierte Verfahren und Prozesse implementiert werden, welche die Risiken und die Angemessenheit der getroffenen Massnahmen nicht nur regelmässig überprüfen, sondern auch bewerten und evaluieren. Solche Massnahmen sind insbesondere bei automatisierten Systemen bedeutsam. Sie tragen dazu bei, dass die Datensicherheit dauerhaft gewährleistet wird und auch ihr Nachweis einfacher erbracht werden kann.
- die Schulung und Beratung der mit der Umsetzung betrauten Personen: Diese Massnahme ist aus Sicht des Bundesrats bedeutsam, da die Umsetzung und Wirksamkeit der Datensicherheit auch insbesondere davon abhängt, ob die involvierten Personen die festgelegten Massnahmen anwenden. So kann eine fehlende Schulung und Beratung zu einer Datensicherheitsverletzung führen. Beispielsweise sollten die Mitarbeiter und Mitarbeiterinnen über das Risiko, Malware zu öffnen, aufgeklärt werden.

Letztlich bleiben bei der Bestimmung der Massnahmen selbstredend die Umstände des Einzelfalls massgeblich.

Die Massnahmen sind gemäss Artikel 1 Absatz 5 wie gemäss geltendem Recht laufend zu überprüfen und ggf. anzupassen. Insbesondere ist zu überprüfen, ob die Massnahmen noch immer dem Risiko angemessen und wirksam sind. Statt «periodisch» muss die Überprüfung neu «über die gesamte Bearbeitungsdauer hinweg» erfolgen. Der Überprüfungsbedarf hängt insbesondere von der Gefährdungslage für die Persönlichkeitsrechte und Grundrechte Betroffener ab: Je höher er ist, desto häufiger müssen die Massnahmen regelmässig überprüft werden. Die neue Formulierung geht in Richtung einer ständigen Überprüfung. Sie lässt

---

[12] Abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/der-edoeb/rechtliche-grundlagen.html.

[13] Siehe auch BRUNO BAERISWYL, in: Stämpflis Handkommentar, Datenschutzgesetz, 1. Auflage 2015, Nr. 26 zu Art. 7.

dem Verantwortlichen und dem Auftragsbearbeiter jedoch einen grossen Ermessensspielraum. Eine Überprüfung kann sich zusätzlich aufdrängen, wenn eine Verletzung der Datensicherheit erfolgt oder die Bearbeitung von Personendaten angepasst worden ist. Artikel 1 Absatz 5 stellt darüber hinaus klar, dass nicht nur die technischen und organisatorischen Massnahmen während der gesamten Dauer der Bearbeitung, also während des gesamten «Lifecycles» der Personendaten, überprüft werden müssen, sondern auch der Schutzbedarf und die Risiken. Durch die Überprüfung des Schutzbedarfs und der Risiken wird (indirekt) auch überprüft, ob die technischen und organisatorischen Massnahmen geeignet sind.

Art. 2 Ziele

Artikel 2 DSV ergänzt Artikel 1 nDSG in Bezug auf den Zweck des Gesetzes und konkretisiert die Ziele zur Gewährleistung der angemessenen Datensicherheit, die nunmehr in Artikel 8 Absatz 2 nDSG festgelegt sind. Nach dieser Bestimmung müssen es die Massnahmen ermöglichen, eine Verletzung der Datensicherheit zu vermeiden. Absolute Sicherheit ist ein unerreichbares Ideal. Mit dem risikobasierten Ansatz sollen die Risiken identifiziert werden (Art. 1 DSV), damit die Massnahmen auf die Ziele abgestimmt und entsprechend ausgewählt werden. Der Verantwortliche und der Auftragsbearbeiter müssen die Ziele und den Umfang des Schutzes bestimmen.

In der Lehre und Praxis werden in der Regel vier Schutzziele festgehalten, die im Französischen unter dem Akronym (C.A.I.D.) bekannt sind: die Vertraulichkeit (*confidentialité*), die Authentizität (*authentification*), die Integrität (*intégrité*) und die Verfügbarkeit (*disponibilité*) der Daten. In Anlehnung an Artikel 32 DSGVO und mit Blick auf eine Harmonisierung mit dem Bundesgesetz über die Informationssicherheit beim Bund[14], das demnächst in Kraft treten soll, soll Artikel 2 die Vertraulichkeit (Bst. a), die Verfügbarkeit (Bst. b), die Integrität (Bst. c) und die Nachvollziehbarkeit (Bst. d) regeln.

- Die Vertraulichkeit (Bst. a): Die Personendaten dürfen nur Berechtigten zugänglich sein. Der Kreis der berechtigten Personen wird durch den Kontext des Aufgabenbereichs sowie den Inhalt und die Wichtigkeit der Daten bestimmt. Er kann sehr weit oder äusserst eng sein. Unter Vertraulichkeit sind auch die Authentifizierung, die damit verbundenen Methoden sowie die Systeme zur Verwaltung und Einschränkung des Zugriffs zur Gewährleistung der Datensicherheit zu verstehen. Schliesslich sollte die Vertraulichkeit des Systems und der Daten gewährleistet sein.
- Die Verfügbarkeit (Bst. b): Gemäss diesem Zweck sorgt der Verantwortliche dafür, dass die Daten jederzeit eingesehen werden können. Diese Anforderung ist umso höher, wenn die Informationen für die Erfüllung wesentlicher oder sogar gesetzlicher Aufgaben ständig verfügbar sein müssen.
- Die Integrität (Bst. c): Dieses Ziel gewährleistet die Richtigkeit der Daten. Es ist insbesondere dann von Bedeutung, wenn die Daten für die Öffentlichkeit bestimmt sind oder weiterverwendet werden sollen. Unter Integrität sind die Authentizität, die Zurechenbarkeit und die Nichtabstreitbarkeit der Daten zu verstehen. Diese Begriffe werden in der Praxis oder in der Lehre auch anstelle von Integrität verwendet.
- Die Nachvollziehbarkeit (Bst. d): Auf Grundlage dieses Ziels können unbefugte Zugriffe oder sogar Missbräuche identifiziert werden. Darüber hinaus kann die Ursache eines Vorfalls ermittelt werden. Der Verantwortliche sorgt für die Aufzeichnung der Ereignisse und der Datenspuren und stellt sicher, dass diese nicht verändert werden können. Die Nachvollziehbarkeit der Bearbeitung kann für das Verfahren (Beweismittel) von Bedeutung sein und

[14] Botschaft des Bundesrates vom 22. Februar 2017 zum Informationssicherheitsgesetz (ISG), BBl **2017** 2953. Für den Text, den das Parlament in der Schlussabstimmung angenommen hat, vgl. BBl **2020** 9975.

erleichtert die Kontrollen und Überwachung. Von Zurechenbarkeit und Nichtabstreitbarkeit von Daten ist in der Praxis auch im Zusammenhang mit Mechanismen der Nachvollziehbarkeit die Rede.

Gestützt auf diese Ziele sollen Verfahren entwickelt werden, um die Wirksamkeit der ergriffenen Massnahmen regelmässig zu kontrollieren, zu analysieren und zu beurteilen (Art. 1 Abs. 5 und Art. 3 DSV).

Art. 3 Technische und organisatorische Massnahmen

Artikel 8 Absatz 1 nDSG verlangt, dass eine angemessene Sicherheit der Personendaten gewährleistet wird. Unter Berücksichtigung der Vernehmlassungsergebnisse sieht Artikel 3 vor, dass organisatorische und technische Massnahmen ergriffen werden müssen, um die Ziele von Artikel 2 zu erreichen. In Anwendung der Verhältnismässigkeit sind ausgehend davon die organisatorischen und technischen Massnahmen des Einzelfalls zu bestimmen. Die Verantwortlichen und Auftragsbearbeiter haben deshalb zu prüfen, mit welchen geeigneten Massnahmen sie die Schutzziele erreichen. Es ist durchaus vorstellbar, dass nicht jedes Schutzziel in jedem Fall von Relevanz ist. Ist ein Schutzziel in einem Fall nicht von Relevanz, so müssen der Verantwortliche und Auftragsbearbeiter aber in der Lage sein, zu begründen, weshalb dies der Fall ist. Die «Eignung» der Massnahmen hängt von den Umständen ab. Der Artikel zeigt dem Verantwortlichen und dem Auftragsbearbeiter in didaktischer Weise eine Reihe von Massnahmen auf, mit denen er die Ziele nach Artikel 2 erreichen kann. Eine Massnahme kann im Übrigen zur Erreichung verschiedener Ziele beitragen.

Der Artikel stellt grösstenteils eine Übernahme des Artikels 9 VDSG dar: Die Regelung steht neu unter dem Titel «Technische und organisatorische Massnahmen». Mit Artikel 3 DSV setzt die Schweiz auch die Anforderungen von Artikel 29 der Richtlinie (EU) 2016/680 um.

Nach Artikel 1 Absatz 3 Buchstabe c DSV ist der Verantwortliche verpflichtet, technische und organisatorische Massnahmen ergreifen, um das Risiko zu verringern. Im Verordnungstext wird bei mehreren technischen und organisatorischen Massnahmen auf «berechtigte» Personen Bezug genommen. Dies setzt nicht zwingend ein direktes Tätigwerden einer Person voraus. Denn darunter können auch Fälle subsumiert werden, bei denen Personendaten in Applikationen oder in einem automatisierten Informationssystem bearbeitet werden.

Artikel 3 Absatz 1 DSV konkretisiert Artikel 2 Absatz 1 Buchstabe a DSV und nennt Massnahmen für die Vertraulichkeit; d. h. Massnahmen, die Zugriffskontrolle (Bst. a), die Zugangskontrolle (Bst. b) sowie die Benutzerkontrolle (Bst. c) gewährleisten sollen.

- An erster Stelle normiert Buchstabe a neu die Zugriffskontrolle. Das Schutzziel wurde aus Artikel 9 Absatz 1 Buchstabe g VDSG übernommen. Es geht hauptsächlich darum, die Zugriffsberechtigungen zu bestimmen, die die Art und den Umfang des Zugriffs regeln. Dabei ist darauf zu achten, dass die berechtigten Personen nur Zugang zu den Personendaten haben, für die sie berechtigt sind. Die zu ergreifenden Massnahmen sind organisatorischer und technischer Art.
- Buchstabe b normiert die in Artikel 9 Absatz 1 Buchstabe a VDSG verankerte Zugangskontrolle. Demnach muss unbefugten Personen der Zugang zu den Räumlichkeiten und Anlagen, in denen Personendaten bearbeitet werden, verwehrt werden. Neu enthält das Schutzziel auch den Begriff «Anlagen». Dadurch soll insbesondere zum Ausdruck kommen, dass auch der Zugang zu mobilen Bearbeitungsanlagen zu unterbinden ist. Der Begriff ist sehr weit gefasst und umfasst von fest angelegten Serveranlagen über Computer bis hin zu Mobiltelefonen oder Tablets jegliche Geräte zur Bearbeitung von Personendaten. Aufgrund

des technischen Fortschritts kann sich «Anlage» sowohl auf Anlagen physischer als auch auf virtueller Natur beziehen. Mögliche Massnahmen sind beispielsweise Alarmanlagen und abschliessbare Serverschränke.
- Buchstabe c enthält die in Artikel 9 Absatz 1 Buchstabe f VDSG geregelte Benutzerkontrolle. Diese ist darauf ausgerichtet, dass die Benutzung von automatisierten Datenbearbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen verhindert wird. Die Massnahmen sorgen dafür, dass die Daten nicht unbefugt benutzt oder weitergegeben werden können. Mögliche Massnahmen sind beispielsweise die regelmässige Kontrolle von Berechtigungen (z. B. Sperrung von Berechtigungen aufgrund von Personalwechsel oder neuen Aufgabenzuteilungen) und der Einsatz von Software gegen Viren oder Spyware oder auch die Sensibilisierung des Personals für Phishing-Methoden.

In Bezug auf Verfügbarkeit und Integrität übernimmt die Artikel 3 Absatz 2 DSV die Ziele von Artikel 2 Absatz 1 Buchstaben b und c DSV. Die diesbezüglichen Massnahmen sollen die Kontrolle der Datenträger (Bst. a), des Speichers (Bst. b), des Transports (Bst. c) sowie der Wiederherstellung (Bst. d) gewährleisten. Die Massnahmen müssen geeignet sein, die Verfügbarkeit, die Zuverlässigkeit und die Integrität zu gewährleisten (Bst. e). Schliesslich muss die Sicherheit des Systems auf dem neuesten Stand gehalten werden (Bst. f).

- Buchstabe a regelt die Datenträgerkontrolle, die derzeit in Artikel 9 Absatz 1 Buchstabe b VDSG normiert ist. Diese beinhaltet, dass unbefugten Personen das Lesen, Kopieren, Verändern, Verschieben, Löschen oder Vernichten von Datenträgern verunmöglicht wird. Es ist insbesondere zu verhindern, dass Personendaten unkontrolliert auf Datenträger (z. B. Festplatten, USB-Sticks) übertragen werden können. Unter Datenträger sind dabei nicht nur physische Träger zu verstehen, sondern auch beispielsweise Cloud-Dienste. Mögliche Massnahmen sind beispielsweise die Verschlüsselung und das ordnungsgemässe Vernichten von Datenträgern. Der Buchstabe entspricht der Vorgabe von Artikel 29 Absatz 2 Buchstabe b der Richtlinie (EU) 2016/680.
- Buchstabe b entspricht Artikel 9 Absatz 1 Buchstabe e VDSG und normiert die Speicherkontrolle. Gemäss der Massnahme dürfen unbefugte Personen Personendaten im Speicher nicht speichern, einsehen, ändern, löschen oder vernichten. Es ist zu verunmöglichen, dass unbefugte Personen auf den Inhalt des Datenspeichers Zugriff haben, diesen einsehen, verändern oder löschen können. Mögliche Massnahmen sind beispielsweise die Festlegung von differenzierten Zugriffsberechtigungen für Daten, Anwendungen und Betriebssysteme und die Protokollierung von Zugriffen auf Anwendungen. Der Buchstabe entspricht der Vorgabe von Artikel 29 Absatz 2 Buchstabe c der Richtlinie (EU) 2016/680.
- Buchstabe c normiert die Transportkontrolle, die derzeit in Artikel 9 Absatz 1 Buchstabe c VDSG geregelt ist. Demnach muss bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern verhindert werden, dass die Daten unbefugt gelesen, kopiert, verändert, gelöscht oder vernichtet werden können. Der Verantwortliche und der Auftragsbearbeiter müssen dafür sorgen, dass der designierte Empfänger bzw. die designierte Empfängerin die Daten in ihrer ursprünglichen Form erhalten und keine Dritte die Daten unbefugt abfangen können. Insbesondere bei besonders schützenswerten Personendaten stellen sich erhöhte Anforderungen an die Massnahmen. In Betracht kommt etwa die Verschlüsselung von Daten bzw. von Datenträgern.
- Bei Buchstabe d geht es um die Möglichkeit der Wiederherstellung der Verfügbarkeit der Personendaten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall. Er wurde in Anlehnung an Artikel 32 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 neu in den Katalog aufgenommen und entspricht der Vorgabe in Artikel 29 Absatz 2 Buchstabe i der Richtlinie (EU) 2016/680. Eine mögliche Massnahme ist das Ausarbeiten und Anwenden eines Backup-Konzepts.

- Buchstabe e bestimmt, dass alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität). Er wurde in Anlehnung an Artikel 32 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 neu in den Katalog aufgenommen und entspricht der Vorgabe in Artikel 29 Absatz 2 Buchstabe j der Richtlinie (EU) 2016/680. Hier geht es insbesondere darum, dass die Stabilität bzw. die Belastbarkeit der eingesetzten Systeme dauerhaft gewährleistet wird. Die Meldung der Fehlfunktionen soll vom System selbst getätigt werden, sodass der Verantwortliche oder der Auftragsbearbeiter automatisch darauf aufmerksam gemacht wird, dass eine Fehlfunktion vorliegt. Wenn eine Fehlfunktion gemeldet wird, bedeutet das nicht automatisch, dass die Funktionen zuverlässig sind; vielmehr muss die Fehlfunktion dafür auch korrigiert werden.
- Bei Buchstabe f geht es um die Gewährleistung der Sicherheit von Betriebssystemen und Anwendungssoftware, die bei der Bearbeitung von Personendaten zur Anwendung gelangen. Da die Bearbeitung von Personendaten auf Systemen und diversen darauf laufenden Anwendungen basiert, ist es notwendig, dass diese auf dem aktuellsten Sicherheitsstand gehalten und kritische Lücken zeitnah geschlossen werden. Buchstabe f ergänzt damit die Vorgaben in Buchstabe d und e, mit dem Ziel, eine ganzheitliche Sicherheit zu gewährleisten. Es wird nicht verlangt, dass jedes System- und Anwendungsupdate sofort installiert wird, sondern dass ein Prozess für die Aktualisierung vorhanden ist (sog. Vulnerability- und Patchmanagement). Die entsprechende Sicherheitsaktualisierung kann zeitlich abgestuft, unter Berücksichtigung der Kritikalitätsstufen (hoch, mittel, tief), umgesetzt werden. Bis zur Behebung von Schwachstellen müssen aber Massnahmen getroffen werden, damit die Datensicherheit dennoch gewährleistet bleibt. Im Unterschied zu Artikel 3 Absatz 3 Buchstabe c geht es bei Buchstabe f nicht um reaktive Massnahmen, sondern die proaktive Behebung von Schwachstellen, für die im System bislang keine Verletzung der Datensicherheit festgestellt wurde.

Absatz 3 nennt die Massnahmen zur Nachvollziehbarkeit (Art. 2 Abs. 1 Bst. d DSV), d. h. Massnahmen, die die Kontrolle der Eingabe (Bst. a) und der Bekanntgabe (Bst. b) gewährleisten sollen, sowie Massnahmen zur Erkennung und Beseitigung (Bst. c).

- In Buchstabe a ist neu die Eingabekontrolle geregelt. Diese verlangt – entsprechend Artikel 9 Absatz 2 Buchstabe h VDSG –, dass nachträglich überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert wurden. Das Schutzziel wurde so angepasst, dass neu explizit zum Ausdruck kommt, dass auch die Veränderung von Personendaten nachträglich überprüfbar sein muss. Als mögliche Massnahme kommt insbesondere die Protokollierung in Betracht.
- Buchstabe b betrifft die Bekanntgabekontrolle. Sie wurde von Artikel 9 Absatz 1 Buchstabe d VDSG übernommen und in der Formulierung leicht angepasst. Gemäss dem neuen Buchstaben b kann überprüft werden, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben wurden. Die Massnahmen sollen es insbesondere ermöglichen, die Datenempfängerinnen und Datenempfänger zu identifizieren. Dabei kann es u. U. ausreichend sein, dass das Organ als solches bekannt ist, ohne dass die natürliche Person in jedem Fall identifizierbar sein muss. Bei Bedarf muss z. B. anhand von Protokollen feststellbar sein, mit welchen Mitteln welche Personendaten an wen bekanntgegeben wurden.
- Buchstabe c verlangt, dass der Verantwortliche und der Auftragsbearbeiter Verletzungen der Datensicherheit im Sinne von Artikel 5 Buchstabe h nDSG rasch erkennen und Mass-

nahmen zur Minderung oder Beseitigung deren Folgen einleiten können. Anders als bei Absatz 2 Buchstabe e geht es hier insbesondere um reaktive Massnahmen, die vom Verantwortlichen und vom Auftragsbearbeiter getroffen werden.

Artikel 9 Absatz 2 VDSG wurde gestrichen, da er aus Sicht des Bundesrats nicht mehr notwendig ist. Die Gründe für die Verweigerung, Einschränkung oder Aufschiebung eines Auskunftsgesuches werden auf Gesetzesebene festgelegt (vgl. Art. 26 nDSG). So sind die Verantwortlichen und Auftragsbearbeiter bereits aufgrund des nDSG verpflichtet, dafür zu sorgen, dass die Betroffenen ihre Rechte wirksam wahrnehmen können, und dies unabhängig von den konkret angewendeten Technologien zur Bearbeitung der Personendaten.

Art. 4 Protokollierung

Die Protokollierung wird in Artikel 10 VDSG geregelt, der aufgrund des Verweises in Artikel 20 Absatz 1 erster Satz VDSG auch auf Bundesorgane Anwendung findet. Artikel 4 übernimmt diese Regelung in geänderter Form. Die Protokollierung stellt eine Massnahme im Sinne von Artikel 3 DSV dar. Dadurch wird dem Umstand Rechnung getragen, dass das Schweizer Recht im Unterschied zur DSGVO keine allgemeine «Rechenschaftspflicht» vorsieht. Überdies wird die Protokollierung auch von gewissen europäischen Datenschutzbehörden empfohlen.[15] Ausserdem handelt es sich bei der Protokollierung um ein klassisches, präventives Mittel zur Gewährleistung der Cybersicherheit.

Der Zweck der Protokollierung besteht darin, dass Bearbeitungen von Personendaten nachträglich überprüfbar sind, so dass im Nachhinein festgestellt werden kann, ob Daten abhandengekommen sind oder gelöscht, vernichtet, verändert oder offengelegt wurden. Ausserdem geht es auch um die Gewährleistung der Zweckkonformität und einer angemessenen Datensicherheit. So können sich aus der Protokollierung auch Hinweise ergeben, ob Personendaten zweckkonform bearbeitet wurden. Weiter können die Protokollierungen auch dazu dienen, Verletzungen der Datensicherheit aufzudecken und aufzuklären. Die Protokollierung hat hingegen nicht zum Ziel, die Nutzerinnen und Nutzer, die Personendaten bearbeiten, zu überwachen. Bei der Protokollierung handelt es sich um einen automatisierten Prozess. Heutzutage gibt es kaum ein Informationssystem oder ein System zur automatisierten Datenbearbeitung, in dem die Datenbearbeitung nicht protokolliert wird.

Artikel 4 Absatz 1 DSV verlangt die Protokollierung für den privaten Verantwortlichen und seinen privaten Auftragsbearbeiter bei der automatisierten Bearbeitung besonders schützenswerter Daten in grossem Umfang oder beim Profiling mit hohem Risiko, wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten können und wenn ohne diese Massnahme nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden. Protokolliert werden müssen zumindest die Vorgänge des Speicherns, Veränderns, Lesens, Bekanntgebens, Löschens und Vernichtens von Daten. Der Vorgang des «Lesens» ist als Zugriff ohne «Verändern» zu verstehen; es reicht demnach aus, wenn die Zugriffe auf Personendaten und das Verändern dieser Daten protokolliert werden. Der Protokollierung des «Lesens» wird damit Genüge getan. Der Satzteil «können die präventiven Massnahmen den Datenschutz nicht gewährleisten» wurde aus dem geltenden Recht übernommen. In der Praxis ist er von untergeordneter Bedeutung, da die präventiven Massnahmen den Datenschutz nur selten gewährleisten.

[15] Siehe z. B. CNIL, Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation (Beschluss über die Annahme einer Empfehlung zur Protokollierung).

Gemäss Absatz 2 protokollieren das verantwortliche Bundesorgan und sein Auftragsbearbeiter bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten. Dies sind die gleichen Bearbeitungsvorgänge, die auch der private Verantwortlichen protokollieren muss, allerdings muss die Protokollierung bei Bundesorganen in einer grösseren Anzahl von Fällen (bei jeder automatisierten Bearbeitung) erfolgen. Damit wird den im Rahmen der Schengener Zusammenarbeit im Strafrechtsbereich geltenden Anforderungen von Artikel 25 der Richtlinie (EU) 2016/680 Rechnung getragen. Wie oben ausgeführt, ist es in Bezug auf das «Lesen» ausreichend, wenn die Zugriffe auf Personendaten und das Verändern dieser Daten protokolliert werden. Für die Umsetzung der Protokollierungspflicht wird für Datenbearbeitungen, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, in Artikel 46 Absatz 1 eine Übergangsfrist von drei Jahren vorgesehen.

In Absatz 3 wird neu festgehalten, dass bei Personendaten, welche allgemein öffentlich zugänglich sind, zumindest das Speichern, Verändern, Löschen und Vernichten der Daten protokolliert werden muss. Dies bedeutet z.B., dass die Konsultation des Staatskalenders, der allgemein öffentlich zugänglich ist, nicht zwingend protokolliert werden muss.

Die Regelung wurde mit einem neuen Absatz 4 ergänzt, wo die Inhalte der Protokollierung konkretisiert werden. So muss die Protokollierung Aufschluss geben über die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.

In Absatz 5 wird Artikel 10 Absatz 2 VDSG in leicht geänderter Form übernommen. Die Protokolle müssen während mindestens eines Jahres getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden. Dies bedeutet allerdings nicht, dass die Protokolle während einer unverhältnismässig langer Dauer aufbewahrt werden dürfen. Die Aufbewahrungsdauer muss im Vergleich zum Ziel einer angemessenen Datensicherheit in einem angemessenen Verhältnis stehen. Im Übrigen bleiben für Bundesorgane jedenfalls die spezialrechtlichen Vorschriften vorbehalten. So sieht insbesondere die Verordnung vom 22. Februar 2012[16] über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen, in Artikel 4 Absatz 1 Buchstabe b vor, dass Daten über die Nutzung der elektronischen Infrastruktur längstens zwei Jahre aufbewahrt werden dürfen. Die getrennte Aufbewahrung vom System ist notwendig, da ansonsten bei Cyberangriffen auch das Protokoll selber manipuliert oder verschlüsselt werden könnte. Die Protokolle sind ausschliesslich den Organen oder Personen zugänglich, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden. Mit letzterer Ergänzung kommt im Verordnungstext neu zum Ausdruck, dass die Protokolle auch Sicherheitsverantwortlichen zugänglich sein sollen, damit diese die Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten wiederherstellen können. Mit dem Ausdruck Wahrung soll überdies sichergestellt werden, dass auch Systemadministratoren Zugriff auf auf die im System generierten Protokolle haben, wenn sie den Verdacht haben, dass eine Sicherheitslücke besteht. Diese Daten dürfen folglich nicht zum Zweck der Überwachung der Nutzer und Nutzerinnen, insbesondere ihrer beruflichen Tätigkeit, verwendet werden. Vorbehalten bleibt natürlich die Verwendung für spezialgesetzlich vorgesehene Zwecke, wie etwa eine allfällige Verwendung in einem Strafverfahren.

[16] SR **172.010.442**

Artikel 10 Absatz 1 dritter Satz VDSG wurde gestrichen. Er wäre systemwidrig, wenn der EDÖB im Bereich der Datensicherheit, die gemäss Artikel 61 Buchstabe c der Strafbarkeit unterliegt, Empfehlungen aussprechen könnte. Zudem kann der EDÖB gemäss seiner allgemeinen Verfügungskompetenz im Rahmen einer Untersuchung nach Artikel 51 nDSG ohnehin eine Protokollierung anordnen.

Art. 5 Bearbeitungsreglement von privaten Personen

Ein Bearbeitungsreglement erstellen musste der «Inhaber einer meldepflichtigen automatisierten Datensammlung» nach Artikel 11*a* Absatz 3 DSG, der nicht aufgrund von Artikel 11*a* Absatz 5 Buchstaben b–d DSG von der Pflicht, seine Datensammlungen anzumelden, ausgenommen war (Art. 11 Abs. 1 VDSG). Da die Meldepflicht für private Verantwortliche (Art. 11*a* DSG) im nDSG nicht mehr besteht, kann Artikel 11 VDSG nicht unverändert übernommen werden. Gemäss dem in der DSGVO vorgesehenen Grundsatz der Rechenschaftspflicht oder «accountability» muss der Verantwortliche die Einhaltung der Grundsätze der Datenbearbeitung nachweisen können (Art. 5 Abs. 2 DSGVO). Das Schweizer Recht kennt keine allgemeine Rechenschaftspflicht oder «accountability», aber die Pflicht zur Erstellung eines Bearbeitungsreglements erfüllt denselben Zweck.

Die Pflicht zur Erstellung eines Bearbeitungsreglements obliegt dem Verantwortlichen sowie dessen Auftragsbearbeiter. Private Auftragsbearbeiter, die im Auftrag von Bundesorganen handeln, fallen unter Artikel 6. Sollte ausnahmsweise einmal ein Bundesorgan als Auftragsbearbeiter eines privaten Verantwortlichen handeln, fällt es nicht unter Artikel 5, wo nur private Auftragsbearbeiter erfasst werden, sondern unter den strengeren Artikel 6. Das rechtfertigt sich durch die besondere Stellung und Verantwortung, die sich aus der Rechtsnatur des Bundesorgans ergibt. Die Bearbeitungsreglemente sind separat zu erstellen.

Entsprechend dem risikobasierten Ansatz der Vorgabe der Datensicherheit soll ein Bearbeitungsreglement immer dann erstellt werden, wenn ein erhöhtes Risiko vorliegt. So müssen private Verantwortliche ein Bearbeitungsreglement für automatisierte Bearbeitungen erstellen, wenn sie besonders schützenswerte Personendaten in grossem Umfang bearbeiten (Bst. a) oder ein Profiling mit hohem Risiko durchführen (Bst. b). Buchstabe a entspricht der Vorgabe in Artikel 22 Absatz 2 Buchstabe a nDSG und bezieht sich auf die Bearbeitung von besonders schützenswerten Personendaten in grossem Umfang. Ausgeschlossen werden damit Fälle, in denen besonders schützenswerte Personen nur vereinzelt bearbeitet werden. Viele Unternehmen, insbesondere «traditionelle» KMU, nehmen keine solche Bearbeitungen vor. Sie sind somit von dieser Bestimmung nicht betroffen.

Absatz 2 enthält eine Auflistung der Inhalte, die im Bearbeitungsreglement mindestens angegeben werden müssen. Die Inhalte wurden von Artikel 11 Absatz 1 bzw. Artikel 21 Absatz 2 VDSG in leicht angepasster Form übernommen und ergänzt. Wie bis anhin ist das Bearbeitungsreglement als eine Dokumentation oder ein Handbuch auszugestalten und sollte dem Verantwortlichen auch dazu dienen.[17]

Wie bisher müssen der private Verantwortliche und Auftragsbearbeiter im Bearbeitungsreglement die interne Organisation beschreiben. Dazu gehört auch die Umschreibung der Architektur und der Funktionsweise der Systeme.

[17] Vgl. Kommentar BJ, 6.1.4.

Absatz 2 legt fest, dass die Datenbearbeitungsverfahren, d. h. insbesondere die Verfahren zum Speichern, Berichtigen, Bekanntgeben, Aufbewahren, Archivieren, Pseudonymisieren, Anonymisieren, Löschen oder Vernichten der Daten, im Bearbeitungsreglement enthalten sein müssen. Dazu gehören auch Massnahmen zur Datenminimierung. Der Grundsatz der Datenminimierung ist ein zentraler Grundsatz des Datenschutzes und geht, wie der Botschaft DSG vom 15. September 2017 zu entnehmen ist[18], implizit aus dem Grundsatz der Verhältnismässigkeit gemäss Artikel 6 Absatz 2 nDSG hervor. Es soll insbesondere festgehalten werden, welche Datenbearbeitungsverfahren vorgenommen werden und wie diese ablaufen. Das Reglement muss auch das Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung enthalten. Die Kontrollverfahren müssen es ermöglichen, die Zugriffsberechtigungen, die Art und den Umfang des Zugriffs festzustellen. Schliesslich ist es von entscheidender Bedeutung, dass das Bearbeitungsreglement auch die technischen und organisatorischen Massnahmen zur Gewährleistung der angemessenen Datensicherheit umfasst. So ist etwa anzugeben, mit welchen Massnahmen den Schutzzielen nach Artikel 2 Rechnung getragen wird. Die Angaben sollten auch Aufschluss über die Konfiguration der Informatikmittel geben, da es sich dabei um eine technische Massnahme handelt. Der bisherige Artikel 21 Absatz 2 Buchstabe h VDSG, der die Konfiguration der Informatikmittel noch ausdrücklich nennt, wurde deshalb nicht übernommen. Es ist dabei ausreichend, dass die wichtigsten Grundkonfigurationen der Informatikmittel im Bearbeitungsreglement erläutert werden. Sie müssen aber nicht bis in die technischen Details ausgeführt werden.

Absatz 3 stellt eine Übernahme von Artikel 11 Absatz 2 VDSG dar. Im Vergleich zum geltenden Recht wurde auf die Ergänzung, dass das Bearbeitungsreglement der Beraterin oder dem Berater in einer für diese oder diesen verständlichen Form zur Verfügung zu stellen ist, verzichtet. Da die Beraterin oder der Berater selbst an der Erstellung des Reglements mitwirkt, ist dieses für sie oder ihn in aller Regel auch verständlich. Die Verpflichtung, dass das Bearbeitungsreglement auch dem Beauftragten auf Anfrage zur Verfügung zu stellen ist, wurde gestrichen. Analog zum Verzeichnis der Bearbeitungstätigkeiten kann der EDÖB dieses aber im Rahmen einer Untersuchung herausverlangen (Art. 50 Abs. 1 Bst. a nDSG).

Art. 6 Bearbeitungsreglement der Bundesorgane

Artikel 6 entspricht, mit einigen Änderungen, Artikel 21 VDSG.

Die Pflicht zur Erstellung eines Bearbeitungsreglements obliegt dem verantwortlichen Bundesorgan sowie dessen Auftragsbearbeiter. Wie oben erwähnt, betrifft Artikel 6 sowohl private Auftragsbearbeiter als auch Bundesorgane, die ausnahmsweise als Auftragsbearbeiter fungieren. Die Bearbeitungsreglemente sind separat zu erstellen.

Im Einleitungssatz von Absatz 1 wird der in Artikel 21 Absatz 1 Einleitungssatz VDSG vorkommende Begriff «Datensammlungen» durch «Bearbeitungen» ersetzt, weil er im nDSG nicht mehr verwendet wird. Diese Bestimmung sieht nun vor, dass die verantwortlichen Bundesorgane in den Fällen nach Absatz 1 Buchstaben a–f ein Bearbeitungsreglement erstellen.

Mit dem nDSG wird der Begriff «Persönlichkeitsprofil» aufgehoben und der Begriff «Profiling» eingeführt. Dementsprechend ist Artikel 21 Absatz 1 Buchstabe a VDSG zu ändern und in Artikel 6 Absatz 1 DSV vorzusehen, dass das verantwortliche Bundesorgan und dessen Auf-

[18] BBl **2017** 6941, 7024.

tragsbearbeiter ein Bearbeitungsreglement erstellen muss, wenn es besonders schützenswerte Personendaten bearbeitet (Bst. a), ein Profiling nach Artikel 5 Buchstabe f nDSG durchführt (Bst. b) oder nach Artikel 34 Absatz 2 Buchstabe c nDSG Daten bearbeitet (Bst. c). Der Fall nach Buchstabe a entspricht dem bisherigen Recht nach dem DSG. Die Buchstaben b und c sind neu. Sie ersetzen Artikel 21 Absatz 1 Buchstabe a VDSG, der das verantwortliche Bundesorgan verpflichtet, für alle automatisierten Datensammlungen, die Persönlichkeitsprofile beinhalten, ein Bearbeitungsreglement zu erstellen.

Artikel 6 Absatz 1 Buchstabe d DSV erfährt gegenüber Artikel 21 Absatz 1 Buchstabe c VDSG nur ein paar redaktionelle Änderungen.

In Artikel 6 Absatz 1 Buchstabe e wird der im entsprechenden Artikel 21 Absatz 1 Buchstabe d VDSG verwendete Begriff «Datensammlungen» durch «Datenbestände» ersetzt.

Aufgrund von Artikel 6 Absatz 1 Buchstabe f DSV ist ein Bearbeitungsreglement auch dann zu erstellen, wenn das verantwortliche Bundesorgan zusammen mit anderen Bundesorganen ein Informationssystem betreibt oder Datenbestände bewirtschaftet. Diese Bestimmung ersetzt Artikel 21 Absatz 1 Buchstabe b VDSG, wonach eine solche Pflicht besteht, wenn eine automatisierte Datensammlung von mehreren Bundesorganen benutzt wird.

Absatz 2 entspricht dem Inhalt des Bearbeitungsreglements für Private nach Artikel 5 Absatz 2 DSV. Es ist an dieser Stelle deshalb auf die oben gemachten Ausführungen zu verweisen.

Absatz 3 wurde in leicht angepasster Form von Artikel 21 Absatz 3 VDSG übernommen. Wie in Artikel 5 Absatz 3 DSV wurde auch an dieser Stelle die Bereitstellung in verständlicher Form gestrichen. Der Begriff «Kontrollorgane» wird durch «Datenschutzberaterin oder Datenschutzberater» ersetzt. Auf die Erwähnung des EDÖB wurde aus den oben im Zusammenhang mit Artikel 5 Absatz 3 DSV genannten Gründen verzichtet.

5.1.2 2. Abschnitt: Bearbeitung durch Auftragsbearbeiter

Art. 7

Artikel 7 DSV regelt die Art der vorgängigen Genehmigung, mit welcher ein Verantwortlicher einen Auftragsbearbeiter zur Übertragung der Datenbearbeitung auf einen Dritten ermächtigen kann, geregelt. Diese Bestimmung orientiert sich an Artikel 22 Absatz 2 der Richtlinie (EU) 2016/680 bzw. Artikel 28 Abs. 2 DSGVO. Sie hält aus Gründen der Rechtssicherheit ausdrücklich fest, was der Bundesrat bereits in der Botschaft zur Totalrevision des Datenschutzgesetzes zur Genehmigung der Subauftragsbearbeitung ausgeführt hat (vgl. BBl *2017* 6941, 7032). Die vorgängige Genehmigung des Verantwortlichen kann spezifischer oder allgemeiner Art sein (Art. 7 Abs. 1 DSV). Bei einer allgemeinen Genehmigung muss der Auftragsbearbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines anderen Subauftragsbearbeiters informieren. Der Verantwortliche kann Widerspruch gegen diese Änderung erheben (Art. 7 Abs. 2 DSV).

5.1.3 3. Abschnitt: Bekanntgabe von Personendaten ins Ausland

Entsprechend der Systematik des Gesetzes wurden die Bestimmungen zur Bekanntgabe von Personendaten ins Ausland bei den allgemeinen Bestimmungen im 1. Kapitel platziert. Mehrere Begriffe im Zusammenhang mit der Datenbekanntgabe ins Ausland sind zu präzisieren. In der DSV erfolgt dies in fünf verschiedenen Artikeln: In einem ersten Artikel werden die Kriterien konkretisiert, die der Bundesrat bei der Beurteilung berücksichtigen muss, ob ein

Staat, ein Gebiet, ein spezifischer Sektor in einem Staat oder eine internationale Organisation einen angemessenen Datenschutz gewährleistet; ein zweiter Artikel legt dar, was die Datenschutzklauseln in einem Vertrag und die spezifischen Garantien zur Gewährleistung eines geeigneten Datenschutzes regeln müssen; in einem dritten Artikel geht es um die Standarddatenschutzklauseln; ein vierter Artikel konzentriert sich auf verbindliche unternehmensinterne Datenschutzvorschriften; aufgrund der in Artikel 16 Absatz 3 nDSG dem Bundesrat zugewiesenen Kompetenz werden in einer letzten Bestimmung weitere geeignete Garantien vorgesehen.

Art. 8 Beurteilung der Angemessenheit des Datenschutzes eines Staates, eines Gebiets, eines spezifischen Sektors in einem Staat oder eines internationalen Organs

Sind bestimmte Kriterien erfüllt, kann der Bundesrat beurteilen, dass ein Staat bzw. ein Gebiet, ein spezifischer Sektor in einem Staat oder ein internationales Organ einen angemessenen Schutz gewährleistet. Gemäss Artikel 7 Absatz 1 Buchstabe d der Organisationsverordnung vom 17. November 1999[19] für das Eidgenössische Justiz- und Polizeidepartement (OV-EJPD) fällt die Aufgabe, die Gewährleistung eines angemessenen Datenschutzes eines Staates, eines Gebietes, eines spezifischen Sektors in einem Staat oder eines internationalen Organs in die Zuständigkeit des Bundesamt für Justiz.[20]

Gemäss Artikel 8 Absatz 1 DSV werden die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe, deren Datenschutz als angemessen eingestuft wurde, im Anhang der Verordnung aufgeführt. Wie in der Botschaft[21] erläutert, handelt es sich dabei um eine «Positiv-Liste». Wenn ein Staat nicht enthalten ist, bedeutet dies nicht zwangsläufig, dass er keine Datenschutzgesetzgebung hat, die ein angemessener Datenschutz gewährleistet; vielmehr ist es denkbar, dass der Staat vom Bundesrat (noch) nicht beurteilt wurde. Nur Staaten, die in der Liste im Anhang aufgeführt werden, können daher als Staaten angesehen werden, die einen angemessenen Datenschutz gewährleisten. Dieses Vorgehen unterscheidet sich etwas vom Vorgehen des EDÖB. Der EDÖB hat nämlich bisher zu jedem Staat angegeben, ob dieser einen angemessenen Schutz, einen unter bestimmten Voraussetzungen angemessenen Schutz oder einen ungenügenden Schutz gewährleistet. Es ist auch darauf hinzuweisen, dass die Liste des EDÖB nicht verbindlich ist und insbesondere die Gerichte im Streitfall nicht bindet.[22] Bevor die Faktoren, die der Bundesrat bei der Beurteilung berücksichtigen muss, im Einzelnen erörtert werden, sollte zunächst geklärt werden, was unter einem «Gebiet» oder einem «spezifischen Sektor in einem Staat» zu verstehen ist. Der Begriff «Gebiet» bezieht sich auf Fälle, in denen das Land nicht einer einzigen Gesetzgebung unterliegt. Dies betrifft namentlich der Fall von föderalen Staaten, nämlich wenn die Gesetzgebung des Zentralstaates nicht einen angemessenen Schutz gewährleistet, während ein Bundesstaat über eine angemessene Datenschutzgesetzgebung verfügt, das jedoch nur auf seinem eigenen Hoheitsgebiet gilt. Zum Begriff «spezifischer Sektor in einem Staat» kann beispielsweise die Liste des EDÖB angeführt werden, in der unter Kanada berücksichtigt wird, dass auf Grundlage eines spezifischen Datenschutzgesetzes für den privaten Bereich nur für diesen Bereich ein angemessenes Schutzniveau anerkannt werden kann.[23] Bis im Juli 2020

---

[19] SR **172.213.1**

[20] BBl **2017** 6941, 7179.

[21] BBl **2017** 7038

[22] Vgl. Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Bern 2011, S. 450 f.

[23] Vgl. https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_d.pdf. In diesem Sinne siehe auch die Angemessenheitsentscheidung der Europäischen Kommission für Kanada, in der anerkannt wird, dass die spezifischen Rechtsvorschriften für den privaten Bereich ein angemessenes Schutzniveau gewährleisten: Entscheidung 2002/2/EG der Kommission vom 20. Dezember 2001 gemäss der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit

galt dies aufgrund des *Privacy Shield CH–US*, der die freie Datenübermittlung nur an Unternehmen erlaubte, die sich zur Einhaltung der verbindlichen Grundsätze des Privacy Shield verpflichtet hatten, auch für die USA.[24] Zu nennen sind weitere spezifische Sektoren wie der Finanz- oder Versicherungssektor oder die Datenbearbeitung durch Auftragsbearbeiter.[25] Der Begriff des internationalen Organs wurde in der Botschaft zum Datenschutzgesetz präzisiert. Er bezieht sich auf «alle internationalen Institutionen, seien dies Organisationen oder Gerichte» (BBl *2017* 6941, 7038)[26].

Beim Entscheid, ob ein Staat, ein Gebiet, ein spezifischer Sektor in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, müssen unter anderem die folgenden Kriterien berücksichtigt werden (Art. 8 Abs. 2 DSV):

- Die internationalen Verpflichtungen des betroffenen Staates oder des internationalen Organs, insbesondere im Bereich des Datenschutzes (Abs. 2 Bst. a): Angesprochen wird damit insbesondere das revidierte Übereinkommen SEV 108.[27] Von Bedeutung sind aber nicht nur Abkommen im Bereich des Datenschutzes, weshalb der Ausdruck «insbesondere» verwendet wird (siehe ebenfalls die Erläuterung zu Bst. c). So können beispielswiese auch Abkommen zur Regelung des Informationsaustauschs beispielsweise spielen auch eine Rolle.
- Die Rechtsstaatlichkeit und die Achtung der Menschenrechte (Abs. 2 Bst. b): In Buchstabe b wird der Begriff «Menschenrechte» verwendet, um die gleiche Terminologie wie in der EMRK und im UNO-Pakt II zu verwenden. Der Bundesrat verfügt über den nötigen Ermessensspielraum, um festzustellen, ob ein Staat einen angemessenen Datenschutz gewährleistet, auch wenn er sich nicht vollumfassend an die international anerkannten Menschenrechte hält. Wichtig ist dabei, dass der Schutz vor unverhältnismässigen Eingriffen in das Privatleben gewährleistet wird, auch wenn der Staat beispielsweise nicht in allen Punkten die Anforderungen der EMRK erfüllt.
- Die geltende Gesetzgebung insbesondere zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung (Abs. 2 Bst. c): Aufgrund des Ausdrucks «insbesondere» ist auch die sektorielle Gesetzgebung mitgemeint. Diese enthalten oft (direkte und/oder indirekte) Regelungen zum Datenschutz. Das gilt z.B. für Staaten, die kein Rahmengesetz zum Datenschutz haben, sondern einzig ein Zivilgesetzbuch. In einigen Fällen haben diese Staaten sektorielle Gesetze, die Datenschutzbestimmungen enthalten. Wichtig ist, dass die anwendbaren Gesetze auch gelten. Daher wird der Fokus auf die einschlägige allgemeine und besondere Gesetzgebung des Staates gerichtet, einschliesslich derjenigen zur öffentlichen Sicherheit, zur Verteidigung, zur nationalen Sicherheit, zum Strafrecht und zum Zugang der Behörden zu Personendaten.
- Die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes (Abs. 2 Bst. d): Es geht nicht nur darum, zu überprüfen, ob die Rechte der betroffenen Personen in Rechtsgrundlagen enthalten sind, sondern auch darum, sicherzustellen, dass diese Rechte tatsächlich umgesetzt werden.

---

des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, ABl. L 2 vom 4. Januar 2002.

[24] Nachdem der EuGH am 16. Juli 2020 den Privacy Shield EU-USA für ungültig erklärt hatte (Urteil «Schrems II»), hat der EDÖB in seiner Staatenliste den Verweis auf einen «angemessenen Datenschutz unter bestimmten Bedingungen» für die USA gestrichen. Siehe dazu die Medienmitteilung des EDÖB (https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-80318.html) und seine Stellungnahme (https://www.newsd.admin.ch/newsd/message/attachments/64258.pdf).

[25] Vgl. De Terwangne, Cécile / Gayrel, Claire, Le RGPD et les transferts internationaux de données à caractère personnel, in: Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie, Cahiers du CRIDS; No. 44, 2018, S. 297 (http://www.crid.be/pdf/public/8344.pdf).

[26] Die oben zitierten Autorinnen nennen beispielsweise die Welt-Anti-Doping-Agentur in Montreal, an die besonders schützenswerte Daten zur Gesundheit der Leistungssportlerinnen und -sportler übermittelt werden. De Terwangne, Cécile / Gayrel, Claire, S. 296.

[27] Protokoll zur Änderung des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SEV Nr. 223.

– Das wirksame Funktionieren einer oder mehrerer unabhängiger Behörden, die im betroffenen Staat mit dem Datenschutz beauftragt sind oder denen ein internationales Organ untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen. In diesem Sinne müssen die Mindestanforderungen des revidierten Übereinkommens SEV 108 erfüllt sein (Abs. 2 Bst. e).

Der dritte Absatz bestimmt, dass der EDÖB bei jeder Beurteilung der Angemessenheit konsultiert wird. Seine Stellungnahme ist für den Bundesrat nicht verbindlich, muss aber berücksichtigt werden, insbesondere im Rahmen der Ämterkonsultation. Der EDÖB kann seine Stellungnahme darüber hinaus veröffentlichen. Der Bundesrat kann auch eine Beurteilung des Schutzniveaus berücksichtigen, welche von einer ausländischen Behörde, die für den Datenschutz zuständig ist (und zu einem Staat mit einem angemessenen Schutzniveau gehört) oder von einem internationalen Organ vorgenommen wurde. Als internationales Organ im Sinne dieses Absatzes kann unter anderem der mit dem revidierten Übereinkommen SEV 108 eingesetzte Ausschuss der Vertragsparteien gelten. Auch Beurteilungen, welche die Europäische Kommission vorgenommen hat, können als Informationsquelle dienen.

Der vierte Absatz sieht vor, dass das Schutzniveau im betreffenden Staat oder im betreffenden Organ periodisch neu beurteilt wird.

Aufgrund der verschiedenen Stellungnahmen im Rahmen des Vernehmlassungsverfahrens sieht ein neuer Absatz 5 vor, dass die vom Bundesamt für Justiz durchgeführten Beurteilungen veröffentlicht werden. Der Begriff der Beurteilung umfasst sowohl die Beurteilung als auch die Neubeurteilung von Staaten, Gebieten, spezifischen Sektoren in einem Staat oder internationalen Organen, die bereits auf der Liste stehen und erneut beurteilt werden. In einer neuen Übergangsbestimmung (Art. 46 Abs. 2) wird klargestellt, dass die Beurteilungen, die vor dem Inkrafttreten der DSV durchgeführt wurden, nicht veröffentlicht werden.

Die Verordnung führt neu die Vornahme einer Interessensabwägung ein, die es ermöglicht, in dringlichen Fällen zu handeln, wenn darauf geschlossen werden kann, dass die Angemessenheit nicht mehr gewährleistet ist. Nach Absatz 6 wird Anhang 1 geändert, wenn festgestellt wird, dass das der Datenschutz in einem Staat, einem Gebiet, einem spezifischen Sektor in einem Staat oder einem internationalen Organ nicht mehr gewährleistet werden kann. Im Fall der USA hat beispielsweise das Urteil «Schrems II» des EuGH vom Juli 2020 den EDÖB dazu veranlasst, seine Einschätzung zu überdenken und seine Liste zu ändern. Wenn Informationen darauf schliessen lassen, dass ein betroffener Staat keinen angemessenen Datenschutz mehr gewährleistet (z. B. aufgrund einer Staatskrise), kann der Bundesrat die Liste dringlich ändern, ohne eine formelle und vollständige Prüfung durchgeführt zu haben. Denn nach Artikel 7 Absatz 3 PublG[28] sind dringliche Veröffentlichungen möglich. Dies gilt allerdings nur bei einer Streichung aus der Liste. Bei einer Hinzufügung zur Liste muss dem Beurteilungsverfahren gefolgt werden (Abs. 1 und 2). Die Änderung hat keine Auswirkungen auf bereits erfolgte Datenbekanntgaben.

Art. 9 Datenschutzklauseln und spezifische Garantien

Nach Artikel 16 Absatz 2 nDSG dürfen Personendaten an einen Staat bekanntgegeben werden, der nicht in Anhang 1 der Verordnung aufgeführt ist – d. h. ohne dass der Bundesrat die Angemessenheit des Datenschutzes als angemessen anerkannt hat –, wenn ein geeigneter

[28] SR **170.512**

Datenschutz gewährleistet wird. Im privaten Sektor kann dieser durch eine Datenschutzklausel in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner gewährleistet sein (Art. 16 Abs. 2 Bst. b nDSG), im öffentlichen Sektor durch spezifische Garantien, die das zuständige Bundesorgan erarbeitet hat (Art. 16 Abs. 2 Bst. c nDSG).

Anders als bei den übrigen in Absatz 2 von Artikel 16 nDSG genannten Instrumenten müssen die Verantwortlichen und die Auftragsbearbeiter diese Garantien nicht vom EDÖB genehmigen lassen, sondern ihm diese vor der Datenbekanntgabe ins Ausland nur mitteilen. Es besteht ein gewisses Risiko, dass die Verantwortlichen und die Auftragsbearbeiter das Schutzniveau, das mit diesen Garantien erreicht werden soll, unterschiedlich beurteilen, wobei dies für den privaten Sektor ebenso gilt wie für den öffentlichen Sektor.

Der Bundesrat erachtet es deshalb als angezeigt, bestimmte Datenschutzstandards festzulegen, und präzisiert in Artikel 9 Absatz 1 DSV, was diese Datenschutzklauseln oder spezifischen Garantien mindestens regeln müssen.

Es handelt sich um folgende Punkte:

- Die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Transparenz, der Zweckbindung und der Richtigkeit (Bst. a).
- Die Kategorien der bekanntgegebenen Personendaten und der betroffenen Personen (Bst. b).
- Die Art und den Zweck der Bekanntgabe von Personendaten (Bst. c).
- Gegebenenfalls die Namen der Staaten oder internationalen Organe, in die oder denen Personendaten bekanntgegeben werden, sowie die Anforderungen an die Bekanntgabe (Bst. d): Der Ausdruck «gegebenenfalls» bietet die Möglichkeit, sich an die Umstände eines Vertrags anzupassen. In bestimmten sehr eng gefassten Verträgen kommt dieser Buchstabe nicht in Betracht. Wenn z.B. im Rahmen des Vertrags keine Daten an ein internationales Organ bekanntgegeben werden, wäre ein solcher Hinweis natürlich überflüssig.
- Die Anforderungen an die Aufbewahrung, die Löschung und Vernichtung von Personendaten (Bst. e).
- Die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger (Bst. f): Die Kategorien von Empfängerinnen und Empfängern können nützlich sein, wenn auch in der Angabe einer generischen Form, soweit dies erforderlich ist (z. B.: Vertreter und Vertreterinnen, Auftragsbearbeiter, Mitverantwortliche, behandelnde Ärztinnen und Ärzte, Gemeinden, externe Partnerorganisationen usw.).
- Die Massnahmen zur Gewährleistung der Datensicherheit (Bst. g).
- Die Pflicht, Verletzungen der Datensicherheit zu melden (Bst. h).
- Falls die Empfängerinnen und Empfänger Verantwortliche sind: die Pflicht, die betroffenen Personen über die Bearbeitung zu informieren (Bst. i): Die Empfängerin oder der Empfänger als Auftragsbearbeiter kann nicht verantwortlich sein und dieser Pflicht nachkommen.
- Die Rechte der betroffenen Person (Bst. j), insbesondere: das Auskunftsrecht und das Recht auf Datenherausgabe oder -übertragung (Ziff. 1), das Recht, der Datenbekanntgabe zu widersprechen (Ziff. 2), das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten (Ziff. 3) und das Recht, eine unabhängige Behörde (Datenschutzbehörde oder Gericht) um Rechtsschutz zu ersuchen (Ziff. 4).

Alle diese Punkte entsprechen den Grundlagen des nDSG. In Absatz 2 wird ferner klargestellt, dass der Verantwortliche bei einer Bekanntgabe der Personendaten ins Ausland angemessene Massnahmen treffen muss, um sicherzustellen, dass die Empfängerin oder der

Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält; der Auftragsbearbeiter muss dies im Fall von Datenschutzklauseln in einem Vertrag ebenfalls sicherstellen (die Auftragsbearbeitung ist auf die spezifischen Garantien nicht anwendbar). So kann mit diesem Absatz (der im Wesentlichen Art. 6 Abs. 2 und 4 VDSG übernimmt) sichergestellt werden, dass die Empfängerin oder der Empfänger der bekanntgegebenen Daten den in der Schweiz geltenden Datenschutzrahmen einhält.

Ein dritter Absatz übernimmt Artikel 6 Absatz 2 VDSG zur Informationspflicht des Verantwortlichen. Er wird nur redaktionell angepasst (z. B. wird in der französischen Version der Begriff «maître du fichier» ersetzt), indem der zweite Teilsatz in Artikel 6 Absatz 2 Buchstabe b VDSG gelöscht wird. Eine Bekanntgabe ins Ausland ist ohnehin nur zulässig, wenn die Datenschutzklauseln oder Garantien einen geeigneten Schutz gewährleisten, indem sie namentlich den Anforderungen von Artikel 9 Absatz 1 DSV gerecht werden. Es ist deshalb nicht notwendig, dies in Artikel 9 Absatz 3 Buchstabe b DSV nochmals zu erwähnen.

Art. 10 Standarddatenschutzklauseln

Wie bei der Datenbekanntgabe ins Ausland, die sich auf Datenschutzklauseln in einem Vertrag und auf spezifische Garantien stützt, sind auch bei der Datenbekanntgabe mittels Standarddatenschutzklauseln (Art. 16 Abs. 2 Bst. d nDSG) die schweizerischen Datenschutzvorschriften einzuhalten. So präzisiert Artikel 10 Absatz 1 DSV, der Artikel 6 Absatz 4 VDSG grundsätzlich entspricht, dass der Verantwortliche oder der Auftragsbearbeiter angemessene Massnahmen treffen muss, um sicherzustellen, dass die Empfängerin oder der Empfänger die Standardklauseln tatsächlich beachtet. Im Kommentar des Bundesamtes für Justiz zur VDSG[29] wird diese Sorgfaltspflicht wie folgt präzisiert: «Die Angemessenheit der geforderten Massnahmen richtet sich nach den Umständen im konkreten Fall und dem Stand der Technik. Geht es um besonders schützenswerte Personendaten oder Persönlichkeitsprofile, sind die Anforderungen höher, als wenn es um einfache Personendaten geht.» Der Begriff «Persönlichkeitsprofile» wird im nDSG zwar nicht mehr verwendet, die Erläuterung ist jedoch weiterhin relevant zum Verständnis, dass die Massnahmen den konkreten Umständen angepasst sein müssen. Dabei handelt es sich um eine Sorgfaltspflicht und der Verantwortliche bzw. der Auftragsbearbeiter muss dafür sorgen, dass die Massnahmen ergriffen werden, und ihre Umsetzung überwachen.

Absatz 2 betrifft die Genehmigung der Standarddatenschutzklauseln durch den EDÖB, die von einer privaten Person oder einem Bundesorgan ausgearbeitet wurden. Der EDÖB gibt eine Stellungnahme ab und veröffentlicht auf seiner Website eine Liste von Standarddatenschutzklauseln, die er genehmigt, ausgestellt oder anerkannt hat. Die Standardklauseln müssen den schweizerischen Datenschutzanforderungen entsprechen und in Übereinstimmung mit dem schweizerischen Datenschutzrecht ausgelegt werden können. Der EDÖB «teilt das Ergebnis der Prüfung der Standarddatenschutzklauseln, die ihm unterbreitet werden, innerhalb von 90 Tagen mit».

Art. 11 Verbindliche unternehmensinterne Datenschutzvorschriften

Verbindliche unternehmensinterne Datenschutzvorschriften gelten für alle Unternehmen, die zum selben Konzern gehören, und müssen von diesen eingehalten werden. Diese Vorschriften müssen nicht nur die in Artikel 9 Absatz 1 DSV genannten Punkte umfassen, sondern

[29] Vgl. Kommentar BJ, 5.2.

auch Angaben zur Organisation und die Kontaktdaten des Konzerns und jeder seiner Einheiten (Abs. 2 Bst. a) sowie Angaben zu den Massnahmen, die innerhalb des Konzerns getroffen wurden, um die Einhaltung der unternehmensinternen Vorschriften zu gewährleisten (Abs. 2 Bst. b).

Diese verbindlichen unternehmensinternen Vorschriften sind gemäss Artikel 16 Absatz 2 Buchstabe e nDSG überdies dem EDÖB vorzulegen.

Artikel 11 DSV umfasst einen neuen Absatz 3, wonach der EDÖB «das Ergebnis der Prüfung der verbindlichen unternehmensinternen Datenschutzvorschriften, die ihm unterbreitet werden, innerhalb von 90 Tagen» mitteilt.

Art. 12 Verhaltenskodizes und Zertifizierungen

Gemäss Artikel 16 Absatz 3 nDSG kann der Bundesrat andere geeignete Garantien vorsehen, welche die Datenbekanntgabe ins Ausland ermöglichen. So lässt sich ein geeigneter Datenschutz auch durch einen Verhaltenskodex oder eine Zertifizierung gewährleisten (Abs. 1).

Mit dieser neuen Massnahme erhalten Unternehmen einen Anreiz, einen solchen Kodex einzuführen oder ihre Systeme, Produkte oder Dienstleistungen zertifizieren zu lassen. Wie bei den Standarddatenschutzklauseln und den verbindlichen unternehmensinternen Vorschriften wird aus Gründen der Kohärenz auch bei den Verhaltenskodizes bestimmt, dass diese vom EDÖB genehmigt werden müssen (Abs. 2). Denn diese Instrumente sind auf ihre Tauglichkeit zu prüfen. Für seine Prüfung kann sich der EDÖB an die Kriterien von Artikel 9 Absatz 1 DSV orientieren. Die Genehmigung der Verhaltenskodizes durch den EDÖB steht nicht im Widerspruch zu Artikel 11 nDSG, der in allgemeiner Weise vorsieht, dass der EDÖB zu den ihm vorgelegten Verhaltenskodizes Stellung nimmt, aber diese nicht genehmigt. Im konkreten Fall, in dem ein Verantwortlicher sich bei der Datenbekanntgabe ins Ausland auf seinen Verhaltenskodex stützt, ist es wie bei den Standarddatenschutzklauseln und den verbindlichen unternehmensinternen Vorschriften angezeigt, dass der EDÖB dieses Instrument genehmigt. Gemäss der Verordnung vom 28. September 2007[30] über die Datenschutzzertifizierungen müssen ausschliesslich ausländische Zertifizierungen vom EDÖB anerkannt werden. Dies wird mit der totalrevidierten Verordnung so aufrechterhalten. Das bedeutet jedoch nicht, dass die Zertifizierung nicht den Anforderungen der Verordnung über die Datenschutzzertifizierungen entsprechen muss.

Zudem muss der Verantwortliche oder der Auftragsbearbeiter, der sich in einem Drittland befindet, die verbindliche und durchsetzbare Verpflichtung eingehen, die im Verhaltenskodex oder in der Zertifizierung enthaltenen Massnahmen anzuwenden (Abs. 3).

Aufhebung von Artikeln 5 und 7 VDSG

Die Artikel 5 und 7 VDSG werden nicht übernommen. Erstere Bestimmung wurde in das nDSG (Art. 18) eingefügt. Die zweite, die dem EDÖB die Kompetenz zuwies, eine Liste der

[30] RS **235.13**

Staaten mit einem angemessenen Datenschutzniveau zu erstellen, ist überholt, weil neu der Bundesrat diese Kompetenz hat (Art. 16 Abs. 1 nDSG).

5.2 2. Kapitel: Pflichten des Verantwortlichen

Art. 13 Modalitäten der Informationspflicht

Die Informationspflicht des Verantwortlichen ist in Artikel 19 nDSG verankert. Ausnahmen und Einschränkungen sind in Artikel 20 nDSG festgelegt. Artikel 19 Absatz 1 nDSG sieht vor, dass die betroffene Person «angemessen» informiert werden muss. Dies bedeutet, dass die Informationen soweit möglich in präziser, transparenter, verständlicher und leicht zugänglicher Form mitgeteilt werden.

Mit anderen Worten muss der Verantwortliche bei der Wahl der Informationsform sicherstellen, dass die betroffene Person bei der Beschaffung ihrer Personendaten die wichtigsten Informationen stets auf der ersten Kommunikationsstufe erhält. Erfolgt die Kommunikation zum Beispiel über eine Internetseite, kann eine gute Praxis darin bestehen, dass alle wesentlichen Informationen auf einen Blick, z. B. in Form einer gegliederten Übersicht verfügbar sind. Um weitere Informationen zu erhalten, kann die betroffene Person danach auf diese zuerst angezeigten Informationen klicken, worauf sich ein Fenster mit detaillierteren Angaben öffnet. Es ist allerdings festzuhalten, dass die Kommunikation über eine Website nicht immer genügt: Die betroffene Person muss wissen, dass sie die Informationen auf einer bestimmten Website findet. Im Fall eines Telefongesprächs können die Informationen auch mündlich mitgeteilt und allenfalls durch einen Link zu einer Website ergänzt werden. Bei aufgezeichneten Informationen muss die betroffene Person die Möglichkeit haben, sich ausführlichere Informationen anzuhören. Für den Fall, dass die Person mit einem Videoüberwachungssystem oder einer Drohne gefilmt wird, muss sie beispielsweise durch ein Hinweisschild oder im Rahmen einer Informationskampagne darauf aufmerksam gemacht werden.

Entsprechend Artikel 19 Absatz 1 nDSG richtet sich Artikel 13 DSV einzig an den Verantwortlichen und nicht an den Auftragsbearbeiter. Es sei jedoch an dieser Stelle darauf hingewiesen, dass die Information des Verantwortlichen gemäss Artikel 19 Absatz 2 Buchstabe c nDSG auch Angaben zu den Empfängerinnen und Empfänger bzw. den Kategorien von Empfängerinnen und Empfängern enthalten muss. Gemäss Ausführungen in der Botschaft zum Datenschutzgesetz gehört auch der Auftragsbearbeiter zu den Empfängerinnen oder Empfänger im Sinne von Artikel 19 Absatz 2 Buchstabe c nDSG (BBl *2017* 6941, 7051). Der Verantwortliche muss daher die betroffene Person bei der Beschaffung von Personendaten auch darüber informieren, dass die Daten an einen Auftragsbearbeiter bekanntgegeben werden.

Art. 14 Aufbewahrung der Datenschutz-Folgenabschätzung

Die Norm konkretisiert die Aufbewahrungsdauer der Datenschutz-Folgenabschätzung im Sinne von Artikel 22 nDSG. Diese ist während mindestens 2 Jahren aufzubewahren. Der Grund für die Aufbewahrung der Datenschutz-Folgenabschätzung über die Vornahme der Datenbearbeitung hinaus besteht darin, dass sie ein zentrales datenschutzrechtliches Instrument darstellt. Sie kann insbesondere bei der Abklärung von Verletzungen der Datensicherheit oder der Beurteilung der Strafbarkeit eines Verhaltens von Bedeutung sein. So gibt die Datenschutz-Folgenabschätzung darüber Auskunft, wie die Risiken für die Persönlichkeit oder die Grundrechte bewertet wurden und welche Massnahmen getroffen wurden. Bei Bundesorganen, die grundsätzlich nur gestützt auf Rechtsgrundlagen Daten bearbeiten können, kann es aufgrund der Beständigkeit gewisser Rechtsgrundlagen vorkommen, dass eine Datenschutz-Folgeabschätzung über einen sehr langen Zeitraum aufzubewahren ist.

Im Falle der Bundesorgane wird weiter zu regeln sein, wie die Datenschutz-Folgenabschätzung zeitlich mit dem Gesetzgebungsverfahren zur Schaffung der Rechtsgrundlagen für die Datenbearbeitung zu koordinieren ist. Es soll vorgesehen werden, dass die Bundesorgane die Datenschutz-Folgenabschätzung zusammen mit den Erlassentwürfen dem Antrag an den Bundesrat beifügen müssen und sie die Resultate der Datenschutz-Folgenabschätzung in der Botschaft des Bundesrats festhalten müssen. Da die Regelung aber nur Weisungscharakter innerhalb der Bundesverwaltung aufweist, ist sie nicht auf Verordnungsstufe zu regeln. Es ist geplant, die Regelung in den Richtlinien für Bundesratsgeschäfte («roter Ordner») und im Botschaftsleitfaden umzusetzen.

Für die Umsetzung der Datenschutz-Folgenabschätzung kann der EDÖB von seiner Kompetenz Gebrauch machen, Arbeitsinstrumente als Empfehlungen der guten Praxis zuhanden von Verantwortlichen im Sinne von Artikel 58 Absatz 1 Buchstabe g nDSG zu erarbeiten. Dabei hat er einen gewissen Ermessensspielraum.

Art. 15 Meldung von Verletzungen der Datensicherheit

Artikel 24 Absatz 2 nDSG enthält die Mindestanforderungen an eine Meldung des Verantwortlichen von Verletzungen der Datensicherheit an den EDÖB: Dazu gehört die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen. Der Inhalt dieser Meldung an den EDÖB wird in Artikel 15 Absatz 1 DSV (ehem. Art. 19 Abs. 1 E-VDSG) weiter präzisiert. Dabei ist zu beachten, dass die Meldung an den EDÖB gemäss Artikel 24 Absatz 1 nDSG auf Verletzungen der Datensicherheit beschränkt ist, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Es müssen nur meldepflichtige Verletzungen gemeldet werden.

Absatz 1 enthält folgenden Katalog an Angaben: Nebst der bereits im Gesetz erwähnten Art der Datensicherheitsverletzung (Bst. a), ist weiter vorgesehen, dass, soweit möglich, auch der Zeitpunkt und die Dauer der Datensicherheitsverletzung mitgeteilt werden muss (Bst. b). Weiter müssen, soweit möglich, auch die Kategorien und die ungefähre Anzahl der Personendaten, die von der Verletzung der Datensicherheit betroffen sind (Bst. c), gemeldet werden, sowie die Kategorien und die ungefähre Anzahl der betroffenen Personen (Bst. d). Diese Informationen sind von grundsätzlicher Bedeutung, damit das Ausmass der Verletzung abgeschätzt werden kann. Dabei ist insbesondere erforderlich, dass bekannt ist, welche Kategorien von Personendaten von der Verletzung betroffen sind (z. B. Adressen, Kreditkartenformationen, Gesundheitsdaten), damit die Ausführungen zu den Folgen, Risiken und Massnahmen überhaupt nachvollziehbar sind. Im Zusammenhang mit der Meldung von Folgen und Risiken für die betroffenen Personen (Bst. e) und den vom Verantwortlichen getroffenen Massnahmen (Bst. f), muss der Verantwortliche bei der Information an die betroffene Person unter anderem auch Ausführungen dazu machen, welche Kategorien von Personendaten in ihrem Fall von der Verletzung betroffen sind. Dies erlaubt es der betroffenen Person konkrete Massnahmen selbst vorzunehmen (z. B. unverzügliche Passwortänderung, falls Anmeldedaten entwendet wurden oder Kreditkartensperre). Schliesslich muss der Verantwortliche den Namen und die Kontaktdaten einer Ansprechperson melden (Bst. g), welche als Anlaufstelle für die Kommunikation mit dem EDÖB als auch den betroffenen Personen fungiert.

Absatz 2 ermöglicht es dem Verantwortlichen, dem EDÖB die Informationen schrittweise zur Verfügung zu stellen, falls es dem Verantwortlichen nicht möglich sein sollte bei Entdeckung der Verletzung der Datensicherheit bereits alle Informationen gemäss Absatz 1 gleichzeitig zu liefern. Da der Verantwortliche die Meldung gemäss Artikel 24 Absatz 1 nDSG «so rasch als möglich» abzusetzen hat, wird in der Praxis insbesondere bei den Informationen nach Absatz

1 Buchstaben b–d regelmässig das Problem auftreten, dass diese unmittelbar nach Entdeckung der Verletzung der Datensicherheit häufig noch gar nicht vorliegen. Daher wird es dem Verantwortlichen ermöglicht, dass er in einem ersten Schritt bei der Entdeckung der Verletzung nur die ihm bekannten Grundangaben liefert. Für die Nachmeldung gilt – wie gemäss Artikel 24 Absatz 1 nDSG –, dass der Verantwortliche die restlichen Angaben «so rasch als möglich» melden muss. Sobald die fehlenden Informationen vorliegen, muss der Verantwortliche diese dem EDÖB mit einer Nachmeldung zur Verfügung stellen. Müssen die Angaben erst noch beschafft werden, so hat er sich ohne Verzögerung darum zu kümmern.

In Absatz 3 wird festgehalten, welche Angaben der betroffenen Person gemacht werden müssen, falls gemäss Artikel 24 Absatz 4 nDSG eine Information an diese zu erfolgen hat. Weiter muss diese Information – im Vergleich zur Meldung an den Beauftragten – in möglichst einfacher und verständlicher Sprache mitgeteilt werden, da nicht vorausgesetzt werden kann, dass einer durchschnittlichen betroffenen Person der Fachjargon dieser technisch geprägten Materie geläufig ist. Die Meldung an den EDÖB ist dabei inhaltlich etwas breiter gefasst als die Information der betroffenen Personen, da sich Ersterer ein Bild über das Ausmass einer Verletzung der Datensicherheit verschaffen können muss.

Absatz 4 sieht vor, dass die mit der gemeldeten Verletzung der Datensicherheit zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen zu dokumentieren sind. Die Unterlagen sind dabei ab dem Zeitpunkt der Meldung der Verletzung der Datensicherheit für mindestens zwei Jahre aufzubewahren.

Im Zusammenhang mit der praktischen Umsetzung der Meldepflicht nach Artikel 24 nDSG ist darauf hinzuweisen, dass aufgrund von Erfahrungen ausländischer Aufsichtsbehörden bei der Umsetzung der ähnlich ausgestalteten Meldepflicht in Artikel 33 der Verordnung (EU) 2016/679 eine grosse Anzahl jährlicher Meldungen zu erwarten ist. So hat der Austausch mit dem Bayerischen Landesamt für Datenschutzaufsicht, dessen Zahlen sich in etwa auf die Schweiz projizieren lassen, ergeben, dass um die 6000 Meldungen pro Jahr eingehen könnten. Damit den Verantwortlichen eine strukturierte Meldemöglichkeit angeboten und die Masse von Meldungen möglichst effizient abgearbeitet werden kann, arbeitet der EDÖB derzeit an der Entwicklung einer webbasierten Meldeoberfläche, voraussichtlich in Form eines interaktiven Formulars. Im Rahmen dieses Projektes prüft der EDÖB derzeit auch die Möglichkeit eines gemeinsamen Meldeportals zusammen mit anderen Bundesorganen, die ähnliche Meldepflichten oder -möglichkeiten im Bereich der Datensicherheit vorsehen (z. B. für die Meldung bei kritischen Infrastrukturen). Mit einem solchen Meldeportal würde sich der Aufwand für den Verantwortlichen reduzieren, falls dieser bei mehreren Bundesstellen Meldungen absetzen muss.

5.3 3. Kapitel: Rechte der betroffenen Person

Das Kapitel zu den Rechten der betroffenen Person beinhaltete im E-DSG nur das Auskunftsrecht und dessen Einschränkungen. Das Parlament hat ein Recht auf Datenherausgabe und -übertragung hinzugefügt. Dementsprechend werden in der Verordnung diese beiden Arten von Rechten der betroffenen Person in getrennten Abschnitten präzisiert.

Der 1. Abschnitt behandelt das Auskunftsrecht. Nach Absprache mit dem Eidgenössischen Departement für auswärtige Angelegenheiten und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport wurde der Inhalt von Artikel 14 VDSG nicht in die DSV übernommen, weil er nicht mehr aktuell ist. Deshalb wird nun das Auskunftsrecht für beide Sektoren, den privaten und den öffentlichen, im gleichen Kapitel geregelt. Dieses folgt der Systematik des nDSG und schliesst an die Bestimmungen zu den Pflichten des Verantwortlichen an.

Die verschiedenen Aspekte des Auskunftsrechts verteilen sich neu auf mehrere Artikel. Ein erster Artikel konzentriert sich auf die Modalitäten des Auskunftsrechts, insbesondere die Form der Auskunftserteilung. Ein zweiter Artikel regelt das Auskunftsrecht, wenn mehrere Verantwortliche gemeinsam Personendaten bearbeiten oder wenn Daten von einem Auftragsbearbeiter bearbeitet werden. Ein dritter Artikel legt die Fristen fest, und ein vierter Artikel regelt die Ausnahmen von der Kostenlosigkeit des Auskunftsrechts.

Der 2. Abschnitt behandelt das Recht auf Datenherausgabe oder -übertragung. Er umfasst folgende Artikel: Artikel 20 DSV behandelt den Umfang des Anspruchs, Artikel 21 DSV die technischen Anforderungen an die Umsetzung und Artikel 22 DSV (ehem. Art. 24 E-VDSG) führt unter Frist, Modalitäten und Zuständigkeit aus, inwiefern die Bestimmungen zum Auskunftsrecht auf das Recht auf Datenherausgabe oder -übertragung anwendbar sind.

5.3.1 1. Abschnitt: Auskunftsrecht

Art. 16 Modalitäten

Diese Bestimmung konkretisiert die in Artikel 25 nDSG vorgesehenen Modalitäten des Auskunftsrechts. Sie übernimmt teilweise Artikel 8 Absatz 5 DSG sowie Artikel 1 Absätze 1–3 VDSG.

Abs. 1

Artikel 16 DSV (ehem. Art. 20 E-VDSG) konzentriert sich in Absatz 1 auf die Form des Auskunftsbegehrens. «Schriftlich» im Sinne von Artikel 16 Absatz 1 DSV umfasst jegliche Formen, die den Nachweis durch Text ermöglichen. Nicht gemeint ist hingegen die sogenannte einfache Schriftlichkeit nach den Artikeln 13–15 des Obligationenrechts[31]. Diese setzt eine Handunterschrift oder eine mit einem qualifizierten Zeitstempel verbundene qualifizierte elektronische Signatur gemäss Bundesgesetz vom 18. März 2016[32] über die elektronische Signatur voraus. Artikel 16 Absatz 1 DSV verlangt hingegen einzig das Vorliegen eines geschriebenen Textes. Art. 16 Abs. 1 DSV übernimmt im Wesentlichen den Inhalt von Artikel 1 Absatz 1 VDSG, gemäss dem die Person ihr Auskunftsrecht «in der Regel in schriftlicher Form beantragen» muss. Im Kommentar zur VDSG des Bundesamtes für Justiz[33] wird bereits präzisiert, dass in bestimmten Fällen und unter Vorbehalt des Einverständnisses des Inhabers der Datensammlung (neu des Verantwortlichen) die mündliche Form genügt. Der erhöhten Klarheit halber wurde Artikel 16 DSV entsprechend umformuliert. Ausserdem wurde Artikel 1 Absatz 1 VDSG in redaktioneller Hinsicht angepasst.

Abs. 2

Im Vergleich zum geltenden Recht legt Artikel 16 Absatz 2 DSV (ehem. Art. 20 Abs. 2 E-VDSG) neu explizit fest, dass die Auskunftserteilung nebst der Schriftform auch in der Form erfolgen kann, in der die Daten vorliegen. In der Regel handelt es sich um Personendaten in Schriftform. Liegen die Daten hingegen z. B. in Form von Bild- oder Tonaufnahmen vor, so erhält die betroffene Person die Daten in dieser Form. Wie oben ausgeführt, ist «schriftlich» im vorliegenden Kontext so zu verstehen, dass das Vorliegen eines geschriebenen Textes verlangt wird.

---

[31] SR **220**

[32] SR **943.03**

[33] Vgl. Kommentar BJ, 3.1.

Wie in Artikel 1 Absatz 3 VDSG vorgesehen, können Personendaten auch an Ort und Stelle eingesehen werden, insbesondere, wenn sie auf verschiedene Dossiers verteilt oder besonders umfangreich sind oder wenn die verlangten Auskünfte der Erläuterung bedürfen. Im Unterschied zu Artikel 1 Absatz 3 VDSG wurde der Passus, wonach die Einsichtnahme vor Ort auf Vorschlag des Verantwortlichen erfolgt, gestrichen. Für die Einsichtnahme vor Ort ist stets erforderlich, dass der Verantwortliche und die betroffene Person einverstanden sind. Auf wessen Vorschlag hin die Einsichtnahme vor Ort erfolgt, ist hingegen nicht massgeblich. Bei der Einsichtnahme an Ort und Stelle muss die betroffene Person gleichwohl die Möglichkeit haben, eine Fotokopie bestimmter Akten in ihrem Dossier zu verlangen. Wie das Bundesgericht in BGE 119 III 141 festgestellt hat, kann die Aushändigung schriftlicher (inkl. elektronischer) Dokumente für die betroffene Person äusserst bedeutsam sein. Die mündliche Mitteilung von Informationen, zum Beispiel am Telefon, ist ebenfalls möglich, sofern die betroffene Person eingewilligt hat. Eine Auskunft in zusammengefasster («aggregierter») Form ist nicht erlaubt.

Abs. 3

Absatz 3 übernimmt Artikel 1 Absatz 2 VDSG in angepasster Form. Er regelt namentlich die Form der Übermittlung des Auskunftsbegehrens und der Auskunftserteilung. So können das Auskunftsbegehren und die Auskunftserteilung auch auf elektronischem Weg erfolgen. Die betroffene Person kann ihr Gesuch beispielsweise mittels E-Mail oder über eine Online-Plattform eines Unternehmens (z. B. die verbreiteten Kundenkontos) einreichen. Die Absenderin oder der Absender trägt nach den allgemeinen Regeln die Beweislast dafür, dass ihre bzw. seine Botschaft die Empfängerin oder den Empfänger erreicht hat. Da die elektronische Übermittlung auch ohne gesetzliche Grundlage zulässig ist, handelt es sich bei Absatz 3 um eine deklaratorische Bestimmung.

Abs. 4

Werden Personendaten in einer technischen Form, also beispielsweise in einem nicht üblichen Dateienformat, geliefert, die für die betroffene Person nicht lesbar und/oder nicht verständlich ist, muss der Verantwortliche imstande sein, ihr ergänzende Erläuterungen zu geben, beispielsweise mündlich.

Abs. 5

Der Verantwortliche muss angemessene Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen. Diese muss deshalb bei ihrer Identifizierung mitwirken. Damit der Verantwortliche die Identifizierung der betroffenen Person sicherstellen kann, braucht er die nötigen Angaben von der betroffenen Person. Im Fall einer mündlichen Auskunft stellt der Verantwortliche vorfrageweise sicher (z. B. durch Angabe der AHV-Nr.), dass er die Auskunft der korrekten Person erteilt. Artikel 16 Absatz 5 DSV (ehem. Art. 20 Abs. 4 E-VDSG) ersetzt die Anforderung gemäss Artikel 1 Absatz 1 VDSG, wonach die betroffene Person sich über ihre Identität ausweisen muss.

Weitere Aspekte

Absatz 4 von Artikel 1 VDSG, der die Frist für die Auskunftserteilung betrifft, wird in einen eigenständigen Artikel umgewandelt (siehe Art. 18 DSV, ehem. Art. 22 E-VDSG unten). Dasselbe gilt für Artikel 1 Absätze 5 und 6 VDSG (siehe Art. 17 DSV, ehem. Art. 21 E-VDSG unten).

Art. 17 Zuständigkeit

Zur Präzisierung der Zuständigkeit in den Fällen, in denen mehreren Verantwortlichen gemeinsam Personendaten bearbeiten, wurde ein separater Artikel vorgesehen.

Abs. 1

Absatz 1 übernimmt Absatz 5 von Artikel 1 VDSG in angepasster Form. In terminologischer Hinsicht wurde der Begriff «Inhaber der Datensammlung» durch «Verantwortlicher» ersetzt. Die Ausnahme von der Möglichkeit, bei jedem Verantwortlichen das Auskunftsrecht geltend zu machen, wurde aufgehoben. Somit kann die betroffene Person nun ihr Auskunftsrecht immer bei jedem Verantwortlichen geltend machen. Im Unterschied zu Artikel 1 Absatz 5 VDSG verpflichtet Artikel 17 Absatz 1 DSV die Verantwortlichen nicht mehr dazu, die Gesuche weiterzuleiten; vielmehr müssen sie in jedem Fall Auskunft erteilen. Der Absatz entspricht Artikel 21 Absatz 2 der Richtlinie (EU) 2016/680 sowie Artikel 26 Absatz 3 DSGVO.

Abs. 2

Absatz 2 übernimmt Artikel 1 Absatz 6 VDSG in angepasster Form. Der im nDSG (Art. 5 Bst. k nDSG) eingeführte Begriff «Auftragsbearbeiter» wird übernommen und der Begriff «Inhaber der Datensammlung» durch «Verantwortlicher» ersetzt. Gemäss Artikel 25 Absatz 4 nDSG bleibt der Verantwortliche auskunftspflichtig, auch wenn er die Personendaten von einem Auftragsbearbeiter bearbeiten lässt. Der Auftragsbearbeiter ist daher von Gesetzes wegen nicht verpflichtet, Auskunftsbegehren selbst zu beantworten. In Artikel 17 Absatz 2 DSV wird deshalb im Unterschied zur VDSG neu vorgesehen, dass der Auftragsbearbeiter den Verantwortlichen bei der Beantwortung unterstützt, sofern er das Begehren nicht im Auftrag des Verantwortlichen beantwortet. Dies heisst, dass der Auftragsbearbeiter dem Verantwortlichen die Daten liefern muss, wenn dieser nicht selbst darüber verfügt.

Art. 18 Frist

Artikel 18 DSV (ehem. Art. 22 E-VDSG) übernimmt ohne wesentliche Änderung den vierten Absatz von Artikel 1 VDSG. Er präzisiert den vom Parlament in Artikel 25 nDSG eingefügten Absatz 7, der die bis anhin in der Verordnung vorgesehene Frist von 30 Tagen auf Gesetzesstufe festlegt. Die Präzisierung, wonach der Entscheid über die Beschränkung des Auskunftsrechts begründet werden muss, wurde gestrichen, da diese Bestimmung bereits in Artikel 26 Absatz 4 nDSG aufgenommen wurde. Ferner wird der Begriff «Gesuchsteller» durch «betroffene Person» ersetzt, damit die Terminologie mit dem nDSG übereinstimmt.

Im Wesentlichen bedeutet die Bestimmung, dass der Verantwortliche der betroffenen Person die verlangte Auskunft innerhalb von 30 Tagen erteilen oder ihr innert dieser Frist mitteilen muss, dass er die Auskunft verweigert, einschränkt oder aufschiebt. Im öffentlichen Bereich

handelt es bei der Auskunftserteilung sowie der Verweigerung, Einschränkung oder Aufschiebung der Auskunft um eine Verfügung im Sinne von Artikel 5 VwVG[34]. Absatz 2 ist nur anwendbar, wenn der Verantwortliche nicht in der Lage ist, die Auskunft innert 30 Tagen seit Eingang des Begehrens zu erteilen (und nicht im Fall, in dem er das Auskunftsrecht im Sinne von Art. 26 nDSG einschränkt): In dem Fall muss der Verantwortliche rechtzeitig, also ohne unangemessene Verzögerung die Frist mitteilen, in der die Auskunft erfolgen wird.

Art. 19 Ausnahme von der Kostenlosigkeit

Der Titel der Bestimmung wird im Vergleich zu Artikel 2 VDSG redaktionell geändert.

Abs. 1

Artikel 2 Absatz 1 Buchstabe a VDSG, der querulatorische Auskunftsgesuche betrifft, wird aufgehoben. Solche Fälle werden neu im nDSG geregelt, das in Artikel 26 Absatz 1 Buchstabe c vorsieht, dass der Verantwortliche die Auskunft verweigern, einschränken oder aufschieben kann, wenn das Auskunftsgesuch offensichtlich querulatorisch ist.

Artikel 2 Absatz 1 Buchstabe b sowie Absatz 2 VDSG werden in leicht angepasster Form übernommen. Der Ausdruck «ausnahmsweise» wird gestrichen, da in der Sachüberschrift des Artikels bereits von «Ausnahme» die Rede ist; der Begriff «Gesuchsteller» (neuer Abs. 3) wird aus Gründen der terminologischen Übereinstimmung mit dem nDSG durch «betroffene Person» ersetzt. Der Ausdruck «besonders grosser Arbeitsaufwand» wird durch «unverhältnismässiger Aufwand» ersetzt, damit die Formulierung mit den vom Nationalrat in Artikel 25 Absatz 6 nDSG vorgenommenen Änderungen übereinstimmt. Es stellt zum Beispiel keinen unverhältnismässigen Aufwand dar, wenn der Verantwortliche Zugang zu zahlreichen Personendaten gewähren muss, wenn sein Interesse gerade darin besteht, möglichst viele Daten zu sammeln. Dasselbe gilt, wenn der Arbeitsaufwand gross ist, weil der Verantwortliche nicht strukturiert genug organisiert ist (Missachtung des Grundsatzes «Privacy by Design»; denn gemäss diesem Grundsatz müssen die Verantwortlichen oder Auftragsbearbeiter über ein System verfügen, das einen einfachen Zugang zu den bearbeiteten Daten ermöglicht).

Abs. 2

Der Betrag von 300 Franken bleibt unverändert. Gemäss dem Landesindex der Konsumentenpreise hat sich der Betrag seit seiner Einführung in der Verordnung nur geringfügig verändert. Zudem soll er auf die betroffene Person nicht abschreckend wirken.

Abs. 3

Der Verantwortliche muss der betroffenen Person die Höhe der Beteiligung vor der Auskunftserteilung mitteilen. Bestätigt die Gesuchstellerin oder der Gesuchsteller das Gesuch nicht innerhalb von zehn Tagen, so gilt es als ohne Kostenfolge zurückgezogen. Die Frist nach Artikel 18 Absatz 1 DSV (ehem. Art. 22 Abs. 1 E-VDSG) beginnt nach Ablauf der 10 Tage Bedenkzeit zu laufen.

5.3.2 2. Abschnitt: Recht auf Datenherausgabe oder -übertragung

Diese Artikel präzisieren, welche verschiedenen Anforderungen für das Recht auf Datenherausgabe oder -übertragung, wie es in Artikel 28 nDSG eingeführt wird, gelten. Vor dem

[34] SR **172.021**

Hintergrund, dass es das Ziel des Gesetzgebers war, eine ähnliche Regelung wie im europäischen Recht zu schaffen, werden dabei die in Artikel 20 DSGVO zum Recht auf Datenübertragbarkeit geltenden Regeln berücksichtigt.

Mit dem Anspruch auf Datenherausgabe oder -übertragung erhalten die betroffenen Personen einerseits das Recht, unter bestimmten Voraussetzungen, ihre Personendaten, welche sie dem Verantwortlichen zur Verfügung gestellt haben, in weiterverwendbarer Form von diesem heraus zu verlangen.

Die herausverlangten Personendaten können für verschiedene Zwecke verwendet werden: beispielsweise für den rein persönlichen Gebrauch (z. B. um die Daten auf einem persönlichen Speicherplatz zu speichern), um sie an einen anderen Onlinedienste-Anbieter weiterzuleiten oder um die Plattform zu wechseln.

Mit dem Anspruch, die Übertragung ihrer Personendaten zu verlangen, erhalten die betroffenen Personen andererseits das Recht, den Verantwortlichen zu ersuchen, dass er diese Personendaten direkt einem anderen Verantwortlichen überträgt (z. B. damit ein neuer Onlinedienste-Anbieter diese Personendaten erweitern oder der betroffenen Person neue Dienste anbieten kann oder um bei einem Anbieterwechsel die eigene «Historie» beizubehalten), sofern dies keinen unverhältnismässigen Aufwand erfordert.

Das Recht auf Datenherausgabe oder -übertragung ist vom Auskunftsrecht nach Artikel 25 nDSG zu unterscheiden. Das Auskunftsrecht berechtigt die betroffene Person, vom Verantwortlichen darüber Auskunft zu verlangen, welche Personendaten dieser über sie bearbeitet. Dies ermöglicht es der betroffenen Person, im Falle einer widerrechtlichen Datenbearbeitung, die Berichtigung oder Löschung ihrer Personendaten zu verlangen.

Dahingegen bezweckt der neue Anspruch auf Datenherausgabe oder -übertragung, die Kontrolle der betroffenen Personen über ihre Personendaten sowie über deren Weiterverwendung zu stärken. Er erlaubt ihr damit, selber über die herausgegebenen oder übertragenen Personendaten zu verfügen, diese weiterzuverwenden oder an andere Verantwortliche weiterzugeben. Daneben erleichtert es dieser neue Anspruch den betroffenen Personen auch, zwischen verschiedenen Angeboten zu wechseln, wodurch zudem Wettbewerb und Innovation gefördert werden.

Für die Verantwortlichen begründet dieser neue Anspruch die Pflicht, die herausverlangten Personendaten binnen vernünftiger Zeit aggregiert zur Verfügung zu stellen und zu ermöglichen, dass sie ohne unverhältnismässigen Aufwand in ein neues System eingebettet werden können. Dafür ist notwendig, dass sie gängige Dateiformate verwenden und gängige, standardisierte Datenverwaltungssysteme implementieren, damit die Daten weiterverwendbar bleiben.

Sowohl bei der Herausgabe der herausverlangten Personendaten sowie bei deren Übertragung haben die Verantwortlichen die datenschutzrechtlichen Grundsätze sowie ihre datenschutzrechtlichen Pflichten zu berücksichtigen.

Art. 20 Umfang des Anspruchs

Abs. 1

Diese Bestimmung präzisiert, welche Personendaten unter den Anspruch auf Datenherausgabe oder -übertragung fallen. Der Anspruch umfasst Personendaten, die die betroffene

Person selbst betreffen sowie automatisiert und auf Grundlage einer Einwilligung oder im Zusammenhang mit einem Vertrag bearbeitet werden (Art. 28 Abs. 1 nDSG).

In erster Linie sind vom Anspruch damit Personendaten ausgeschlossen, welche in Papierform aufbewahrt werden.

Keine Anwendung findet der Anspruch sodann auf Verantwortliche, welche Personendaten in Erfüllung einer öffentlichen Aufgabe oder in einem öffentlichen Interesse bearbeiten. Dies entspricht der Regelung von Artikel 20 Absatz 3 DSGVO sowie dem primär wirtschaftlichen Zweck des Anspruchs auf Datenherausgabe oder -übertragung. Bundesorgane, welche im Rahmen ihrer gesetzlichen Aufgaben sowie gestützt auf eine gesetzliche Grundlage Personendaten bearbeiten, sind deshalb grundsätzlich nicht vom Anspruch auf Datenherausgabe oder -übertragung betroffen. Sofern Bundesorgane allerdings Personendaten beispielsweise im Wettbewerb mit Privaten bearbeiten, ist denkbar, dass diese Personendaten vom Anspruch umfasst werden. Auf jeden Fall ist es am Verantwortlichen zu prüfen, auf welche Personendaten, die dieser bearbeitet, der Anspruch Anwendung finden könnte und welche davon ausgenommen sind.

Nicht vom Anspruch umfasst sind des Weiteren anonymisierte Personendaten oder solche, welche die betroffene Person nicht betreffen. Pseudonymisierte Personendaten, die eindeutig mit der betroffenen Person in Zusammenhang gebracht werden können, sind hingegen von Artikel 20 Absatz 1 DSV erfasst. In der Praxis dürften in vielen Fällen auch Informationen betroffen sein, welche die Personendaten von mehreren Personen umfassen, wie z. B. der Kontoverlauf einer Kundin oder eines Kunden oder Daten zu Telefongesprächen oder Nachrichten, welche Angaben über Dritte enthalten. Im Rahmen einer Anfrage um Herausgabe oder Übertragung von Personendaten sollten der Gesuchstellerin oder dem Gesuchsteller auch diese Aufzeichnungen bereitgestellt werden. Die Personendaten von Dritten dürfen jedoch nicht für Zwecke bearbeitet werden, welche deren Rechte und Freiheiten beeinträchtigen. Dies wäre der Fall, wenn der neue Verantwortliche die übermittelten Personendaten von Dritten für seine eigene Zwecke verwendet, beispielsweise, um diesen die eigenen Dienste anzubieten. Keine Beeinträchtigung würde hingegen vorliegen, wenn bei einer Übermittlung von Kontoinformationen auf ein neues Bankkonto auf Anlass des Kontoinhabers, die Kontaktadresse im Kontoverlauf seines Bankkontos, weiterhin für denselben Zweck, d.h. als Kontaktadresse und für seinen persönlichen Gebrauch verwendet wird.

Weiter fallen unter Artikel 20 Absatz 1 DSV nur diejenigen Personendaten, welche die betroffene Person einem Verantwortlichen aktiv zur Verfügung stellt. Dies betrifft gemäss Buchstabe a zum einen Personendaten, welche sie dem Verantwortlichen *direkt* und bewusst angibt, wie z. B. ihre Kontaktdaten über ein Online-Formular oder durch die Tätigung von «Likes». Gemäss Buchstabe b umfasst der Anspruch zum anderen auch Personendaten, welche die betroffene Person *indirekt*, das heisst durch ihre Aktivitäten bei der Nutzung eines Dienstes oder eines Gerätes (wissentlich oder unwissentlich) erzeugt und die vom Verantwortlichen beobachtet werden (sogenannte Nutzungsdaten oder «beobachtete» Daten, wie z. B. Suchabfragen, Aktivitäten-Protokolle, Verlauf einer Website-Nutzung).

Dass diese Personendaten vom Anspruch auf Herausgabe und Übertragung umfasst sind, entspricht der europäischen Regelung sowie dem Sinn und Zweck der Norm in Artikel 28 nDSG, wonach die betroffene Person die von ihr einem Verantwortlichen zur Verfügung gestellten Personendaten herausverlangen und weiterverwenden können soll.

Abs. 2

Absatz 2 beschreibt, welche Personendaten nicht als von der betroffenen Person im Sinne von Artikel 28 Absatz 1 nDSG bekanntgegebene Personendaten anzusehen sind. Damit präzisiert diese Regelung den Geltungsbereich des Anspruchs auf Datenherausgabe oder -übertragung. Nicht vom Anspruch umfasst sind demnach Personendaten, welche ein Verantwortlicher aus Rückschlüssen aus den durch die betroffene Person im Sinne von Artikel 20 Absatz 1 Buchstaben a und b bereitgestellten oder beobachteten Personendaten selber ableitet oder durch eigene Analysen dieser Personendaten erzeugt. Zu denken ist beispielsweise an die Bewertung des Gesundheitszustands eines Nutzers, Nutzer- oder Risikoprofile, Kreditrisikoanalysen etc. Im Unterschied zu den bereitgestellten Personendaten beziehen sich hier die Leistungen und Investitionen des Verantwortlichen auf die Analyse und Auswertung der bereitgestellten Daten und nicht auf das Sammeln und Bearbeiten der Personendaten.

Die Ausnahme dieser Personendaten vom Anspruch auf Datenherausgabe oder -übertragung entspricht der Regelung im europäischen Recht. Da es Ziel dieses Anspruchs ist, der betroffenen Person eine Weiterverwendung ihrer Personendaten zu ermöglichen, erscheint es gerechtfertigt, eine Ausnahme für solche Personendaten vorzusehen, welche ein Verantwortlicher durch Auswertung und Einsatz eigener Ressourcen (Eigenleistungen, Eigen-Investition, firmeninterne Algorithmen und Analyseverfahren) erzeugt. Im Unterschied zu den durch die betroffene Person «bereitgestellten Personendaten» gemäss Absatz 1, ist bei diesen durch den Verantwortlichen erzeugten Personendaten, dessen Interesse am Schutz seiner Eigenleistung und eigenen Investition höher zu gewichten. Solche Personendaten fallen daher nicht in den Geltungsbereich des Anspruchs auf Datenherausgabe oder -übertragung.

Im Rahmen des Auskunftsrechts nach Artikel 25 nDSG und der dazugehörigen Verordnungsbestimmungen (Art. 16–19 DSV) hat die betroffene Person jedoch die Möglichkeit, Auskunft vom Verantwortlichen über diese Personendaten, ihren Bearbeitungszweck, ihre Aufbewahrungsdauer sowie bei Vorliegen automatisierter Einzelentscheidungen, über die Logik, auf der diese Entscheidung beruht, zu erhalten.

Wichtig festzuhalten ist, dass die Regelung in Artikel 20 Absatz 2 nicht als eine Einschränkung vom in Artikel 28 nDSG eingeführten Anspruch auf Datenherausgabe oder -übertragung zu verstehen ist, sondern der Auslegung der gesetzlichen Bestimmung dient, indem sie den Geltungsbereich des Anspruchs präzisiert.

Vielmehr gelten aufgrund des Verweises in Artikel 29 Absatz 1 nDSG auf Artikel 26 Absatz 1 und 2 nDSG die für die Einschränkung des Auskunftsrechts vorgesehenen Gründe sinngemäss ebenso für die Verweigerung, Einschränkung oder den Aufschub einer Herausgabe oder Übertragung der Personendaten, beispielsweise zum Schutz überwiegender Interessen des Verantwortlichen (z. B. bei Geschäftsgeheimnissen oder geistigem Eigentum) oder zum Schutz von überwiegender Interessen Dritter. Dies sollte jedoch nicht dazu führen, dass der betroffenen Person jegliche Informationsweitergabe verweigert wird. Vielmehr muss im Rahmen einer Verhältnismässigkeitsprüfung und Interessenabwägung im Einzelfall bestimmt werden, ob und welche Personendaten an die betroffene Person herauszugeben oder auf einen anderen Verantwortlichen zu übertragen sind.

Verweigert oder beschränkt der Verantwortliche die Herausgabe oder Übertragung von Personendaten oder schiebt diese auf, ist er gemäss Artikel 29 Absatz 2 nDSG der betroffenen Person gegenüber zur Begründung verpflichtet.

Art. 21 Technische Anforderungen an die Umsetzung

Abs. 1

Diese Bestimmung präzisiert, was als gängiges elektronisches Format im Sinne von Artikel 28 Absatz 1 nDSG anzusehen ist. Dies sind namentlich solche Formate, die es ermöglichen, dass die Personendaten mit einem verhältnismässigen Aufwand übertragen und von der betroffenen Person oder einem anderen Verantwortlichen weiterverwendet werden können.

Sofern Personendaten nicht in einem allgemein lesbaren Format vorliegen (insbesondere bei proprietären oder wenig gebräuchlichen Formaten), müssen sie vom Verantwortlichen in ein gängiges elektronisches Format überführt werden. Die Datenformate sollten es der betroffenen Person ermöglichen, ihre Daten in einem computerlesbaren Standardformat direkt von ihrem persönlichen Konto oder Bereich hochzuladen. Es sind daher Datenformate zu wählen, die für die Art der betreffenden Daten geeignet sind. Zu bevorzugen sind offene und interoperable Formate wie z. B. XML und JSON für umfangreichere Lösungen, sowie CSV, ODT, ODS usw., welche in vielen Fällen für die Datenherausgabe und -übertragung geeignet sind, da sie ohne nennenswerte Kompatibilitätsprobleme von anderen Verantwortlichen übernommen werden können. Daten, die in einem schwer zu verarbeitenden Format (z. B. ein Bild oder PDF) oder einem proprietären Format geliefert werden, dessen Nutzung den Erwerb einer Software oder einer kostenpflichtigen Lizenz voraussetzt, stellen a priori kein geeignetes Format dar.

Des Weiteren sollte der Inhalt der übermittelten Informationen mit geeigneten und verständlichen Metadaten genau beschrieben werden, damit sie sinnvoll in ein neues System übernommen werden können. Die betroffenen Personen und die Verantwortlichen, welche die Daten im Rahmen einer Datenübertragung übernehmen, müssen verstehen, um welche Art von Daten es sich handelt. Diese Metadaten sollten umfangreich genug sein, um die Nutzung und Wiederverwendung der Daten zu ermöglichen, ohne Geschäftsgeheimnisse offenzulegen.

Abs. 2

Entsprechend dem europäischen Recht präzisiert diese Bestimmung, dass das Recht der betroffenen Person, sie betreffende Personendaten vom Verantwortlichen heraus zu verlangen oder durch diesen an einen anderen Verantwortlichen übertragen zu lassen, für den Verantwortlichen nicht die Pflicht begründet, technisch kompatible Datenbearbeitungssysteme zu übernehmen oder beizubehalten.

Obwohl die Einführung von Standards für Datenformate grundsätzlich möglich wäre, dürfte sich das jeweils am besten geeignete Format je nach Branche und Sektor unterscheiden. Daher erscheint ausreichend, die Verwendung gängiger Formate vorzusehen, ohne diese Formate näher oder gar abschliessend zu spezifizieren. Aus technischer Sicht ist erforderlich, dass die Verantwortlichen die Voraussetzungen schaffen, um Personendaten austauschen zu können. Zudem müssen die ausgetauschten Personendaten durch die betroffene Person oder den neuen Verantwortlichen genutzt werden können. Dazu haben die Verantwortlichen die Personendaten in interoperablen Formaten zur Verfügung zu stellen und diese mit geeigneten Metadaten für die betroffene Person und den neuen Verantwortlichen verständlich zu beschreiben, um ihre Weiterverwendung zu ermöglichen.

Abs. 3

Absatz 3 präzisiert, wann im Sinne von Artikel 28 Absatz 3 nDSG eine Übertragung einen unverhältnismässigen Aufwand erfordert und der Verantwortliche nicht verpflichtet ist, Personendaten auf Verlangen der betroffenen Person an einen anderen Verantwortlichen zu übertragen. Wiederum im Einklang mit dem europäischen Recht ist von einem verhältnismässigen Aufwand für eine Übertragung auszugehen, wenn diese technisch möglich und machbar ist.

Der Verantwortliche ist demnach verpflichtet, die Personendaten auf Verlangen der betroffenen Person direkt und in einem interoperablen Format an einen anderen Verantwortlichen zu übermitteln. Selbst wenn der andere Verantwortliche dieses Format nicht unterstützt, kann eine direkte Datenübertragung auch erfolgen, wenn die Kommunikation zwischen zwei Systemen auf gesicherte Weise möglich ist und das empfangende System technisch in der Lage ist, die eingehenden Daten zu empfangen. Ob eine Übertragung technisch machbar ist, ist von Fall zu Fall zu überprüfen. Denkbar wäre auch, dass der Verantwortliche eine sichere Anwendungsprogramm-Schnittstellen (API) zur Verfügung stellt, um dem anderen Verantwortlichen zu ermöglichen, die Personendaten automatisch abzurufen. Ist eine direkte Datenübertragung wegen technischer Hindernisse jedoch nicht möglich, muss der Verantwortliche die betroffene Person über diese Hindernisse informieren (Art. 29 Abs. 2 nDSG).

Der Verantwortliche darf die Übermittlung der Personendaten jedoch nicht ungerechtfertigt behindern, indem er technische Hürden vorsieht, welche den Datenzugriff, die Datenübertragung oder die Datenwiederverwendung durch die betroffene Person oder einen anderen Verantwortlichen verlangsamt oder verhindert. Dies wäre beispielsweise der Fall, wenn keine Dateninteroperabilität geboten wird bzw. kein Zugriff auf ein Datenformat, keine Programmierschnittstelle oder nicht das bereitgestellte Format angeboten wird, wenn übermässige Verzögerungen auftreten oder die Abfrage des vollständigen Datensatzes zu kompliziert ist, wenn Daten absichtlich verschleiert werden, oder wenn spezifische oder nicht gerechtfertigte Sektor-spezifische Normungs- oder Akkreditierungsanforderungen aufgestellt werden.

Art. 22 Frist, Modalitäten und Zuständigkeiten

Was die Modalitäten des Rechts auf Datenherausgabe oder -übertragung betrifft, sind verschiedene Bestimmungen zum Auskunftsrecht sinngemäss anwendbar. Das betrifft die Form, in der die betroffene Person die Herausgabe oder Übertragung ihrer Personendaten verlangen kann (Art. 16 Abs. 1 DSV, ehem. Art. 20 Abs. 1 E-VDSG), sowie die angemessenen Massnahmen, die getroffen werden müssen, um die Identifizierung der betroffenen Person sicherzustellen (Art. 16 Abs. 5 DSV, ehem. Art. 20 Abs. 4 E-VDSG).

Sinngemäss anwendbar sind auch die Bestimmungen zur Regelung der Zuständigkeiten bei Auskunftsgesuchen bei mehreren Verantwortlichen (Art. 17 Abs. 1 DSV, ehem. Art. 21 Abs. 1 E-VDSG), oder bei Datenbearbeitungen durch einen Auftragsbearbeiter (Art. 17 Abs. 2 DSV, ehem. Art. 21 Abs. 2 E-VDSG). Anzumerken ist, dass auch Personendaten, die durch Auftragsbearbeiter bearbeitet werden, dem Anspruch auf Datenherausgabe oder -übertragung unterliegen. In diesem Fall obliegt es dem Verantwortlichen, die technischen und organisatorischen Lösungen zu schaffen, mit denen dieses Recht durchgesetzt werden kann. Der Auftragsbearbeiter muss den Verantwortlichen bei der Erfüllung seiner Pflichten in Bezug auf das Recht auf Datenherausgabe oder -übertragung unterstützen (Art. 17 Abs. 2 DSV, ehem. Art. 21 Abs. 2 E-VDSG).

Schliesslich sind auch die Bestimmungen zu den Fristen (Art. 18 DSV, ehem. Art. 22 E-VDSG) und den Ausnahmen von der Kostenlosigkeit (Art. 19 DSV, ehem. Art. 23 E-

VDSG) bei Auskunftsgesuchen sinngemäss auf das Recht auf Datenherausgabe oder -übertragung anwendbar.

5.4 4. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Art. 23 Datenschutzberaterin oder Datenschutzberater

In Artikel 10 Absatz 2 nDSG werden in nicht abschliessender Weise zwei Aufgabenbereiche der Datenschutzberaterin oder des Datenschutzberaters eines privaten Verantwortlichen geregelt: Sie oder er schult und berät den privaten Verantwortlichen in Fragen des Datenschutzes (Bst. a) und wirkt beim Vollzug der Datenschutzvorschriften mit (Bst. b). Da sich diese Aufgabenbereiche genügend konkret aus dem Gesetz ergeben, werden sie entgegen dem Vernehmlassungsentwurf zukünftig nicht nochmals in der Verordnung definiert.

Bst. a und b

Diese Bestimmungen entsprechen inhaltlich Artikel 12*b* Absatz 2 Buchstaben b und c VDSG.

Die Aufzählung, zu welchen Dokumenten die Datenschutzberaterin oder der Datenschutzberater Zugang haben muss, wurde der Terminologie im nDSG angepasst. Der Zugang ist dabei nicht uneingeschränkt, sondern es ist nur Zugang zu denjenigen Unterlagen zu geben, welche die Datenschutzberaterin oder der Datenschutzberater auch tatsächlich zur Aufgabenerfüllung benötigt. So ist insbesondere der Zugang zu Personendaten nur dann zu gewähren, wenn diese zur Aufgabenerfüllung benötigt werden. Prüft die Datenschutzberaterin oder der Datenschutzberater beispielsweise in genereller Weise die internen Datenschutzvorschriften oder Prozesse zur Datenbearbeitung, wird sie oder er in der Regel keine Personendaten einsehen können müssen.

Artikel 12*b* Absatz 2 Buchstabe a VDSG wird dagegen nicht übernommen, weil die darin genannte Anforderung neu im Gesetz vorgesehen ist (Art. 10 Abs. 3 Bst a nDSG).

Bst. c

Der Verantwortliche muss der Datenschutzberaterin oder dem Datenschutzberater das Recht einräumen, in wichtigen Fällen das oberste Leitungs- oder Verwaltungsorgan zu informieren. Gemeint ist damit die oberste Leitung des privaten Verantwortlichen, also das Organ, welches auch die Verantwortung für die Einhaltung der Datenschutzvorschriften trägt. Die Bestimmung statuiert ein Eskalationsrecht der Datenschutzberaterin oder des Datenschutzberaters. Dies ist nötig, damit die Datenschutzberaterin oder der Datenschutzberater bei unternehmensinternen Prüfungen der Einhaltung datenschutzrechtlicher Regeln nicht nur die ihr oder ihm zur Verfügung stehenden Dokumenten vertrauen muss, sondern auch die Beschaffung zusätzlicher Informationen und Dokumente durchsetzen kann. Zudem wird damit gewährleistet, dass die Datenschutzberaterin oder der Datenschutzberater im Falle komplexer Verhältnisse und besonders schwerwiegender Verstösse den höchsten Organen des Verantwortlichen oder des Auftragsbearbeiters berichten und einen Entscheid bewirken kann.

Aufhebung von Artikel 12a VDSG

Diese Bestimmung wird aufgehoben, da ihr Inhalt neu ins Gesetz (Art. 10 Abs. 3 Bst. b und c nDSG) aufgenommen wurde.

Art. 24 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten

Aufgrund von Artikel 12 nDSG müssen die Verantwortlichen und die Auftragsbearbeiter je ein Verzeichnis ihrer Bearbeitungstätigkeiten führen. Dieses muss einige Mindestangaben enthalten. Für das Verzeichnis des Verantwortlichen sind dies: die Identität des Verantwortlichen, den Bearbeitungszweck, eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten, die Kategorien der Empfängerinnen und Empfänger, wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer sowie eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8 nDSG, und, falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2 nDSG (Art. 12 Abs. 2 nDSG).

Für manche KMU kann das Führen eines solchen Verzeichnisses einen unverhältnismässigen Verwaltungsaufwand bedeuten, im Vergleich zu den möglichen Risiken, welche die Datenbearbeitung für die Persönlichkeit der betroffenen Personen mit sich bringt. Da der Bundesrat nach Artikel 12 Absatz 5 nDSG Ausnahmen für Unternehmen, einschliesslich Einzelunternehmen, vorzusehen hat, ist er dementsprechend auch befugt, diese Ausnahmen bei natürlichen Personen und anderen Rechtseinheiten wie Vereinen und Stiftungen anzuwenden. Dies erscheint angemessen, weil das Führen des Verzeichnisses für sie, ebenso wie für die KMU, einen unverhältnismässigen Aufwand bedeuten könnte.

Artikel 24 DSV (ehem. Art. 26 E-VDSG) konkretisiert somit Artikel 12 Absatz 5 nDSG, indem er bestimmt, für wen diese Ausnahmen gelten und in welchen Fällen die Risiken von Persönlichkeitsverletzungen im Sinne dieser Bestimmung gering sind (vgl. Botschaft, BBl *2017* 7037). Er sieht vor, dass Unternehmen und andere privatrechtliche Organisationen mit weniger als 250 Mitarbeitenden am 1. Januar eines Jahres (unabhängig vom Beschäftigungsgrad) sowie natürliche Personen von der Pflicht befreit sind, ein Verzeichnis der Bearbeitungstätigkeiten zu führen. Allerdings gilt dies nur, wenn nicht in grossem Umfang besonders schützenswerte Personendaten bearbeitet werden (Bst. a) und wenn kein Profiling mit hohem Risiko durchgeführt wird (Bst. b). Die Anforderung von Artikel 24 Buchstabe a DSV entspricht dabei Artikel 22 Absatz 2 Buchstabe a nDSG. Mit anderen Worten sind nur KMU, die gewisse Datenbearbeitungen mit hohem Risiko durchführen, verpflichtet, ein Verzeichnis der Bearbeitungstätigkeiten zu führen. Die Aufzählung der Datenbearbeitungen mit hohem Risiko ist in dieser Bestimmung abschliessend. Für die Vorgabe in Buchstabe a sei auf die Ausführungen zur gleich ausgestalteten Vorgabe in Artikel 5 Absatz 1 Buchstabe a DSV (ehem. Art. 4 Abs. 1 Bst. a E-VDSG) zur Pflicht von privaten Personen zur Erstellung eines Bearbeitungsreglements verwiesen.

Als umfangreiche Bearbeitungen besonders schützenswerter Daten gelten insbesondere Datenbearbeitungen, die grosse Mengen von Daten oder eine grosse Zahl von Personen betreffen.

KMU, welche Daten im Sinne von Artikel 24 Buchstabe a und b DSV bearbeiten, müssen nur für diese Datenbearbeitungen, nicht aber für andere Datenbearbeitungen ein Verzeichnis der Bearbeitungstätigkeiten führen. Natürlich bleibt es auch den KMU, die von der Pflicht ausgenommen sind, nicht verwehrt, freiwillig ein Verzeichnis der Bearbeitungstätigkeiten zu führen. Gerade wenn ein Verantwortlicher regelmässig Personendaten bearbeitet, ist es ein nützliches und einfaches Instrument, um einen Überblick über die Bearbeitungstätigkeiten zu behalten, was dem Verantwortlichen auch die Einhaltung anderer Verpflichtungen, wie etwa der Informationsplicht, erleichtern kann.

5.5 5. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane

5.5.1 1. Abschnitt: Datenschutzberaterin oder -berater

Die Artikel 25–28 DSV (ehem. Art. 25–30 E-VDSG) ersetzen Artikel 23 VDSG, der sich mit der Datenschutzberaterin oder dem Datenschutzberater von Bundesorganen befasst.

Art. 25 Ernennung

Artikel 25 DSV setzt Artikel 10 Absatz 4 nDSG und Artikel 32 der Richtlinie (EU) 2016/680 um. Die Regelung, wonach mehrere Bundesorgane gemeinsam eine Datenschutzberaterin oder einen Datenschutzberater bezeichnen können, soll es insbesondere kleineren Bundesorganen oder Departementen mit zentralisierter Organisationstruktur ermöglichen, sinnvolle und ressourceneinsparende Synergien zu nutzen. Hingegen kann beispielsweise von grösseren Bundesämtern erwartet werden, dass diese für sich alleine über eine Datenschutzberaterin oder einen Datenschutzberater verfügen. Natürlich steht es den Bundesorganen auch offen, mehrere Beraterinnen und Berater zu bezeichnen.

Art. 26 Anforderungen und Aufgaben

Abs. 1

Artikel 26 Absatz 1 DSV übernimmt in Buchstabe a die Anforderung des Artikels 12*a* Absatz 2 letzter Teilsatz VDSG. In Buchstabe b wird – wie bisher in Artikel 12*b* Absatz 2 Buchstabe a VDSG geregelt und analog zur Regelung bei den privaten Verantwortlichen in Artikel 10 Absatz 3 Buchstabe a nDSG – neu für alle Bundesorgane verbindlich vorgesehen (bisher mussten nur diejenigen Bundesorgane die Anforderungen von Art. 12*a* und Art. 12*b* VDSG erfüllen, die sich von der Pflicht befreien wollten, ihre Datensammlungen anzumelden, s. Art. 23 Abs. 2 VDSG), dass die Datenschutzberaterin oder der Datenschutzberater ihre oder seine Funktion fachlich unabhängig und weisungsungebunden ausübt. Dadurch wird die Rolle der Datenschutzberaterin oder des Datenschutzberaters in den üblicherweise hierarchisch geprägten Bundesorganen gestärkt und institutionalisiert, damit sie oder er ihre oder seine Aufgaben wirksam erfüllen kann. Zwar ist die Rolle der Datenschutzberaterin oder des Datenschutzberaters lediglich beratend und unterstützend und somit das mögliche Konfliktpotenzial mit den verantwortlichen und vorgesetzten Stellen als herabgesetzt anzusehen. Dennoch muss gewährleistet sein, dass die Datenschutzberaterin oder der Datenschutzberater ihre Empfehlungen – mögen sie in der Natur der Sache liegend teilweise unliebsam sein – frei aussprechen können, ohne Nachteile befürchten zu müssen. Die Unabhängigkeit impliziert auch, dass sich die Datenschutzberaterin oder der Datenschutzberater in wichtigen Fällen – wie dies für Private in Artikel 23 Buchstabe c DSV explizit vorgesehen wird – an die oberste Leitung des Bundesorgans werden kann. Die Unabhängigkeit der Datenschutzberaterin oder des Datenschutzberaters ist vor allem durch organisatorische Massnahmen sicherzustellen: So ist insbesondere zu verhindern, dass sich die Tätigkeit als Datenschutzberaterin oder -berater negativ auf das Mitarbeitergespräch auswirken kann.

Abs. 2

Die Aufgaben der Datenschutzberaterin oder des Datenschutzberaters des Bundesorganes in Absatz 2 wurden terminologisch mit der Bestimmung bei den privaten Verantwortlichen (Art. 10 Abs. 3 nDSG) abgestimmt. In Absatz 2 Buchstabe a wird festgehalten, dass die Datenschutzberaterin oder der Datenschutzberater, wie bereits in Artikel 10 Absatz 2 Buchstabe b

nDSG festgehalten, bei der Anwendung der Datenschutzvorschriften mitwirkt. Dies beinhaltet insbesondere, dass sie oder er nach Ziffer 1. die Bearbeitung von Personendaten prüft und Korrekturmassnahmen empfiehlt, wenn eine Verletzung der Datenschutzvorschriften festgestellt wird; und nach Ziffer 2. den Verantwortlichen bei der Erstellung der Datenschutz-Folgenabschätzung berät und deren Ausführung überprüft. Die Mitwirkung der Datenschutzberaterin oder des Datenschutzberaters kann dazu beitragen, dass der EDÖB entlastet wird. Die Vorgabe in Ziffer 2. entspricht Artikel 7 Buchstabe c der Richtlinie (EU) 2016/680. Die Datenschutzberaterin oder der Datenschutzberater ist als beratende und unterstützende Stelle zu verstehen und nicht als Überwachungsorgan. In Bezug auf die Prüfung von Bearbeitungen und Empfehlung von Korrekturmassnahmen ist daher darauf hinzuweisen, dass es nicht etwa darum geht, eine aktive Prüfpflicht einzuführen beziehungsweise systematische Kontrollen aller Datenbearbeitungen vorzuschreiben. Vielmehr ist es ausreichend, wenn sie oder er aktiv wird, falls beispielsweise Anfragen der verantwortlichen Stellen zur Prüfung einer Datenbearbeitung vorliegen oder ihr oder ihm Hinweise zugetragen werden, dass Datenschutzvorschriften verletzt worden sind. Natürlich bleibt es aber auch unbenommen, dass die Datenschutzberaterin oder der Datenschutzberater proaktiv prüft. Weiter dient die Datenschutzberaterin oder der Datenschutzberater gemäss Absatz 2 Buchstabe b als Anlaufstelle für die betroffenen Personen, beispielsweise im Falle eines Auskunftsgesuches nach Artikel 25 nDSG.

Art. 27 Pflichten des Bundesorgans

Artikel 27 Absatz 1 Buchstabe a DSV (ehem. Art. 29 Abs. 1 E-VDSG) ist identisch zur Regelung bei den privaten Verantwortlichen in Artikel 22 Buchstabe b DSV (ehem. Art. 25 Abs. 2 Bst. b E-VDSG). Hier kann daher sinngemäss auf die dortigen Ausführungen verwiesen werden. Stehen spezialgesetzliche Grundlagen dem Zugang der Datenschutzberaterin oder des Datenschutzberaters zu gewissen Informationen, insbesondere Personendaten, entgegen, gehen diese gemäss dem allgemeinen Grundsatz der Lex specialis vor. Gegebenenfalls sind die Personendaten zu schwärzen, sofern die Datenschutzberaterin oder der Datenschutzberater für ihre oder seine Aufgabenerfüllung Zugang zu Informationen benötigt, die Personendaten beinhalten. Gemäss Artikel 27 Absatz 1 Buchstabe b DSV ist das Bundesorgan neu verpflichtet, dafür zu sorgen, dass die Beraterin oder der Berater über Verletzungen der Datensicherheit informiert wird. Diese Pflicht kann z. B. dadurch gewährleistet werden, dass das Bundesorgan, die Mitarbeitenden mittels Weisung dazu verpflichtet, im Fall einer Verletzung der Datensicherheit die Beraterin bzw. den Berater zu informieren. Die Pflicht betrifft nicht nur Verletzungen, die dem EDÖB gestützt auf Artikel 24 nDSG gemeldet werden müssen, sondern bezieht sich auf jegliche Verletzungen der Datensicherheit. Die Datenschutzberaterin oder der Datenschutzberater berät den Verantwortlichen bei der Frage, ob die Verletzung einer Meldepflicht im Sinne von Artikel 24 nDSG unterliegt. Die Meldung an sich liegt aber in der Verantwortung des Verantwortlichen: Er entscheidet darüber, ob und welche Verletzungen dem EDÖB gemeldet werden.

Absatz 2 wurde neu eingefügt und sieht eine analoge Regelung wie in Artikel 10 Absatz 3 Buchstabe d nDSG bei den privaten Verantwortlichen vor. Dadurch soll den betroffenen Personen die Ausübung ihrer Rechte erleichtert werden, indem zumindest eine fachliche Ansprechperson unmittelbar ausfindig gemacht werden kann. Dabei ist es nicht erforderlich, den Namen der Datenschutzberaterin oder des Datenschutzberaters zu veröffentlichen. So genügt es, wenn etwa eine E-Mail-Adresse der fachlich zuständigen Stelle angegeben wird. Weiter sind auch dem EDÖB die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters mitzuteilen.

Art. 28 Anlaufstelle des EDÖB

Artikel 28 DSV (ehem. Art. 30 E-VDSG) übernimmt in präzisierter Form den Sinngehalt von Artikel 23 Absatz 3 VDSG. Die Formulierung wurde aber angepasst, da sie als Kontaktbeschränkung missverstanden wurde. Den Bundesorganen soll es unbenommen bleiben, auch über andere Stellen mit dem EDÖB zu verkehren und nicht nur über die Datenschutzberaterin oder den Datenschutzberater. Es ist nicht die Meinung, dass sie oder er als Verbindungsperson für den EDÖB fungiert, sondern als Anlaufstelle, da sie oder er in Fragen im Zusammenhang mit der Bearbeitung von Personendaten durch das eigene Bundesorgan über die notwendigen Fachkenntnisse und das interne Wissen verfügt.

5.5.2 2. Abschnitt: Informationspflichten

Art. 29 Informationspflicht bei der Bekanntgabe von Personendaten

Diese Bestimmung entspricht den Artikeln 12 und 26 VDSG und betrifft die Zuverlässigkeit der bekanntgegebenen Personendaten. Nebst der «Aktualität» und der «Zuverlässigkeit» der Personendaten wird in Artikel 29 DSV (ehem. Art. 15 E-VDSG) neu die «Vollständigkeit» erwähnt. Zur Sicherstellung der Datenqualität müssen die Daten aktuell, zuverlässig und vollständig (d. h. weder nur teilweise vorhanden noch lückenhaft) sein. Die Bestimmung wird so an Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680 angepasst. Sie ergänzt Artikel 6 Absatz 5 nDSG.

Art. 30 Informationspflicht bei der systematischen Beschaffung von Personendaten

Die Regelung entspricht dem geltenden Artikel 24 VDSG: Ist die betroffene Person nicht zur Auskunft verpflichtet, so muss das verantwortliche Bundesorgan diese auf die Freiwilligkeit ihrer Auskunftserteilung hinweisen. Entsprechend der Regelung des Artikels 24 VDSG gilt diese Pflicht ebenfalls einzig für die systematische Beschaffung von Personendaten. Sie betrifft insbesondere den Bereich der Statistik und Forschung.

5.5.3 3. Abschnitt: Meldung der Projekte zur automatisierten Bearbeitung von Personendaten an den EDÖB

Art. 31

In Artikel 31 Absatz 1 DSV wird geregelt, dass das verantwortliche Bundesorgan dem EDÖB die geplanten automatisierten Bearbeitungstätigkeiten zum Zeitpunkt der Projektfreigabe oder des Entscheids zur Entwicklung zu melden hat. Im Vergleich zur subsidiären Meldung an den EDÖB nach Artikel 20 Absatz 2 VDSG, die auf eine inhaltliche Prüfung der Projekte abzielt, dient die vorliegende Meldung dem EDÖB hingegen zur reinen Übersicht über geplante Projekte, in denen automatisiert Personendaten bearbeitet werden sollen. In erster Linie soll die Meldung es dem EDÖB ermöglichen, sich ein Gesamtbild über die geplanten Projekte verschaffen zu können und so auch seine Ressourcenplanung im Bereich der Beratungstätigkeiten und Begleitung von Gesetzgebungsprojekten optimieren zu können. In zweiter Linie dient diese Meldung natürlich auch dem Persönlichkeitsschutz.

Da sich die Projekte im Zeitpunkt der Anmeldung noch in einem frühen Stadium befinden, beschränkt sich der Inhalt der Meldung gemäss Absatz 2 auf eine Teilmenge der Angaben, die in Artikel 12 Absatz 2 nDSG verlangt werden, nämlich auf die Buchstaben a–d. Wie die Meldung der Verzeichnisse der bereits bestehenden Bearbeitungstätigkeiten gemäss Artikel 12 nDSG, nimmt der EDÖB auch die Meldungen der geplanten Bearbeitungstätigkeiten im Register der Bearbeitungstätigkeiten gemäss Artikel 56 nDSG auf. Die Angaben zur Meldung

der geplanten Bearbeitungstätigkeiten werden allerdings nicht veröffentlicht (siehe Art. 42 Abs. 2 DSV). Das verantwortliche Bundesorgan aktualisiert den Eintrag gemäss Absatz 4 beim erfolgreichen Abschluss des Projektes, also beim Übergang in den produktiven Betrieb (bzw. überführt den Eintrag in eine Meldung nach Art. 12 Abs. 4 nDSG), oder bei der Projekteinstellung (d. h. Löschung des Eintrags). Die Meldung ist für den EDÖB daher erst zum Zeitpunkt der Projektfreigabe oder des Entscheids zur Entwicklung des Projekts «sichtbar».

5.5.4 4. Abschnitt: Pilotversuche

Art. 32 Unentbehrlichkeit des Pilotversuchs

Aufgrund von Artikel 35 Absatz 1 nDSG kann der Bundesrat vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder andere Datenbearbeitungen nach Artikel 34 Absatz 2 Buchstaben b und c nDSG bewilligen, wenn bestimmte Voraussetzungen kumulativ erfüllt sind. Eine dieser Voraussetzungen besteht darin, dass für die praktische Umsetzung der Datenbearbeitung eine Testphase vor dem Inkrafttreten, insbesondere aus technischen Gründen, unentbehrlich ist. Um die Regelungsdichte in Artikel 35 nDSG zu vermindern, hat der Bundesrat diese Präzisierungen von Artikel 17*a* Absatz 2 DSG in die Verordnung verschoben.

Artikel 32 DSV bestimmt, in welchen Fällen eine Testphase als unentbehrlich anzusehen ist. Er übernimmt mit einigen redaktionellen Änderungen Artikel 17*a* Absatz 2 DSG. So ist etwa der Begriff der «technischen Neuerungen» wie bis anhin zu verstehen: Davon umfasst wird einerseits der Einsatz neuer Technologien, aber auch der Einsatz von bereits bekannter Technologie in einer neuen Umgebung bzw. beim Umsetzen neuer Lösungen. Als Beispiel dafür kann die SwissCovid App[35] herangezogen werden: Sie basiert zwar auf bereits bekannten Technologien wie Bluetooth, welche aber noch nie in einer vergleichbaren Lösung eingesetzt wurden. Einzig Buchstabe c wird angepasst: Neu werden vom Wortlaut alle Abrufverfahren erfasst und nicht mehr nur diejenigen, die einen Zugang für kantonale Behörden schaffen. Dieser einschränkende Wortlaut hatte entstehungsgeschichtliche Gründe, in der Sache kann aber nicht entscheidend sein, wer der Adressatenkreis des Abrufverfahrens ist, sondern der technische Aspekt steht für die Annahme der Unentbehrlichkeit im Vordergrund (vgl. Art. 35 Abs. 1 Bst. c nDSG).

Mindestens eine Bedingung nach Buchstaben a–c muss erfüllt sein, was insbesondere bedeutet, dass ein Pilotversuch nicht nur aus reinen Zeitgründen eingesetzt werden darf.

Art. 33 Verfahren bei der Bewilligung des Pilotversuchs

Diese Bestimmung übernimmt mit einigen redaktionellen Anpassungen Artikel 27 VDSG. Die Verweise werden wo nötig auf das nDSG angepasst. Ein neuer Absatz 6 wurde hinzugefügt, in welchem – ähnlich wie bisher in Artikel 17*a* Absatz 3 DSG – festgehalten wird, dass die automatisierte Datenbearbeitung in einer Verordnung geregelt wird. Dadurch wird die Transparenz der Pilotversuche gewährleistet.

Art. 34 Evaluationsbericht

Diese Bestimmung übernimmt Artikel 27*a* VDSG.

---

[35] Vgl. Art. 60*a* Epidemiengesetz vom 28. September 2012 (SR **818.101**) und die Verordnung vom 24. Juni 2020 über das Proximity-Tracing-System für das Coronavirus Sars-CoV-2 (SR **818.101.25**).

Nach Artikel 34 DSV unterbreitet das zuständige Bundesorgan dem EDÖB den Entwurf des Evaluationsberichts zur Stellungnahme. Wenn es dies für notwendig erachtet, passt das zuständige Bundesorgan den Evaluationsbericht an.

5.5.5 5. Abschnitt: Datenbearbeitung für nicht personenbezogene Zwecke

Art. 35

Um sicherzustellen, dass die Anwendung der Ausnahmen nach Artikel 39 Absatz 2 nDSG nicht über den gesetzlichen Rahmen hinausgeht, wird in der Verordnung präzisiert, dass bei einer Datenbearbeitung für nicht personenbezogene Zwecke (z. B. für Forschung, Planung oder Statistik), die gleichzeitig einem anderen Zweck dient, diese Ausnahmen nur für die Bearbeitung zu den in Artikel 39 nDSG genannten Zwecken anwendbar sind.

5.6 6. Kapitel: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Art. 36 Sitz und ständiges Sekretariat

Diese Bestimmung entspricht grundsätzlich Artikel 30 VDSG.

Artikel 36 Absatz 1 DSV (ehem. Art. 37 Abs. 1 E-VDSG) bleibt materiell unverändert. Auf die bisherige Nennung des Sekretariats wird aber hier verzichtet, da sich durch die Änderung der Terminologie von «Beauftragten» zu «EDÖB» bereits ergibt, dass damit die Behörde als Ganzes gemeint ist und somit auch das Sekretariat umfasst wird.

Artikel 36 Absatz 2 DSV (ehem. Art. 37 Abs. 1 E-VDSG) regelt das Arbeitsverhältnis des ständigen Sekretariats des EDÖB. Inhaltlich entspricht die Bestimmung dem heutigen Artikel 30 Absatz 2 VDSG. Sie enthält im Vergleich zum geltenden Recht aber (terminologische) Anpassungen und eine Ergänzung. Die oder der Beauftragte und das ständige Sekretariat des EDÖB bilden auch nach der Totalrevision des DSG eine dezentralisierte Verwaltungseinheit ohne Rechtspersönlichkeit, die der Bundeskanzlei administrativ zugeordnet ist (Art. 43 Abs. 4 zweiter Satz nDSG, Art. 2 Abs. 1 Bst. e [BPG][36], Art. 2 Abs. 3 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[37] [RVOG] sowie Art. 8 Abs. 1 Bst. b i. V. m. Anhang 1 Bst. A Ziff. 2.1.1 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[38] [RVOV]). Wie bisher ist in Artikel 43 Absatz 5 zweiter Satz nDSG vorgesehen, dass die oder der Beauftragte ihr bzw. sein Personal selbst anstellt und in diesem Rahmen über gewisse Kompetenzen verfügt. So werden beispielsweise die Arbeitsverträge des Personals des EDÖB von der bzw. dem Beauftragten unterzeichnet. Die oder der Beauftragte gilt für das Sekretariat des EDÖB aber auch weiterhin nicht als personal- oder vorsorgerechtlicher Arbeitgeber im Sinne des BPG. Arbeitgeber ist gemäss Artikel 3 Absatz 1 Buchstabe a BPG der Bundesrat. Auf das Arbeitsverhältnis der Angestellten des ständigen Sekretariats des EDÖB ist deshalb gemäss Artikel 36 Absatz 2 erster Satz DSV weiterhin die Bundespersonalgesetzgebung anwendbar. Somit sind weiterhin die Bundespersonalverordnung vom 3. Juli 2001[39] (BPV), die Verordnung des EFD vom 6. Dezember 2001 zur Bundespersonalverordnung[40] (VBPV) und die Verordnung vom 22. November 2017 über den

---

[36] SR **172.220.1**

[37] SR **172.010**

[38] SR **172.010.1**

[39] SR **172.220.111.3**

[40] SR **172.220.111.31**

Schutz von Personendaten des Bundespersonals[41] (BPDV) anwendbar. Der bisherige Artikel 30 Absatz 2 VDSG erfährt diesbezüglich lediglich eine terminologische Anpassung («Angestellte des ständigen Sekretariats des EDÖB» statt «Sekretariat des Beauftragten» und «Bundespersonalgesetzgebung» statt «Bundespersonalgesetz [...] sowie [...] dessen Vollzugsbestimmungen»). Zusätzlich wird in Artikel 36 Absatz 2 zweiter Satz DSV klargestellt, dass die Angestellten des ständigen Sekretariats des EDÖB im Rahmen des Vorsorgewerks Bund bei der Pensionskasse des Bundes versichert sind. Diese Ergänzung bringt keine materielle Änderung mit sich, sondern hält lediglich die auch schon bisher bestehende vorsorgerechtliche Regelung für das ständige Sekretariat des EDÖB ausdrücklich fest (vgl. Art. 32*a* Abs. 1 und Art. 32*d* Abs. 1 BPG). Das Personal bleibt demnach gemäss den Bestimmungen des Vorsorgereglements vom 15. Juni 2007 für die Angestellten und die Rentenbeziehenden des Vorsorgewerks Bund[42] (VRAB) versichert.

Betreffend das Arbeitsverhältnis des ständigen Sekretariats des EDÖB wird also vorläufig der Status quo beibehalten. Dies rechtfertigt sich insbesondere auch deshalb, weil die administrative Zuordnung zur Bundeskanzlei dem EDÖB erlaubt, seine Ressourcen auf den operativen Betrieb zu konzentrieren. Die Zusammenarbeit zwischen der Bundeskanzlei und dem EDÖB ist so ausgestaltet, dass die Unabhängigkeit des EDÖB gewährleistet bleibt. Gleichwohl stellt sich die Frage, ob der oder dem Beauftragten gegenüber den Angestellten des ständigen Sekretariats personal- und vorsorgerechtliche Arbeitgeberbefugnisse zukommen sollten. Diese Frage ist bei nächster Gelegenheit auf formell-gesetzlicher Stufe zu klären. Die koordinierte Überprüfung und Anpassung der spezialgesetzlichen Rechtsgrundlagen für die Daten juristischer Personen, die in den fünf Jahren nach Inkrafttreten des nDSG erfolgen soll (vgl. Art. 71 nDSG), könnte dazu Gelegenheit bieten.

Die Ausführungsbestimmungen zum Arbeitsverhältnis der oder des Beauftragten sind dagegen nicht durch den Bundesrat, sondern durch die Bundesversammlung zu erlassen. Denn das Arbeitsverhältnis der oder des Beauftragten wird neu mit der Wahl durch die Vereinigte Bundesversammlung begründet (Art. 43 Abs. 1 nDSG). Im Rahmen der parlamentarischen Initiative 21.443 hat die SPK-N am 27. Januar 2022 einen Entwurf für eine Verordnung der Bundesversammlung verabschiedet, der die Ausführungsbestimmungen zum Arbeitsverhältnis der oder des Beauftragten enthält. Ausserdem sind in diesem Zusammenhang einzelne Änderungen des nDSG vorgesehen. Das Parlament hat die Vorlagen in der Schlussabstimmung vom 17. Juni 2022 angenommen.

Artikel 30 Absatz 3 VDSG wurde nicht beibehalten, da der EDÖB neu ein eigenständiges Budget führt, welches in Artikel 45 nDSG sowie in Artikel 142 Absätze 2 und 3 des Parlamentsgesetzes vom 13. Dezember 2002[43] (nParlG) abschliessend geregelt wird.

Art. 37 Kommunikationsweg

Artikel 37 DSV stellt weitgehend eine Übernahme von Artikel 31 Absätze 1 und 1bis VDSG dar. Artikel 31 Absatz 2 wurde nicht in die DSV übernommen, da sich aus der Unabhängigkeit und der Weisungsungebundenheit des EDÖB ohnehin ergibt, dass der EDÖB mit anderen Verwaltungseinheiten direkt kommunizieren kann. Die Streichung führt daher zu keiner materiell-rechtlichen Änderung. Im Vergleich zu Artikel 31 VDSG wurde der erste Absatz geändert. Mit der neuen Formulierung soll präzisiert werden, dass der EDÖB bei Fragen, die nicht

41 SR **172.220.111.4**

42 SR **172.220.141.1**

43 SR **171.10** [BBl **2020** 7639, 7677]

auf der Traktandenliste einer Bundesratssitzung stehen, auch mit dem Bundesrat in Kontakt treten kann, indem er z. B. Stellungnahmen an diesen weiterleiten lässt. Abgesehen davon bleibt Absatz 1 inhaltlich unverändert, weil die Bundeskanzlerin oder der Bundeskanzler sämtliche Mitteilungen an den Bundesrat weiterleiten muss und hierbei keinen Handlungsspielraum hat. Dies gilt auch für das Mitberichtsverfahren. Bei Absatz 2 wurde einzig die Formulierung leicht angepasst; der materielle-rechtliche Gehalt entspricht aber Artikel 31 Absatz 1bis VDSG.

Art. 38 Mitteilung von Entscheiden, Richtlinien und Projekten

Diese Bestimmung entspricht, abgesehen von terminologischen und systematischen Anpassungen, Artikel 32 Absatz 1 VDSG.

Absatz 2: Der Einbezug des EDÖB sollte möglichst frühzeitig erfolgen. Er ist spätestens im Rahmen der Ämterkonsultation zu konsultieren.

Art. 39 Bearbeitung von Personendaten

Nach geltendem Recht wird in Artikel 32 Absatz 2 VDSG festgehalten, für welche Zwecke der EDÖB ein Informations- und Dokumentationssystem betreibt. Der im Rahmen der Totalrevision des DSG neu eingefügte Artikel 57*h* RVOG hält aber zukünftig in allgemeiner Weise fest, dass die Einheiten der Bundesverwaltung zur Verwaltung ihrer Dokumente elektronische Geschäftsverwaltungssysteme führen. Zukünftig ist es daher nicht notwendig auf die Verwendung des Geschäftsverwaltungssystems in der DSV hinzuweisen.

Hingegen werden die Zwecke, zu denen der EDÖB Personendaten bearbeitet, neu ausführlicher geregelt (Abs. 1). Er kann Personendaten, einschliesslich besonders schützenswerter Personendaten, insbesondere zu folgenden Zwecken bearbeiten: zur Ausübung seiner Aufsichtstätigkeiten (Bst. a), zur Ausübung seiner Beratungstätigkeiten (Bst. b), zur Zusammenarbeit mit Bundesbehörden, kantonalen und ausländischen Behörden (Bst. c), zur Aufgabenerfüllung im Rahmen der Strafbestimmungen nach dem DSG (Bst. d), zur Durchführung von Schlichtungsverfahren und zum Erlass von Empfehlungen nach dem Bundesgesetz vom 17. Dezember 2004[44] über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) (Bst. e), zur Durchführung von Evaluationen nach dem BGÖ (Bst. f), zur Durchführung von Verfahren für den Zugang zu amtlichen Dokumenten nach dem BGÖ (Bst. g), zur Information der parlamentarischen Aufsicht (Bst. h), zur Information der Öffentlichkeit (Bst. i) und zur Ausübung seiner Schulungstätigkeiten (Bst. j).

Art. 40 Selbstkontrolle

Artikel 48 nDSG sieht vor, dass der EDÖB durch geeignete Massnahmen sicherstellen muss, dass die Datenschutzvorschriften innerhalb seiner Behörde rechtskonform vollzogen werden. In der Botschaft zum Datenschutzgesetz wird präzisiert, dass der Bundesrat die Aufgabe hat, die vom EDÖB zu ergreifenden Massnahmen in der Verordnung zu konkretisieren (BBl *2017* 6941, 7089).

Vom EDÖB wird gemäss Artikel 40 DSV erwartet, dass er für sämtliche von ihm durchgeführten automatisierten Bearbeitungen ein Bearbeitungsreglement erstellt, und nicht nur in den in Artikel 6 Absatz 1 DSV genannten Fällen, wie z. B. bei der Bearbeitung von besonders

[44] SR **152.3**

schützenswerten Personendaten oder bei einem Profiling. Auch wenn dies (anders als noch in Art. 41 Abs. 2 E-VDSG) nicht ausdrücklich festgehalten wird, so muss der EDÖB ebenso wie andere Bundesorgane, welche zur Erstellung eines Bearbeitungsreglements verpflichtet sind (vgl. Art. 6 DSV), interne Prozesse vorsehen, die gewährleisten, dass seine Datenbearbeitungen entsprechend dem Bearbeitungsreglement durchgeführt werden, und die Einhaltung des Bearbeitungsreglements überprüfen.

Art. 41 Zusammenarbeit mit dem NCSC

Damit der EDÖB bei der Analyse einer eingetretenen Verletzung der Datensicherheit, die der Verantwortliche ihm gestützt auf Artikel 24 nDSG und Artikel 15 DSV (ehem. Art. 19 E-VDSG) gemeldet hat, die technischen Fachspezialistinnen und Fachspezialisten des NCSC miteinbeziehen kann, wird in Artikel 41 Absatz 1 DSV (ehem. Art. 42 E-VDSG) vorgesehen, dass der EDÖB die Angaben zur Meldung einer Verletzung der Datensicherheit dem an das NCSC weiterleiten kann. Die Weiterleitung kann jegliche Angaben gemäss Artikel 15 Absatz 1 DSV enthalten, muss sich aber gleichzeitig auf die für das NCSC für die Analyse des Vorfalls notwendigen Daten beschränken. Dabei kann die Mitteilung des EDÖB an das NCSC auch Personendaten enthalten. Vorausgesetzt ist, dass der Verantwortliche, der zur Meldung an den EDÖB verpflichtet ist, vorgängig sein Einverständnis zur Weiterleitung gegeben hat. Ausserdem darf die Weiterleitung nicht dazu führen, dass Artikel 24 Absatz 6 nDSG umgangen wird, wonach die Meldung nur mit Einverständnis der meldepflichtigen Person im Rahmen eines Strafverfahrens verwendet werden darf. Artikel 41 Absatz 1 DSV ermöglicht dem EDÖB keine systematische Weiterleitung von Meldungen an das NCSC. Vielmehr darf der EDÖB von dieser Möglichkeit nur in Einzelfällen, wo das technische Fachwissen des NCSC für die Abklärung eines Vorfalls erforderlich ist, Gebrauch machen. Die Bestimmung soll bei nächster Gelegenheit auf Gesetzesstufe überführt werden. Aus diesem Grund wird im Anhang des Vorentwurfs zur Änderung des Informationssicherheitsgesetzes vom 18. Dezember 2020[45] (ISG), welchen der Bundesrat am 12. Januar 2022 in die Vernehmlassung geschickt hat[46], ein neuer Artikel 24 Absatz 5bis nDSG vorgesehen. Darin soll auch die Bekanntgabe von besonders schützenswerten Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen des meldepflichtigen Verantwortlichen durch den EDÖB an das NCSC geregelt werden. Falls und sobald der neue Artikel 24 Absatz 5bis nDSG in Kraft tritt, kann Artikel 41 Absatz 1 DSV wieder aufgehoben werden.

Artikel 41 Absatz 2 DSV hält fest, dass sich der EDÖB und der NCSC in überschneidenden Tätigkeitsbereichen koordinieren. Die Norm entspricht im Grundsatz Artikel 20 Absatz 3 zweiter Satz VDSG. Der EDÖB wird dazu verpflichtet, das NCSC zur Stellungnahme einzuladen, bevor er anordnet, dass das Bundesorgan die Vorkehren nach Artikel 8 nDSG trifft. Die rechtliche Grundlage für eine solche Anordnung ist 51 Absatz 3 Buchstabe b nDSG. Ziel ist es insbesondere, dass der EDÖB und das NCSC in demselben Bereich nicht unterschiedliche Vorgaben an die Bundesorgane stellen. Die Unabhängigkeit des EDÖB bleibt allerdings gewährleistet, da er einzig dazu verpflichtet wird, die Stellungnahme einzuholen, nicht aber auch diese zu berücksichtigen.

Art. 42 Register der Bearbeitungstätigkeiten der Bundesorgane

Aufgrund von Artikel 12 Absatz 4 nDSG müssen die Bundesorgane ihre Verzeichnisse der Bearbeitungstätigkeiten dem EDÖB melden. Von diesem wiederum wird in Artikel 56

---

[45] SR **126** [BBl **2020** 9975]

[46] Die Vernehmlassungsunterlagen sind abrufbar unter <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-86768.html>.

nDSG verlangt, dass er ein Register der Bearbeitungstätigkeiten der Bundesorgane führt und dieses veröffentlicht.

In Artikel 42 Absatz 1 DSV wird präzisiert, was das Register des EDÖB enthalten muss, nämlich die Angaben, die die Bundesorgane gemäss Artikel 12 Absatz 2 nDSG machen müssen. Zusätzlich enthält das Register auch die Angaben zu den geplanten automatisierten Bearbeitungstätigkeiten der Bundesorgane gemäss Artikel 31 Absatz 2 DSV.

Der zweite Absatz präzisiert, dass das Register des EDÖB im Internet zu veröffentlichen ist. Nicht veröffentlicht werden dabei die Registereinträge über die geplanten automatisierten Bearbeitungstätigkeiten der Bundesorgane gemäss Artikel 31 DSV, da diese im Zeitpunkt ihrer Anmeldung als noch nicht definitiv angesehen werden können beziehungsweise noch Änderungen unterliegen könnten.

Art. 43 Verhaltenskodizes

Aufgrund von Artikel 22 Absatz 5 nDSG kann der private Verantwortliche von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn er nach Artikel 13 nDSG zertifiziert ist oder, wenn er einen Verhaltenskodex nach Artikel 11 nDSG einhält, der bestimmte Voraussetzungen erfüllt. Wird ein Verhaltenskodex dem EDÖB vorgelegt, gibt dieser in seiner Stellungnahme an, ob nach seiner Einschätzung die Voraussetzungen erfüllt sind, um von der Erstellung einer Datenschutz-Folgenabschätzung abzusehen. Mit dieser Bestimmung wird präzisiert, dass ein Verantwortlicher, der auf eine Datenschutz-Folgenabschätzung verzichten will, dem EDÖB seinen Verhaltenskodex vorlegen muss und dieser die Möglichkeit haben muss, den Kodex zu beurteilen. Es geht nicht um eine Genehmigung, aber wenn ein Verantwortlicher, entgegen der Stellungnahme des EDÖB, von der Ausnahme nach Artikel 22 Absatz 5 Buchstaben a–c Gebrauch machen will, kann der EDÖB aufgrund von Artikel 51 Absatz 3 Buchstabe d nDSG anordnen, dass der Verantwortliche eine Datenschutz-Folgenabschätzung vornimmt.

Art. 44 Gebühren

Aufgrund von Artikel 59 Absatz 1 nDSG muss der EDÖB für bestimmte Dienstleistungen, die er für private Personen erbringt, Gebühren erheben. Dazu gehören die Stellungnahme zu einem Verhaltenskodex (Bst. a), die Genehmigung von Standarddatenschutzklauseln und verbindlichen unternehmensinternen Datenschutzvorschriften (Bst. b), die Prüfung der Datenschutz-Folgenabschätzung (Bst. c), vorsorgliche Massnahmen und Massnahmen nach Artikel 51 nDSG (Bst. d) sowie Beratungen in Fragen des Datenschutzes (Bst. e).

Mit Artikel 59 Absatz 2 nDSG wird der Bundesrat beauftragt, die Höhe der Gebühren festzulegen.

Artikel 44 Absatz 1 DSV (ehem. Art. 44 Abs. 1 E-VDSG) hält den Grundsatz fest, dass die Gebühren sich nach dem Zeitaufwand bemessen. Gemäss Absatz 2 gilt ein Stundenansatz von 150–250 Franken je nach Funktion des ausführenden Personals. Der Betrag richtet sich nach dem Stundenansatz des Personals der erforderlichen Funktion, um die Dienstleistung erbringen zu können. Der EDÖB berechnet die Gebühren demnach ausgehend von den aufgewendeten Stunden des ausführenden Personals. Hierbei sind jegliche Personen miteinzubeziehen, die zur Erbringung der Dienstleistung einen Beitrag geleistet haben. Gemäss Absatz 3 hat der EDÖB die Möglichkeit bei einer Dienstleistung von aussergewöhnlichem Umfang, besonderer Schwierigkeit oder Dringlichkeit Zuschläge von bis zu 50 Prozent der Gebühr gemäss Absatz 2 zu erheben. Die Regelung präzisiert die allgemeine Vorgabe von

Artikel 5 Absatz 3 der Allgemeinen Gebührenverordnung vom 8. September 2004[47] (AllgGebV). Im Fall, dass die Dienstleistung des EDÖB durch die gebührenpflichtige Person zu kommerziellen Zwecken weiterverwendet werden kann, kann der EDÖB gemäss Absatz 4 Zuschläge bis zu 100 Prozent der Gebühr nach Absatz 2 erheben. Wenn der EDÖB beispielsweise ein Tool beurteilt, dass von der gesuchstellenden Person als datenschutzkonforme Anwendung weiterverkauft werden kann, soll der EDÖB die Möglichkeit haben, die Gebühr zu erhöhen, so dass sie ungefähr dem Stundenlohn eines spezialisierten Anwalts entspricht. Massgeblich ist dabei, ob die Dienstleistung geeignet ist, zu kommerziellen Zwecken weiterverwendet zu werden, unabhängig davon, ob dies tatsächlich geschieht. Die Regelung gemäss Absatz 4 betrifft insbesondere den Fall der Beratung im Sinne von Artikel 59 Absatz 1 Buchstabe e nDSG. Gleichwohl ist auch denkbar, dass der EDÖB Standarddatenschutzklauseln oder Verhaltenskodizes beurteilt, die zu kommerziellen weiterverwendet werden können, z. B. weil sie als Prototyp für weitere Standarddatenschutzklauseln oder Verhaltenskodizes herangezogen werden können. In Absatz 5 wird im Übrigen die AllgGebV für anwendbar erklärt. Die AllgGebV ihrerseits regelt insbesondere die Grundsätze der Gebührenerhebung, die Ausnahmen von der Gebührenpflicht sowie das Inkassoverfahren.

5.7 7. Kapitel: Schlussbestimmungen

Art. 45 Aufhebung und Änderung anderer Erlasse

Da die Bestimmungen zur Aufhebung und zur Änderung anderer Erlasse zusammen mehr als eine Druckseite umfassen, werden sie in einem Anhang aufgeführt. Die Aufhebung und Änderung anderer Erlasse wird unter Ziffer 7 kommentiert.

Art. 46 Übergangsbestimmungen

Artikel 4 Absatz 2 verpflichtet die verantwortlichen Bundesorgane und ihre Auftragsbearbeiter dazu, die automatisierte Bearbeitung von Personendaten zu protokollieren. Für Datenbearbeitungen, die in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, gilt die Pflicht zur Protokollierung aufgrund der Vorgabe von Artikel 25 der genannten Richtlinie seit dem Inkrafttreten des Schengen-Datenschutzgesetzes. Verschiedene Bundesorgane haben im Zusammenhang mit der Umsetzung von Artikel 4 Absatz 2 DSV auf einen Mehraufwand hingewiesen. Um diesem Mehraufwand Rechnung zu tragen, wird in Artikel 46 Absatz 1 für die restlichen Datenbearbeitungen eine Übergangsfrist von drei Jahren ab Inkrafttreten der Verordnung oder spätestens nach Ende des Lebenszyklus des Systems vorgesehen. In dieser Zeit gilt für diese Datenbearbeitungen Artikel 4 Absatz 1 der Verordnung.

In Artikel 8 Absatz 5 DSV wird die Pflicht zur Veröffentlichung von Beurteilungen eingeführt. Artikel 46 Absatz 2 legt fest, dass die Beurteilungen, die vor dem Inkrafttreten der Verordnung durchgeführt wurden, nicht veröffentlicht werden.

Gemäss Artikel 31 DSV müssen Bundesorgane dem EDÖB neu ihre geplanten automatisierten Bearbeitungstätigkeiten melden und zwar im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung. In Absatz 3 wird daher übergangsrechtlich festgelegt, dass Artikel 31 DSV nicht anwendbar ist auf geplante automatisierte Bearbeitungstätigkeiten, bei denen im Zeitpunkt des Inkrafttretens der Verordnung die Projektfreigabe oder der Entscheid zur Projektentwicklung bereits erfolgt ist.

[47] SR **172.041.1**

6 Erläuterungen zu Anhang 1 (Staaten, Gebiete, spezifische Sektoren in einem Staat und internationale Organe mit einem angemessenen Datenschutzniveau)

Aufgrund von Artikel 16 Absatz 1 nDSG ist der Bundesrat dafür zuständig und hat die Aufgabe zu beurteilen, welcher Staat (oder welches Gebiet oder welcher spezifischer Sektor eines Staates) und welches internationales Organ ein angemessenes Schutzniveau für die Bekanntgabe von Personendaten ins Ausland gewährleistet.

Eine Liste der Staaten wird im Anhang der Verordnung veröffentlicht. Ziel dieser Liste ist es, einen einheitlichen Raum in Sachen Datenschutz zu schaffen. Die Liste wird regelmässig überprüft werden, um einerseits die Praxis anderer Staaten und andererseits die Entwicklungen auf internationaler Ebene, insbesondere die Ratifizierungen des revidierten Übereinkommens SEV 108, zu berücksichtigen. Die Liste ist folglich nicht endgültig und könnte vor dem Inkrafttreten der Verordnung noch geändert werden.

Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Daten zu Strafverfolgungszwecken nur dann ein, wenn dies im Anhang angegeben ist. So bedeutet die Angabe eines Sternchens (*), dass die Beurteilung der Angemessenheit des Datenschutzes die Bekanntgabe von Personendaten entsprechend der Richtlinie (EU) 2016/680[48] mit einschliesst, während zwei Sternchen (**) bedeuten, dass die Bekanntgabe von Personendaten gemäss einem Durchführungsbeschluss der Europäischen Kommission, mit welchem die Angemessenheit des Datenschutzes entsprechend der Richtlinie (EU) 2016/680 festgestellt wird, mit eingeschlossen ist (das trifft zurzeit auf das Vereinigte Königreich zu). Drei Sternchen (***) schliesslich bedeuten, dass die Beurteilung der Angemessenheit des Datenschutzes die Bekanntgabe von Personendaten im Rahmen der von der Richtlinie (EU) 2016/680 vorgesehenen Zusammenarbeit nicht miteinschliesst.

7 Erläuterungen zu Anhang 2 (Aufhebung und Änderung anderer Erlasse)

7.1 Aufhebung der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993

Da es sich bei der DSV um eine Totalrevision der aktuellen VDSG handelt, muss diese aufgehoben werden.

7.2 Übersicht über die Änderungen im sektoriellen Verordnungsrecht

Da es sich beim Datenschutzrecht um eine Querschnittsmaterie handelt, müssen die Änderungen, die im nDSG und in der DSV vorgenommen werden, in den Datenschutzbestimmungen im sektoriellen Verordnungsrecht nachvollzogen werden.

Bei den Änderungen handelt es sich in erster Linie um begriffliche Anpassungen. Dazu gehören insbesondere folgende Änderungen:

– Der Begriff «Persönlichkeitsprofil» wurde im nDSG aufgehoben und durch den Begriff «Profiling» ersetzt.[49] Wird im sektoriellen Gesetz der Begriff «Persönlichkeitsprofil» ersatzlos gestrichen, so wird auch in den dazugehörigen Verordnungen eine Streichung vorgenommen.

---

[48] 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 119/89 vom 4.5.2016, S. 89.

[49] Vgl. die Ausführungen in der Botschaft DSG vom 15. September 2017 (BBl **2017** 6941, 7021, 7109).

Wenn der Begriff durch eine neue Formulierung ersetzt wird, so wird diese auch in die dazugehörigen Verordnungen übernommen.
- Auf den Begriff «Datensammlung» wird im nDSG ebenfalls verzichtet.[50] Der Begriff wird im sektoriellen Verordnungsrecht insbesondere durch «Datenbank», «Datenbearbeitung», «Datenbestände» oder «Datenerhebung» ersetzt. Steht der Begriff nicht im Zusammenhang mit Datenschutzbestimmungen, so kann auf eine Änderung verzichtet werden. Der Begriff «Inhaber einer Datensammlung» wird entsprechend Artikel 5 Buchstabe j nDSG durch «Verantwortlicher» ersetzt.
- Bei der Bezeichnung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten wird auf Gesetzesebene neu zwischen der oder dem Beauftragten und der Institution unterschieden. Die Abkürzung «EDÖB» meint die Institution, «die oder der Beauftragte» bezeichnet die Leiterin oder den Leiter des EDÖB. Der Begriffsunterscheidung wird im sektoriellen Verordnungsrecht nachvollzogen.
- Der Begriff «Daten über administrative und strafrechtliche Verfolgungen und Sanktionen» wird entsprechend Artikel 5 Buchstabe c Ziffer 5 nDSG durch «Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen» ersetzt.

Weiter müssen im sektoriellen Verordnungsrecht die Verweise an das nDSG bzw. die DSV angepasst werden. Eine Anpassung muss auch dann erfolgen, wenn das DSG im Ingress einer Verordnung erwähnt wird.

Mit dem nDSG werden die Daten juristischer Personen vom sachlichen Geltungsbereich des Gesetzes ausgenommen.[51] Der Begriff «Personendaten» bezieht sich daher neu einzig auf Daten natürlicher Personen. Diese Neuerung führt dazu, dass die Rechtsgrundlagen, mit denen Bundesorgane zur Bearbeitung und Bekanntgabe von Personendaten ermächtigt werden, inskünftig nicht mehr anwendbar sind, soweit es um Daten juristischer Personen geht. Aufgrund des Legalitätsprinzips bedarf jedoch auch die staatliche Bearbeitung bzw. Bekanntgabe von Daten juristischer Personen einer gesetzlichen Grundlage. Inskünftig wird der Umgang mit Daten juristischer Personen deshalb zum Teil im RVOG geregelt. Andernteils müssen alle spezialgesetzlichen Datenschutzbestimmungen daraufhin geprüft werden, ob sie für Daten juristischer Person beibehalten werden sollen oder angepasst werden müssen. In Artikel 71 nDSG ist deshalb eine Übergangsbestimmung vorgesehen, wonach für Bundesorgane Vorschriften in anderen Bundeserlassen, die sich auf Personendaten beziehen, während fünf Jahren nach Inkrafttreten des nDSG weiter Anwendung auf Daten juristischer Personen finden. In diesen fünf Jahren soll eine vom BJ koordinierte Überprüfung und Anpassung der spezialgesetzlichen Rechtsgrundlagen für Daten juristischer Personen stattfinden. Allerdings wurden im Rahmen der Totalrevision des DSG in einzelnen Gesetzen aus Gründen der Praktikabilität und der Rechtssicherheit die Rechtsgrundlagen betreffend die Daten juristischer Personen bereits angepasst. Für diese Fälle müssen auch auf Verordnungsstufe die notwendigen Anpassungen vorgenommen werden. Der Bundesrat hat sich dazu entschieden, hier einen zurückhaltenden Ansatz zu verfolgen. Aus diesem Grund werden nicht jegliche Verordnungen angepasst, die gestützt auf ein sektorielles Gesetz erlassen worden sind, dessen Rechtsgrundlagen betreffend die Daten juristischer Personen angepasst wurden. Ziel ist es insbesondere zu vermeiden, dass Rechtskonflikte entstehen, weil Verordnungen angepasst werden, die sich auch auf andere sektorielle Gesetze stützen, in welchen die Rechtsgrundlagen betreffend Daten juristischer Personen im Anhang 1/II nDSG (noch) nicht angepasst wurden. Es wird zwischen den Verordnungen zum RVOG und den anderen Sachgesetzen unter-

[50] Vgl. die Ausführungen in der Botschaft DSG vom 15. September 2017 (BBl **2017** 6941, 7023 f.).

[51] Vgl. die Ausführungen in der Botschaft DSG vom 15. September 2017 (BBl **2017** 6941, 6972, 7011 f.)

schieden. Im RVOG wurden die Bestimmungen zur Bearbeitung von Daten in Geschäftsverwaltungssystemen (Art. 57*h*–*h*[ter] RVOG) sowie bei der Nutzung der elektronischen Infrastruktur (Art. 57*i*–57*l* RVOG) angepasst. Auf Verordnungsstufe soll eine analoge Anpassung erfolgen: Die Anpassung soll sich daher auf Verordnungen beschränken, die sich auf dieselben Regelungsaspekte beziehen. Ausserdem wird – aus den oben erwähnten Gründen – darauf verzichtet, Verordnungen anzupassen, die sich auch auf andere sektorielle Gesetze abstützen, in denen keine Anpassung im Rahmen der Totalrevision des DSG erfolgt ist. Bei den anderen Sachgesetzen (z. B. BGÖ, Nationalbankengesetz) wird ein gesamtheitlicher Ansatz verfolgt. Um für den gesamten Sachbereich eine kohärente Lösung zu generieren, wurden einerseits jegliche Verordnungen angepasst, die sich einzig auf das angepasste Gesetz abstützen. Weiter wurden auch die Bestimmungen einer Verordnung angepasst, wenn sich eine Anpassung in inhaltlicher Hinsicht aufdrängt (z. B. weil es sich um eine Präzisierung oder Umsetzung einer angepassten Gesetzesbestimmung handelt). Für die Verordnungen, die nicht angepasst werden, gilt aber jedenfalls die Übergangsbestimmung von Artikel 71 nDSG, wonach sich der Begriff «Personendaten» weiterhin auf Daten natürlicher und juristischer Personen bezieht. Im Anhang DSV werden folgende Verordnungen bereits angepasst:

- Öffentlichkeitsverordnung vom 24. Mai 2006[52] (vgl. Ziff. 7.15)
- Verordnung vom 22. Februar 2012[53] über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (vgl. Ziff. 7.18)
- Verordnung von 30. Juni 1993[54] über die Organisation der Bundesstatistik (vgl. Ziff. 7.53)
- Statistikerhebungsverordnung vom 30. Juni 1993[55] (vgl. Ziff. 7.54)
- Verordnung vom 25. Juni 2003[56] über die Gebühren und Entschädigungen für statistische Dienstleistungen von Verwaltungseinheiten des Bundes (vgl. Ziff. 7.56)
- Verordnung vom 9. Juni 2017[57] über das eidgenössische Gebäude- und Wohnungsregister (vgl. Ziff. 7.57)
- Verordnung vom 30. Juni 1993[58] über das Betriebs- und Unternehmensregister (vgl. Ziff. 7.58)
- Energieverordnung vom 1. November 2017[59] (vgl. Ziff. 7.76)
- Stromversorgungsverordnung vom 14. März 2008[60] (vgl. Ziff. 7.79)
- Verordnung gegen die Schwarzarbeit vom 6. September 2006[61] (vgl. Ziff. 7.114)

Schliesslich werden die Bestimmungen in den sektoriellen Verordnungen auch an die Neuerungen in der DSV angeglichen, damit mit Inkrafttreten der neuen Verordnung kein Widerspruch entsteht. Beispielhaft sei hier auf die Änderung in Artikel 4 Absatz 5 DSV verwiesen, wonach die Protokolle getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden. Hingegen wird die Dauer der Aufbewahrung der Protokolle im sektoriellen Recht weiterhin wie gemäss geltendem Recht geregelt. In Bezug auf die Modalitäten

---

52 SR **152.31**

53 SR **172.010.442**

54 SR **431.011**

55 SR **431.012.1**

56 SR **431.09**

57 SR **431.841**

58 SR **431.903**

59 SR **730.01**

60 SR **734.71**

61 SR **822.411**

des Auskunftsrechts wurden die Datenschutzbestimmungen im sektoriellen Recht so angepasst, dass sie für die Form des Auskunftsersuchens auf Artikel 16 DSV verweisen. Die Ergänzung, wonach sich die Person über ihre Identität ausweisen muss, wurde im sektoriellen Verordnungsrecht gelöscht, da diese Anforderung neu in der DSV in Artikel 16 Absatz 5 geregelt wird und eine Präzisierung im sektoriellen Recht nicht notwendig erscheint.

7.3 Verordnung vom 4. März 2011[62] über die Personensicherheitsprüfungen

Art. 12 Abs. 1 Bst. e, Abs. 2 Bst. a Ziff. 2 und Anhang 1, Ziff. 2.1, zweite. Zeile

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte wird gemäss Artikel 43 Absatz 1 nDSG neu nicht mehr durch den Bundesrat, sondern durch das Parlament gewählt. Es obliegt der Wahlbehörde zu bestimmen, ob der/die Beauftragte weiterhin einer Personensicherheitsprüfung unterliegen soll. Die Nennung der/s Beauftragten in Artikel 12 Absatz 1 Buchstabe e und Absatz 2 Buchstabe a Ziffer 2 und Anhang 1, Ziffer 2.1 wurde daher aufgehoben. Sämtliche Funktionen innerhalb des EDÖB, ausgenommen die Leiterin oder der Leiter des EDÖB, unterstehen aber einer Personensicherheitsprüfung. Anhang 1, Ziff. 2.1 wurde entsprechend angepasst.

Art. 21 Abs. 2

Der Verweis wird an die neue Nummerierung des nDSG angepasst.

7.4 Verordnung vom 4. Dezember 2009[63] über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN

Art. 9 Abs. 1 Bst. a Ziff. 3 und Abs. 4 Bst. b

Der Ausdruck «die oder der Datenschutz- und Informationsschutzbeauftragte von fedpol» wird durch «die Datenschutzberaterin oder der Datenschutzberater von fedpol» ersetzt.

Art. 13 Abs. 1 Bst. a

Der Verweis wird an die DSV angepasst. Der Verweis auf Artikel 20 VDSG wird durch die Artikel 1–4 und 6 DSV ersetzt, da die Regelung der Datensicherheit im 1. Abschnitt als Einheit zu betrachten ist. Der Verweis bezieht sich daher neu auch auf die Regelung des Bearbeitungsreglements, das ebenfalls im Abschnitt zur Datensicherheit geregelt wird.

7.5 Verordnung vom 16. August 2017[64] über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes

Art. 13 Abs. 1 Bst. a

Der Verweis wird an die DSV angepasst. Der Verweis auf Artikel 20 VDSG wird durch die Artikel 1–4 und 6 DSV ersetzt, da die Regelung der Datensicherheit im 1. Abschnitt als Einheit

---

62 SR **120.4**

63 SR **120.52**

64 SR **121.2**

zu betrachten ist. Der Verweis bezieht sich daher neu auch auf die Regelung des Bearbeitungsreglements, das ebenfalls im Abschnitt zur Datensicherheit geregelt wird.

Art. 17 Abs. 3, 23 Abs. 3, 30 Abs. 3, 67 Abs. 2

Entsprechend der Änderung in Artikel 44 Absatz 1 Nachrichtendienstgesetz (Ziffer 2 Anhang 1/II nDSG) wird der Begriff «Persönlichkeitsprofil» durch «Personendaten, einschliesslich Personendaten, welche die Beurteilung des Gefährlichkeitsgrades einer Person erlauben, zu bearbeiten, unabhängig davon, ob es sich um besonders schützenswerte Personendaten handelt oder nicht» ersetzt.

Art. 38 Abs. 1, 44 Abs. 1, 59 Abs. 1

Diese Änderung betrifft nur den französischen und italienischen Text. Der Begriff «fichier» wird durch «données des dossiers» ersetzt.

7.6 Verordnung vom 24. Oktober 2007[65] über Zulassung, Aufenthalt und Erwerbstätigkeit

Art. 89a

Diese Bestimmung wird in zwei Punkten geändert. Einerseits bezieht sich der Verweis auf das Ausländergesetz neu auf Artikel 111*d* Absatz 3 und nicht mehr auf Artikel 111*d* als Ganzen. Andererseits wird Artikel 89*a* an die Terminologie von Artikel 16 nDSG und die geeigneten Garantien nach den Artikeln 9–12 DSV angepasst.

7.7 Verordnung vom 10. November 2021[66] über das Einreise- und Ausreisesystem

Art. 18 Abs. 1 und 20 Abs. 2 Bst. a

Die Verweise werden an das nDSG bzw. die DSV angepasst.

7.8 Asylverordnung 3 vom 11. August 1999[67]

Art. 1b Abs. 2 erster Satz

Der Begriff «Persönlichkeitsprofil» wird gestrichen.

Art. 6a

Artikel 6*a* wird an die Terminologie von Artikel 16 nDSG und die geeigneten Garantien nach den Artikeln 9–12 DSV angepasst.

Art. 12 Bst. a

Der Verweis wird an die DSV angepasst.

---

65 SR **142.201**

66 SR **142.206**

67 SR **142.314**

7.9 Visa-Informationssystem-Verordnung vom 18. Dezember 2013[68]

Art. 31 Abs. 1

Die Norm wird so angepasst, dass sie für die Form des Auskunftsersuchens neu auf Artikel 16 DSV verweist. In Bezug auf das Berichtigungs- und Löschungsrecht wird neu auf das nDSG verwiesen.

Art. 32 Abs. 1 Einleitungssatz, Bst. a und c

Die Formulierung des Einleitungssatzes wurde formell leicht angepasst. In Buchstabe a wird der Begriff «Inhaber der Datensammlung» durch den Begriff «Verantwortlicher» ersetzt. Wie Buchstabe c wird auch Buchstabe a angepasst, damit er Artikel 19 Absatz 2 nDSG entspricht.

Art. 34 Bst. a

Der Verweis wird an die DSV angepasst.

7.10 ZEMIS-Verordnung vom 12. April 2006[69]

Art. 13 Abs. 1 Einleitungssatz und Abs. 4

Der Begriff «fichiers électroniques» wird durch «banques de données» ersetzt. Diese Änderung betrifft nur den französischen Text.

Art. 14 Abs. 2

Absatz 2 wird aufgehoben, da er in Widerspruch zu Artikel 39 nDSG steht.

Art. 17 Abs. 1 Bst. a

Der Verweis wird an die DSV angepasst.

Art. 19 Abs. 1 und 2

In Absatz 1 wird der Verweis an das nDSG angepasst. In der deutschen Fassung wird der Begriff «besonders schützenswerte Personendaten» durch «Personendaten» ersetzt, um den Inhalt an die französische und italienische Fassung anzugleichen.

Absatz 2 wird in seiner Formulierung angepasst, um ihn an die Vorgaben von Artikel 20 Absatz 1 DSV anzugleichen.

7.11 Ausweisverordnung vom 20. September 2002[70]

Art. 40 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren. Um die Vorgaben im sektoriellen Recht zu

---

[68] SR **142.512**

[69] SR **142.513**

[70] SR **143.11**

vereinheitlichen, wird die Vorgabe, dass die Protokolle revisionsgerecht aufzubewahren sind, gelöscht.

Art. 42 Abs. 1 und 3

Absatz 1 wird so angepasst, dass er für die Form des Auskunftsersuchens neu auf Artikel 16 DSV verweist. In Absatz 3 wird der Verweis an das nDSG angepasst.

Art. 43

Der Verweis wird an das nDSG angepasst.

7.12 Verordnung vom 14. November 2012[71] über die Ausstellung von Reisedokumenten für ausländische Personen

Art. 30 Abs. 1, 3 und 5

Absatz 1 wird so angepasst, dass er für die Form des Auskunftsersuchens neu auf Artikel 16 DSV verweist. In den Absätzen 3 und 5 werden die Verweise an das nDSG angepasst.

7.13 Verordnung vom 2. November 2016[72] zum Bundesgesetz zum Internationalen Übereinkommen zum Schutz aller Personen vor dem Verschwindenlassen

Art. 10 Abs. 2

Der Verweis wird an die neue Nummerierung des nDSG angepasst.

7.14 Archivierungsverordnung vom 8. September 1999[73]

Art. 12 Abs. 3 erster Satz und Art. 14 Abs. 1 erster Satz

Der Begriff «Persönlichkeitsprofile» wird gestrichen.

Art. 26 Abs. 2

Absatz 2 wird aufgehoben, da es sich um einen veralteten Verweis handelt.

7.15 Öffentlichkeitsverordnung vom 24. Mai 2006[74]

Art. 12 Abs. 1, 2 erster und zweiter Satz sowie Abs. 3, 12a Abs. 1 Einleitungssatz und 2, 12b Abs. 1 Einleitungssatz, Bst. b und c sowie 4, 13 Abs. 1, 3 und 4, 13a Sachüberschrift, 21 Einleitungssatz

Der oder die eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (der oder die Beauftragte) wird durch der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, «EDÖB» oder er/dieser bzw. ihm ersetzt. Die Änderungen in Artikel 12 Absatz 2 erster und zweiter Satz sowie Absatz 3, Artikel 12*b* Absatz 1 Buchstaben b und c, Artikel 13 Absatz 3 betreffen nur die deutsche Fassung.

---

[71] SR **143.5**

[72] SR **150.21**

[73] SR **152.11**

[74] SR **152.31**

Art. 13 Abs. 3 und 4

Entsprechend den Änderungen im Öffentlichkeitsgesetz (Ziffer 10 Anhang 1/II nDSG) wird der Begriff «Personendaten» in Artikel 13 Absätze 3 und 4 mit dem Schutz von Daten juristischer Personen ergänzt. Die Änderungen in Absatz 4 betreffen nur die deutsche Fassung.

7.16 Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[75]

Art. 27i

Der Verweis wird an das nDSG angepasst.

7.17 GEVER-Verordnung vom 3. April 2019[76]

Ingress

Aufgrund der Änderungen im RVOG (Ziff. 13 Anhang 1/II nDSG) stützt sich die GEVER-Verordnung neu auf Artikel 57*h*^{ter} RVOG. Der Ingress wird entsprechend angepasst.

Art. 2 Abs. 3

Der Absatz wird angepasst, damit er dem neuen Artikel 57*h* Absatz 1 RVOG entspricht (vgl. Ziff. 13 Anhang 1/II nDSG).

7.18 Verordnung vom 22. Februar 2012[77] über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen

Titel

Entsprechend den Änderungen im Regierungs- und Verwaltungsorganisationsgesetz (Ziff. 13 Anhang 1/II nDSG) wird der Titel der Verordnung um den Schutz von Daten juristischer Personen erweitert.

Art. 1 Bst. a und b

Bei den Begriffen «bewirtschaftete Daten» und «nicht bewirtschaftete Daten» wird der Ausdruck «Personendaten» durch «Personendaten und Daten juristischer Personen» ersetzt.

Art. 10 Abs. 3

Artikel 10 Absatz 3 wird angepasst, da neu grundsätzlich jedes Bundesorgan über eine Datenschutzberaterin oder einen Datenschutzberater verfügen muss.

Art. 14

Der Begriff «Personendaten» wird durch «ihre Daten» ersetzt.

---

[75] SR **172.010.1**

[76] SR **172.010.441**

[77] SR **172.010.442**

7.19 Verordnung vom 25. November 2020[78] über die digitale Transformation und die Informatik

Art. 26 Abs. 2

Der Begriff «Persönlichkeitsprofil» wird gestrichen.

7.20 Verordnung vom 19. Oktober 2016[79] über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes

Art. 11 Abs. 2

Diese Bestimmung wird gestrichen, da der Begriff «Persönlichkeitsprofil» im nDSG nicht mehr vorkommt.

Art. 13 Abs. 4, 18 Abs. 1 zweiter Satz

Die Pflicht des Verantwortlichen, Datensammlungen dem EDÖB zu melden, wird mit dem nDSG aufgehoben (Art. 11*a* DSG). Das nDSG sieht in Artikel 12 Absatz 4 nDSG neu vor, dass das verantwortliche Bundesorgan das Verzeichnis der Bearbeitungstätigkeiten dem EDÖB melden muss. Artikel 13 Absatz 4 Buchstabe b wird daher so angepasst, dass die Meldung neu an Artikel 12 Absatz 4 nDSG geknüpft wird.

Ausserdem werden in Artikel 13 Absatz 4 und Artikel 18 Absatz 1 zweiter Satz die Verweise an die DSV angepasst.

Art. 17 Abs. 2, 26 Abs. 2

Um die Terminologie zu vereinheitlichen, wird in der deutschen und italienischen Version eine Änderung vorgenommen. Die Begriffe «Datenschutzverantwortliche», «Datenschutzverantwortlicher» und «responsabile della protezione dei dati» werden durch «Datenschutzberaterin», «Datenschutzberater» und «consulente per la protezione dei dati» ersetzt (vgl. hierzu die Ausführungen in der Botschaft DSG vom 15. September 2017, BBl *2017* 6941, 7032 f.).

Art. 25 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.21 Verordnung vom 20. Juni 2018[80] über das Datenbearbeitungssystem des Sprachdienstes EDA

Ingress

Aufgrund der Änderungen im RVOG (Ziff. 13 Anhang 1/II nDSG) stützt sich die Verordnung neu auf Artikel 57*h*^{ter} RVOG. Der Ingress wird entsprechend angepasst.

---

78 SR **172.010.58**

79 SR **172.010.59**

80 SR **172.010.60**

Art. 13 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.22 Gebührenverordnung fedpol vom 4. Mai 2016[81]

Art. 1 Abs. 1 Bst. d

Der Verweis wird an die DSV angepasst.

7.23 Verordnung vom 12. Februar 2020[82] über das öffentliche Beschaffungswesen

Art. 24 Abs. 2 zweiter Satz

Der Verweis wird an das nDSG angepasst.

7.24 Organisationsverordnung für die Bundeskanzlei vom 29. Oktober 2008[83]

Art. 5a Abs. 3 Bst. c, 10 Abs. 1

Die Abkürzung EDÖB wird in Artikel 5*a* Absatz 3 Buchstabe c eingeführt und in Artikel 10 Absatz 1 übernommen.

7.25 IVIPS-Verordnung vom 18. November 2015[84]

Art. 11 Abs. 1 Bst. a

Der Verweis wird an die DSV angepasst.

7.26 Verordnung vom 25. November 1998[85] über den Sonderstab Geiselnahme und Erpressung

Art. 14 Sachüberschrift, Abs. 1 und 2 erster Satz

In der Sachüberschrift und in Absatz 1 wird der Begriff «Datensammlung» durch «Datenbank» ersetzt. Aufgrund der Aufhebung des Begriffs «Dateninhaber» muss Absatz 2 angepasst werden.

7.27 Verordnung vom 22. November 2017[86] über den Schutz von Personendaten des Bundespersonals

Art. 2

Der Begriff «Datensammlung» wird durch «Datenbank» ersetzt.

---

81 SR **172.043.60**

82 SR **172.056.11**

83 SR **172.210.10**

84 SR **172.211.21**

85 SR **172.213.80**

86 SR **172.220.111.4**

Art. 9 Abs. 1

Der Begriff «Persönlichkeitsprofil» wird gestrichen.

Art. 34 Abs. 1 Bst. b

Die Pflicht des Verantwortlichen, Datensammlungen dem EDÖB zu melden, wird mit dem nDSG aufgehoben (Art. 11*a* DSG). Das nDSG sieht in Artikel 12 Absatz 4 nDSG neu vor, dass das verantwortliche Bundesorgan das Verzeichnis der Bearbeitungstätigkeiten dem EDÖB melden muss. Artikel 34 Absatz 1 Buchstabe b wird daher so angepasst, dass die Meldung neu an Artikel 12 Absatz 4 nDSG geknüpft wird.

Art. 16 Abs. 2, 28 Abs. 2, 37 Abs. 2, 44 Abs. 2, 51 Abs. 2, 57 Abs. 2, 65 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.28 Web-EDA-Verordnung vom 5. November 2014[87]

Ingress

Aufgrund der Änderungen im RVOG (Ziff. 13 Anhang 1/II nDSG) stützt sich die Web-EDA-Verordnung neu auf Artikel 57*h*^{ter} RVOG. Der Ingress wird entsprechend angepasst.

Art. 12 Abs. 1 Bst. a

Der Verweis wird an die DSV angepasst.

Art. 13 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren. Die Aufbewahrungsdauer wurde an die Mindestdauer nach Artikel 4 Absatz 5 DSV angepasst.

7.29 Zivilstandsverordnung vom 28. April 2004[88]

Art. 83 Abs. 2–4

Mit den Anpassungen in Artikel 83 Absätze 2–4 ZStV wird der Gesetzesauftrag in Artikel 45*a* Absatz 5 Ziffer 5 Zivilgesetzbuch erfüllt. Dort wird der Bundesrat beauftragt, unter Mitwirkung der Kantone die Aufsicht über die Einhaltung der Datenschutzvorschriften für das Personenstandsregister zu regeln. Aufgrund des neuen Artikels 2 Absatz 4 nDSG wird der Grundsatz, wonach die öffentlichen Register des Privatrechtsverkehrs vom Geltungsbereich des DSG ausgenommen sind, aufgehoben. Dies hat zur Folge, dass das Personenstandsregister in Bezug auf die Einhaltung der Datenschutzvorschriften neu der Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten untersteht (Art. 4 Abs. 2 nDSG e contrario). Für die Koordination dieser Aufsicht wird in Absatz 2 neu vorgesehen, dass das EAZW den EDÖB zur Stellungnahme einlädt, bevor es eine Massnahme trifft, die Fragen des Datenschutzes und der Datensicherheit betrifft. Wird der EDÖB seinerseits im Rahmen

---

[87] SR **172.220.111.42**

[88] SR **211.112.2**

seiner Aufsicht tätig, so ist er aufgrund von Absatz 4 verpflichtet, sich mit dem EAZW und nötigenfalls auch mit den kantonalen Datenschutzbehörden zu koordinieren. Absatz 3 entspricht Artikel 83 Absatz 2 ZStV.

7.30 Verordnung vom 18. November 1992[89] über die amtliche Vermessung

Art. 40 Abs. 5

Die Befugnis, eine Datensammlung zu führen, wird durch die Bearbeitung von Daten ersetzt.

7.31 Handelsregisterverordnung vom 17. Oktober 2007[90]

Art. 12c Abs. 2

In französische und italienische Fassung wird der Begriff «Datensammlung» durch «Datenbank» ersetzt.

7.32 Ordipro-Verordnung vom 22. März 2019[91]

Art. 15 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.33 Verordnung E-VERA vom 17. August 2016[92]

Art. 9 Sachüberschrift und Abs. 1 Einleitungssatz

In der französischen Fassung wird der Begriff «fichier» gestrichen. In der deutschen und der italienischen Fassung werden die Begriffe «Datensatz» bzw. «set di dati» durch «Daten» bzw. «dati» ersetzt. In allen drei Fassungen sind ausserdem grammatikalische Anpassungen erforderlich.

Art. 14 Abs. 1 Bst. a

Der Verweis wird an die DSV angepasst.

Art. 15 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

---

89 SR **211.432.2**

90 SR **221.411**

91 SR **235.21**

92 SR **235.22**

7.34 Verordnung EDA-CV vom 26. April 2017[93]

Art. 6 Sachüberschrift

Die Änderung betrifft nur den deutschen Text. Der Begriff «Datensatz» wird durch «Daten» ersetzt, damit die Terminologie innerhalb der Verordnungen über die Informationssysteme des EDA einheitlich bleibt (vgl. Art. 9 Abs. 1 Verordnung E-VERA).

Art. 11 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.35 Verordnung «e-vent» vom 17. Oktober 2018[94]

Ingress

Aufgrund der Änderungen im RVOG (Ziff. 13 Anhang 1/II nDSG) stützt sich die Verordnung «e-vent» neu auf Artikel 57*h*^{ter} RVOG. Der Ingress wird entsprechend angepasst.

Art. 13 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.36 Plato-Verordnung vom 25. September 2020[95]

Ingress

Aufgrund der Änderungen im RVOG (Ziff. 13 Anhang 1/II nDSG) stützt sich die Plato-Verordnung neu auf Artikel 57*h*^{ter} RVOG. Der Ingress wird entsprechend angepasst.

Art. 14 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.37 Verordnung vom 26. Juni 2013[96] über die Eidgenössische Fachkommission zur Beurteilung der Behandelbarkeit lebenslänglich verwahrter Straftäter

Art. 13 Abs. 1

Der Verweis wird an das nDSG angepasst.

---

93 SR **235.23**

94 SR **235.25**

95 SR **235.26**

96 SR **311.039.2**

7.38 Verordnung vom 7. November 2012[97] über den ausserprozessualen Zeugenschutz

Art. 13 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

Art. 15 Abs. 1 Bst. b

Der Verweis wird an die DSV angepasst.

7.39 Verordnung vom 20. September 2013[98] über das Informationssystem für Strafsachen des Bundesamts für Zoll und Grenzsicherheit

Art. 3

Der Verweis wird an die neue Nummerierung der DSV angepasst.

Art. 14 Abs. 1 und 2

In Absatz 1 wird der Verweis an die neue Nummerierung des nDSG angepasst.

Mit der Revision des Bundesgesetzes vom 22. März 1974[99] über das Verwaltungsstrafrecht (Ziff. 27 Anhang 1/II nDSG) wird ein neuer Artikel 18*d* eingefügt, der das Auskunftsrecht der Parteien und anderen Verfahrensbeteiligten bei hängigen Verfahren regelt. Folglich ist Artikel 18*d* in Absatz 2 aufzunehmen.

Art. 18 Abs. 1

Der Verweis auf die Artikel 20 und 21 VDSG wird durch die Artikel 1–4 und 6 DSV ersetzt.

7.40 VOSTRA-Verordnung vom 29. September 2006[100]

Art. 18 Abs. 5

Der Begriff «Datensammlung» wird durch «Datenbank» ersetzt.

Art. 26 Abs. 1 zweiter Satz, 2 und 4

Die Verweise werden an die neue Nummerierung des nDSG angepasst. Absatz 2 wird so angepasst, dass er für die Form des Auskunftsersuchens neu auf Artikel 16 DSV verweist.

Art. 27 Abs. 1 Bst. b

Der Verweis wird an die neue Nummerierung der DSV angepasst.

---

97 SR **312.21**

98 SR **313.041**

99 SR **313.0**

100 SR **331**

Art. 32

Der Verweis wird an die neue Nummerierung des nDSG angepasst. Ausserdem wird die Norm in terminologischer Hinsicht an Artikel 39 nDSG angeglichen.

7.41 ELPAG-Verordnung vom 23. September 2016[101]

Ingress

Aufgrund der Änderungen im RVOG (Ziff. 13 Anhang 1/II nDSG) stützt sich die ELPAG-Verordnung neu auf Artikel 57*h*^{ter} RVOG. Der Ingress wird entsprechend angepasst.

Art. 14 Abs. 1 Einleitungssatz und Bst. a

Der Verweis wird an die neue Datenschutzgesetzgebung angepasst. Die Änderung im Einleitungssatz betrifft nur die französische Fassung. Der Ausdruck «sécurité informatique» wird durch «sécurité des données» ersetzt, um die französische Fassung an den deutschen und italienischen Text anzugleichen.

Art. 15 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren. Um die Vorgaben im sektoriellen Recht zu vereinheitlichen, wird der Passus «ab Erstellung» gelöscht.

Art. 17

Der Verweis wird an das nDSG angepasst.

7.42 Verordnung vom 30. November 2001[102] über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei

Art. 6 Abs. 1 Bst. c und d, 2 Bst. b und c

Die Formulierung wurde angepasst, da Artikel 13 Absatz 2 ZentG keine Voraussetzungen mehr enthält, sondern auf die Vorgaben im StGB verweist.

7.43 JANUS-Verordnung vom 15. Oktober 2008[103]

Art. 19 Abs. 1 Bst. a und b, 2 Bst. a und b

Die Formulierung wurde angepasst, da Artikel 13 Absatz 2 ZentG keine Voraussetzungen mehr enthält, sondern auf die Vorgaben im StGB verweist.

Art. 24 Abs. 1, 26

Die Verweise werden an das nDSG und die neue Nummerierung der DSV angepasst.

---

[101] SR **351.12**

[102] SR **360.1**

[103] SR **360.2**

Art. 26 Bst. a, 29l zweiter Satz, 29n Abs. 1 Bst. a, 29v Abs. 1 zweiter Satz, 29w Abs. 1 Bst. a

Die Verweise werden an die neue Datenschutzgesetzgebung angepasst.

Art. 27 Abs. 1 zweiter Satz, 29i Abs. 2, 29t Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

Anhang 2 Ziff. 4.1 erste Zeile zweite Spalte

Der Begriff «Datensammlung» wird durch «Datenbank» ersetzt.

7.44 RIPOL-Verordnung vom 26. Oktober 2016[104]

Art. 2 Abs. 1 Einleitungssatz und Bst. f, 13 Abs. 1 und 14 Abs. 2 Bst. a

Im Einleitungssatz von Artikel 2 Absatz 1 wird der Begriff «Inhaber der Datenbank» durch «Bundesorgan» ersetzt. Die übrigen Änderungen sind Anpassungen der Verweise an die neue Datenschutzgesetzgebung.

Art. 13 Abs. 1bis und 2

Mit der Revision des Bundesgesetzes vom 13. Juni 2008[105] über die polizeilichen Informationssysteme des Bundes (Ziff. 30 Anhang 1/II nDSG) wird ein neuer Artikel 8*a* BPI eingefügt, durch den das Auskunftsrecht bei Ausschreibungen zur Festnahme zum Zweck der Auslieferung in einem der Systeme nach Artikel 2 BPI, namentlich das automatisierte Polizeifahndungssystem (RIPOL), eingeschränkt wird. Folglich ist Artikel 8*a* BPI in Artikel 13 der RIPOL-Verordnung in einem neuen Absatz 1bis aufzunehmen.

Absatz 2 wird so angepasst, dass er für die Form des Auskunftsersuchens neu auf Artikel 16 DSV verweist.

Art. 15 Abs. 1 zweiter Satz und 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.45 IPAS-Verordnung vom 15. Oktober 2008[106]

Art. 9a, 13 zweiter Satz

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

---

[104] SR **361.0**

[105] SR **361**

[106] SR **361.2**

Die Anpassung in Artikel 9a zweiter Satz betrifft nur die deutsche und italienische Fassung. Der Begriff «Datenschutzbeauftragten» wird durch «Datenschutzberaterin» bzw. «Datenschutzberater» ersetzt.

Art. 10 und 12 Bst. a

Die Verweise werden an die neue Datenschutzgesetzgebung des Bundes angepasst.

7.46 Verordnung vom 6. Dezember 2013[107] über die Bearbeitung biometrischer erkennungsdienstlicher Daten

Art. 3 Abs. 1 Bst. b und d

Die Änderungen betreffen nur den französischen und italienischen Text. Der Begriff «fichier» wird durch «registre» ersetzt.

Art. 3a zweiter Satz, 6 und 14 Bst. a

Die Verweise werden an die neue Datenschutzgesetzgebung angepasst.

Art. 5 Abs. 2

Der Absatz wird so angepasst, dass er für die Form des Auskunftsersuchens neu auf Artikel 16 DSV verweist.

7.47 Polizeiindex-Verordnung vom 15. Oktober 2008[108]

Art. 7 Abs. 1, 12 Abs. 1 Bst. a

Die Verweise werden an die neue Datenschutzgesetzgebung angepasst.

Art. 8 Abs. 1 Bst. c und d

Die Verweise auf die RIPOL-Verordnung vom 15. Oktober 2008[109] und die N-SIS-Verordnung vom 8. März 2013[110] werden aktualisiert.

Art. 11 Abs. 1, 2 Einleitungssatz und 3

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

Die Anpassung in Absatz 1 und 2 betrifft nur die deutsche Fassung. Der Begriff «Datenschutzbeauftragten» wird durch «Datenschutzberaterin» bzw. «Datenschutzberater» ersetzt.

---

[107] SR **361.3**

[108] SR **361.4**

[109] SR **361.0**

[110] SR **362.0**

7.48 N-SIS-Verordnung vom 8. März 2013[111]

Art. 50 Abs. 1

Der Absatz wird so angepasst, dass er für die Form des Auskunftsersuchens neu auf Artikel 16 DSV verweist. In Bezug auf das Berichtigungs- und Löschungsrecht wird neu auf das nDSG verwiesen. In der französischen und italienischen Fassung wird im Titel und in Absatz 1 der Ausdruck «droit à l'information» durch «droit d'accès» ersetzt, um der deutschen Fassung zu entsprechen.

Art. 50 Abs. 6

Mit der Revision des Bundesgesetzes vom 13. Juni 2008[112] über die polizeilichen Informationssysteme des Bundes (Ziff. 30 Anhang 1/II nDSG) wird ein neuer Artikel 8*a* BPI eingefügt, mit dem das Auskunftsrecht bei Ausschreibungen zur Festnahme zum Zweck der Auslieferung in einem der Systeme nach Artikel 2 dieses Gesetzes, namentlich im Schengener Informationssystem, eingeschränkt wird. Folglich ist Artikel 8*a* im neuen Absatz 6 von Artikel 50 aufzunehmen.

Art. 51 Abs. 1 und 2 Bst. c, 53 Abs. 1 Bst. a

Die Verweise werden an die neue Datenschutzgesetzgebung angepasst.

7.49 DNA-Profil-Verordnung vom 3. Dezember 2004[113]

Art. 8 Abs. 1

Der Begriff «Inhaber» wird durch den Ausdruck «verantwortliches Bundesorgan» ersetzt. Der zweite Teil des Satzes von Absatz 1 kann gestrichen werden.

Art. 17 Abs. 1 und 3 erster Satz, Art. 19 Abs. 1 Bst. a

Der Verweis wird an die Nummerierung des nDSG bzw. der DSV angepasst.

Artikel 17 Absatz 3 wird in der Formulierung angepasst, da Artikel 62 DSG selbst keine Verschwiegenheitspflicht normiert, sondern nur die Folgen bei Verletzung dieser Pflicht regelt.

In Artikel 19 Absatz 1 Buchstabe a wird der Verweis auf die Artikel 20–23 VDSG durch die Artikel 1–4 und 6 DSV ersetzt, da sich die Regelung von Artikel 19 gemäss deren Sachüberschrift einzig auf den Regelungsbereich der Datensicherheit bezieht. Die Bestimmungen zur Auftragsbearbeitung und zum Datenschutzberater in der DSV finden aber im Rahmen ihres Geltungsbereiches ebenfalls Anwendung.

---

[111] SR **362.0**

[112] SR **361**

[113] SR **363.1**

7.50 Interpol-Verordnung vom 21. Juni 2013[114]

Art. 4 Abs. 1 Bst. f, 11 Abs. 4 dritter Satz, 12 Abs. 2 zweiter Satz, 16 Abs. 1, 17 Abs. 1

Der Ausdruck «der oder die Datenschutz- und Informationsschutzverantwortliche von fedpol» wird durch «die Datenschutzberaterin oder der Datenschutzberater von fedpol» ersetzt (vgl. hierzu die Ausführungen in der Botschaft DSG vom 15. September 2017, BBl *2017* 6941, 7032 f.).

Art. 16 Abs. 1 und 7

Absatz 1 verweist für die Form des Auskunftsbegehrens neu auf Artikel 16 DSV. Absatz 7 bezieht sich auf das Berichtigungs- und Löschungsrecht und verweist insoweit auf das nDSG.

7.51 Verordnung vom 15. September 2017[115] über die Informationssysteme im Berufsbildungs- und im Hochschulbereich

Art. 20, 21 Abs. 1 Bst. a

Der Verweis wird an das nDSG angepasst.

7.52 Forschungs- und Innovationsförderungsverordnung vom 29. November 2013[116]

Art. 41a Abs. 3

Der Begriff «Persönlichkeitsprofil» wird gestrichen und der Verweis an die Nummerierung des nDSG angepasst.

7.53 Verordnung vom 30. Juni 1993[117] über die Organisation der Bundesstatistik

Art. 9 Abs. 1 zweiter Satz und 4

Diese Änderung betrifft nur den deutschen und italienischen Text. Um die beiden Sprachfassungen an die französische Fassung anzugleichen, wird der Ausdruck «administrative Datensammlungen» durch «Beständen von administrativen Daten» ersetzt.

Art. 10

Der Verweis auf die Datenschutzgesetzgebung wird angepasst. Entsprechend Artikel 16 Bundesstatistikgesetz (Ziff. 35 Anhang 1/II nDSG, BStatG) gilt der Verweis auf die Datenschutzbestimmungen in Absatz 1 nur für Personendaten. Absatz 2, der die Datensicherheit betrifft, findet entsprechend Artikel 15 Absatz 1 BStatG hingegen sowohl auf Personendaten als auch auf Daten juristischer Personen Anwendung. So wird auch in der Botschaft DSG (BBl *2017* 6941, 7133) ausgeführt, dass der Grundsatz der Datensicherheit für beide Kategorien von Personen gelten muss.

---

[114] SR **366.1**

[115] SR **412.108.1**

[116] SR **420.11**

[117] SR **431.011**

7.54 Statistikerhebungsverordnung vom 30. Juni 1993[118]

Art. 5 Abs. 2 Einleitungssatz und 3

In Artikel 5 Absatz 2 wird der Begriff «Personendaten» durch «Personendaten sowie Daten juristischer Personen» ersetzt. In Absatz 3 wird der französische Text an die deutsche Terminologie angepasst («mesures d'organisation» wird durch «mesures techniques et organisationnelles» ersetzt). Der Verweis in Absatz 3 wird so angepasst, dass die Bestimmungen zur Datensicherheit für Daten juristischer Personen sinngemäss zur Anwendung gelangen (vgl. die Ausführungen bei Ziff. 7.53).

Art. 13m Abs. 1

Aufgrund der Aufhebung des Begriffs «Persönlichkeitsprofil» wurde Artikel 14*a* des Bundesstatistikgesetzes vom 9. Oktober 1992[119] zu den Datenverknüpfungen geändert (vgl. Ziff. 35 Anhang 1/II nDSG). So wurde der Begriff «Persönlichkeitsprofile» durch den Ausdruck «die wesentlichen Merkmale einer natürlichen oder juristischen Person» ersetzt. Dieselbe Änderung wird in Artikel 13*m* Absatz 1 vorgenommen.

Anhang

Im ganzen Anhang wird «Schweizerische Studierendendatei SHIS» durch «Schweizerische Datenbank der Studierenden SHIS» und «Schweizerische Hochschulpersonaldatei» durch «schweizerische Datenbank des Hochschulpersonals» ersetzt, mit den nötigen grammatikalischen Anpassungen.

7.55 Verordnung vom 26. Januar 2011[120] über die Unternehmens-Identifikationsnummer

Art. 3 Abs. 1 Bst. b und d, 8 Abs. 4 und 20 Abs. 3

Der Begriff «Datensammlung» wird durch «Datenbank» ersetzt.

7.56 Verordnung vom 25. Juni 2003[121] über die Gebühren und Entschädigungen für statistische Dienstleistungen von Verwaltungseinheiten des Bundes

Art. 1 Bst. d

Der Begriff «Personendaten» wurde durch «Personendaten und Daten juristischer Personen» ersetzt.

---

[118] SR **431.012.1**

[119] SR **431.01**

[120] SR **431.031**

[121] SR **431.09**

7.57 Verordnung vom 9. Juni 2017[122] über das eidgenössische Gebäude- und Wohnungsregister

Art. 9 Abs. 2 Bst. f

Die Änderung betrifft nur den deutschen Text. Der Begriff «Datensammlung» wird durch «Datenbank» ersetzt.

Art. 18 Abs. 1 Bst. a und Abs. 2

Der Verweis wird an die DSV angepasst. Im Bereich der Statistik gelangen die Bestimmungen zur Datensicherheit für Daten juristischer Personen sinngemäss zur Anwendung (vgl. die Ausführungen Ziff. 7.53).

7.58 Verordnung vom 30. Juni 1993[123] über das Betriebs- und Unternehmensregister

Art. 9a Abs. 2, 10 Abs. 3, 14 Abs. 1, 15 Bst. a

Die Verweise werden an das nDSG und die DSV angepasst.

Art. 15 Abs. 2

Im Bereich der Statistik gelangen die Bestimmungen zur Datensicherheit für Daten juristischer Personen sinngemäss zur Anwendung (vgl. die Ausführungen Ziff. 7.53).

7.59 Verordnung vom 4. September 2013[124] über den Verkehr mit Tieren und Pflanzen geschützter Arten

Art. 54

In Absatz 1 wird der Verweis an das nDSG angepasst. Absatz 2 verweist für die Form des Auskunftsbegehrens neu auf Artikel 16 DSV.

7.60 Animex-ch-Verordnung vom 1. September 2010[125]

Art. 18 Abs. 1 und 2

In Absatz 1 wird der Verweis an das nDSG angepasst. Absatz 2 verweist für die Form des Auskunftsbegehrens neu auf Artikel 16 DSV.

7.61 Verordnung vom 4. Dezember 2009[126] über den Nachrichtendienst der Armee

Art. 8 Sachüberschrift und Einleitungssatz

Diese Bestimmung muss aufgrund der Aufhebung des Begriffs «Persönlichkeitsprofil» geändert werden. Entsprechend Artikel 99 Absatz 2 MG wird der Ausdruck «einschliesslich Personendaten, welche die Beurteilung des Grades der Gefährlichkeit einer Person erlauben,

---

[122] SR **431.841**

[123] SR **431.903**

[124] SR **453.0**

[125] SR **455.61**

[126] SR **510.291**

[...] unabhängig davon, ob es sich um besonders schützenswerte Personendaten handelt oder nicht» eingefügt (vgl. Ziff. 40 Anhang 1/II nDSG).

Art. 9

Nach Artikel 56 nDSG führt der EDÖB ein öffentliches Register der Bearbeitungstätigkeiten, welche die Bundesorgane ihm gemeldet haben (Art. 12 Abs. 4 nDSG), und nicht mehr ein Register der Datensammlungen (Art. 11*a* Abs. 1 DSG). Gemäss Artikel 99 Absatz 3 Buchstabe d Militärgesetz (Ziff. 40 Anhang 1/II nDSG) regelt der Bundesrat Ausnahmen zur Registrierung von Datenbearbeitungstätigkeiten, wenn diese die Informationsbeschaffung gefährden würden. Artikel 9 Absatz 1 sieht deshalb vor, dass Datenbearbeitungstätigkeiten, die im Rahmen der Informationsbeschaffung nach Artikel 99 Absatz 2 MG durchgeführt werden, dem EDÖB nicht gemeldet werden müssen, wenn dies die Informationsbeschaffung gefährden würde. Nach Absatz 2 muss der NDA den EDÖB aber in allgemeiner Form über diese Datenbearbeitungstätigkeiten informieren.

Art. 10 Abs. 2

Der Begriff «selbstständige Datensammlungen» wird durch «selbstständige Datenbanken» ersetzt.

7.62 Verordnung vom 17. Oktober 2012[127] über die elektronische Kriegführung und die Funkaufklärung

Art. 4 Abs. 5

Die Pflicht, Datensammlungen anzumelden, wird durch die Meldung der Verzeichnisse der Bearbeitungstätigkeiten ersetzt.

7.63 Informationsschutzverordnung vom 4. Juli 2007[128]

Art. 3 Bst. h

Der Begriff «Datensammlungen» wird durch «Datenbestände» ersetzt. Die französische Fassung wurde an die anderen Sprachfassungen angeglichen.

7.64 Geoinformationsverordnung vom 21. Mai 2008[129]

Im ganzen Erlass

«Datensammlung» wird durch «Daten» ersetzt.

Art. 3a

Im Anhang zum totalrevidierten DSG wurde eine Änderung von Artikel 11 Absatz 2 Geoinformationsgesetz[130] (GeoIG) vorgenommen. Demnach kann der Bundesrat Ausnahmen von der Pflicht, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, vorsehen, wenn aufgrund der

---

[127] SR **510.292**

[128] SR **510.411**

[129] SR **510.620**

[130] SR **510.62**

Bearbeitung lediglich ein beschränktes Risiko für einen Eingriff in die Grundrechte der betroffenen Person besteht. Der Katalog der Geobasisdaten im Anhang 1 der Geoinformationsverordnung (GeoIV) enthält nach derzeitigem Stand nur wenig Personendaten und bezüglich der Bearbeitung dieser besteht kein oder nur ein kleines Risiko für einen Eingriff in ein Grundrecht, zumal die betreffende Spezialgesetzgebung des Bundes in aller Regel die Bekanntgabe der Personendaten ausdrücklich vorsieht. Der Katalog der Geobasisdaten im Anhang 1 entspricht daher den Anforderungen von Artikel 11 Absatz 2 GeoIG. Bei jeder Ergänzung von Anhang 1 muss geprüft werden, ob die Voraussetzungen auch bei den neuen Datensätzen erfüllt sind.

7.65 Verordnung vom 16. Dezember 2009[131] über die militärischen Informationssysteme

Art. 2a, 2b Bst. b, Anhang 1 Titel und erste Zeile vierte Spalte

Der Begriff «Inhaber der Datensammlung» wird gestrichen.

Gliederungstitel vor Art. 72h, 5. Abschnitt, Art. 72h, Art. 72h^{bis}, Art. 72h^{quater}, Art. 72h^{quinquies}, Anhang 35d Titel

Der Begriff «Hilfsdatensammlungen» wird durch «Hilfsdatenbanken» ersetzt.

7.66 Verordnung vom 21. November 2018[132] über die Militärische Sicherheit

Art. 4 Abs. 3

Der Verweis wird an das nDSG angepasst.

Art. 5

Nach Artikel 56 nDSG führt der EDÖB ein öffentliches Register der Bearbeitungstätigkeiten, welche die Bundesorgane ihm gemeldet haben (Art. 12 Abs. 4 nDSG), und nicht mehr ein Register der Datensammlungen (Art. 11*a* Abs. 1 DSG). Gemäss Artikel 100 Absatz 4 Buchstabe c Ziffer 2 Militärgesetz (Ziff. 40 Anhang 1/II nDSG) regelt der Bundesrat Ausnahmen von der Pflicht, Verzeichnisse der Bearbeitungstätigkeiten beim EDÖB zur Registrierung zu melden, wenn diese die Informationsbeschaffung gefährden würde. Artikel 5 sieht deshalb vor, dass Datenbearbeitungstätigkeiten, die im Rahmen eines Assistenz- oder eines Aktivdienstes durchgeführt werden, dem EDÖB nicht gemeldet werden müssen, wenn dies die Informationsbeschaffung und die Erfüllung der Aufgaben nach dieser Verordnung gefährden würde. Nach Absatz 2 muss der NDA den EDÖB aber in allgemeiner Form über diese Datenbearbeitungstätigkeiten informieren. Der Ausdruck «die Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte» wird in Absatz 2 gelöscht, da sich der Absatz auf den EDÖB bezieht.

7.67 Waffenverordnung vom 2. Juli 2008[133]

Art. 58 Abs. 1 Bst. h, 59 Abs. 1 Einleitungssatz, 59a Abs. 1 Einleitungssatz, 60 Sachüberschrift, 66a erster Satz, 66b, 66d, 68 Abs. 2 Bst. c, 69 Bst. c und 70 Abs. 1 Bst. c und Abs. 2 Bst. c

---

[131] SR **510.911**

[132] SR **513.61**

[133] SR **514.541**

Diese Änderung betrifft nur die französische Fassung. Der Begriff «fichier» wird durch «banque de données» ersetzt.

Art. 64

Die Bestimmung wird in zwei Punkten geändert. Einerseits bezieht sich der Verweis auf das Waffengesetz neu auf Artikel 32*e* Absatz 3 und nicht mehr auf Artikel 32*e* als Ganzen. Andererseits wird Artikel 64 an die Terminologie von Artikel 16 nDSG und die geeigneten Garantien nach den Artikeln 9–12 DSV angepasst.

Art. 65, 66b und 66c Abs. 1 Bst. a

Die Verweise werden an das nDSG bzw. die DSV angepasst.

Art. 66a zweiter Satz

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.68 Zivilschutzverordnung vom 11. November 2020[134]

Art. 37 Abs. 3

Die Begriffe «Inhaber der Daten» und «Datenherr» werden durch den Ausdruck «ist für die [...] Daten verantwortlich» ersetzt.

7.69 Verordnung vom 12. August 2015[135] über die Meldestelle für lebenswichtige Humanarzneimittel

Art. 8 Abs. 2 Bst. a

Der Verweis wird an die DSV angepasst.

7.70 Finanzhaushaltverordnung vom 5. April 2006[136]

Art. 1 Abs. 1 Bst. g und Abs. 2, 26 Abs. 2

Der EDÖB verfügt nach dem nDSG über neue Budgetkompetenzen. Gemäss Artikel 45 nDSG reicht der EDÖB den Entwurf seines Budgets jährlich über die Bundeskanzlei dem Bundesrat ein, der diesen unverändert an die Bundesversammlung weiterleitet. Im Parlamentsgesetz (Ziff. 12 Anhang 1/II nDSG, ParlG) wird in Artikel 142 Absatz 2 daher neu vorgesehen, dass der Bundesrat den Entwurf für den Voranschlag sowie die Rechnung des EDÖB unverändert in seinen Entwurf für den Voranschlag und in die Rechnung des Bundes aufnimmt. Gemäss Absatz 3 vertritt der EDÖB den Entwurf für seinen Voranschlag und seine Rechnung vor der Bundesversammlung. Aufgrund dieser Änderungen werden auch Artikel 1 Absätze 1 und 2 und Artikel 26 Absatz 2 der Finanzhaushaltverordnung angepasst.

---

[134] SR **520.11**

[135] SR **531.215.32**

[136] SR **611.01**

7.71 Zollverordnung vom 1. November 2006[137]

Art. 226 Abs. 3 Bst. b

Nach Artikel 103 Absatz 1 Einleitungssatz des revidierten Zollgesetzes (Ziff. 48 Anhang 1/II nDSG) darf das Bundesamt für Zoll und Grenzsicherheit neu die Identität einer Person durch die Abnahme genetischer Daten festhalten. Die heute in Artikel 226 Absatz 3 Buchstabe b Ziffer 1 vorgesehene Gesetzesgrundlage kann folglich gestrichen werden (vgl. Ziff. 9.2.37 der Botschaft des Bundesrates vom 15. September).

7.72 Verordnung 4. April 2007[138] über den Einsatz von Bildaufnahme-, Bildaufzeichnungs- und anderen Überwachungsgeräten durch das Bundesamt für Zoll und Grenzsicherheit

Art. 10 Abs. 1

Der Verweis wird an das nDSG angepasst.

7.73 Datenbearbeitungsverordnung für das BAZG vom 23. August 2017[139]

Ingress

Aufgrund der Änderungen im RVOG (Ziff. 13 Anhang 1/II nDSG) stützt sich die Datenbearbeitungsverordnung für die EZV neu auf Artikel 57*h*^{ter} RVOG. Der Ingress wird entsprechend angepasst.

Art. 8 und 12 Abs. 1

Der Verweis wird an das nDSG bzw. die DSV angepasst. In Artikel 12 wird der Verweis auf die Artikel 20 und 21 VDSG daher durch die Artikel 1–4 und 6 DSV ersetzt.

Anhang 73

Im ganzen Anhang 73 wird «Hilfsdatensammlung» durch «Hilfsdatenbank» ersetzt.

7.74 Verordnung vom 12. Oktober 2011[140] über die Statistik des Aussenhandels

Art. 13

Der Begriff «Datensammlungen» wird durch «Datenbanken» ersetzt.

7.75 Mehrwertsteuerverordnung vom 27. November 2009[141]

Art. 135 Abs. 2

---

137 SR **631.01**

138 SR **631.053**

139 SR **631.061**

140 SR **632.14**

141 SR **641.201**

Diese Änderung erfolgt im Rahmen der im Anhang des DSG vorgenommenen Anpassung von Artikel 14 Absatz 3 Nationalbankgesetz[142] zur Schaffung einer Rechtsgrundlage für den Datenaustausch zwischen der SNB, der ESTV und dem BFS für statistische Zwecke.[143]

7.76 Energieverordnung vom 1. November 2017[144]

Art. 70

Entsprechend der Änderung im Energiesatz (Ziff. 56 Anhang 1/II nDSG) wird der Begriff «Personendaten» durch «Personendaten sowie Daten juristischer Personen» ersetzt. Ausserdem wird der Ausdruck «administrative und strafrechtliche Verfolgungen und Sanktionen» entsprechend der Vorgabe in Artikel 5 Buchstabe c nDSG durch «verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen» ersetzt.

7.77 Verordnung vom 9. Juni 2006[145] über die Anforderungen an das Personal von Kernanlagen

Art. 39 Abs. 1 Einleitungssatz

Der Begriff «Persönlichkeitsprofils» wird gestrichen.

7.78 Verordnung vom 9. Juni 2006[146] über die Betriebswachen von Kernanlagen

Art. 18 Abs. 1

Der Begriff «Persönlichkeitsprofils» wird gestrichen.

7.79 Stromversorgungsverordnung vom 14. März 2008[147]

Art. 8d Abs. 1, Abs. 2 Bst. a und 3

Der Ausdruck «Persönlichkeitsprofile» wird gestrichen. Entsprechend der Änderung im Stromversorgungsgesetz (Ziff. 59 Anhang 1/II nDSG, StromVG) wird der Begriff «Personendaten» durch «Personendaten sowie Daten juristischer Personen» ersetzt.

Art. 8d Abs. 5 zweiter Satz

Der Verweis wird an die DSV angepasst. Entsprechend der Änderung in Artikel 17*c* Absatz 1 StromVG werden die Bestimmungen der VDSG für Daten juristischer Personen sinngemäss für anwendbar erklärt.

---

142 SR **951.11**

143 Vgl. Botschaft DSG vom 15. September 2017 (BBl **2017** 6941, 7148 f.).

144 SR **730.01**

145 SR **732.143.1**

146 SR **732.143.2**

147 SR **734.71**

7.80 Verordnung vom 30. November 2018[148] über das Informationssystem Strassenverkehrsunfälle

Ingress

Die Bestimmungen des nDSG werden angepasst.

Art. 17 Abs. 4

Der Verweis wird an das nDSG und die DSV angepasst.

7.81 Verordnung vom 30. November 2018[149] über das Informationssystem Verkehrszulassung

Ingress

Die Bestimmungen des nDSG werden angepasst.

Art. 18 Abs. 5

Der Verweis wird an die DSV angepasst.

7.82 Videoüberwachungsverordnung ÖV vom 4. November 2009[150]

Art. 6 Abs. 2

Der Verweis wird an die DSV angepasst.

7.83 Verordnung vom 17. Dezember 2014[151] über die Sicherheitsuntersuchung von Zwischenfällen im Verkehrswesen

Art. 19 Abs. 2

In Absatz 2 wird der Verweis an das nDSG angepasst.

Ausserdem wird in der französischen Fassung eine formelle Anpassung vorgenommen, damit wie in den anderen Sprachfassungen neu zwei Absätze bestehen.

7.84 Verordnung vom 2. September 2015[152] über die Zulassung als Strassentransportunternehmen im Personen- und Güterverkehr

Art. 14

Die Norm verweist für die Form des Auskunftsbegehrens neu auf Artikel 16 DSV. In Bezug auf das Berichtigungsrecht wird neu auf das nDSG verwiesen.

---

[148] SR **741.57**

[149] SR **741.58**

[150] SR **742.147.2**

[151] SR **742.161**

[152] SR **744.103**

7.85 Verordnung vom 4. November 2009[153] über die Personenbeförderung

Art. 58b Abs. 1

Die Norm verweist für die Form des Auskunftsbegehrens neu auf Artikel 16 DSV. In Bezug auf das Berichtigungsrecht wird neu auf das nDSG verwiesen.

7.86 Verordnung vom 18. Dezember 1995[154] über den Flugsicherungsdienst

Art. 40a Abs. 1 und 2

Im Absatz 1 wurde «die Erbringer» (Plural) mit «der Erbringer» (Singular) ersetzt, um Kohärenz mit den folgenden Absätzen zu gewährleisten. Im Absatz 2 wird der Begriff «Datensammlung» durch den Begriff «Datenbank» ersetzt.

7.87 Verordnung vom 15. November 2017[155] über die Überwachung des Post- und Fernmeldeverkehrs

Art. 8 Abs. 2

Die Ausdrücke «Datenschutzbeauftragte» und «Datenschutzbeauftragter» werden durch «Datenschutzberaterin» und «Datenschutzberater» ersetzt.

7.88 Verordnung vom 15. November 2017[156] über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs

Art. 7 Abs. 4, 8 Abs. 2 erster Satz

Der Verweis wird an die DSV und das nDSG angepasst.

7.89 Verordnung vom 9. März 2007[157] über Fernmeldedienste

Art. 48 Abs. 3 zweiter Satz

Der Ausdruck «administrative und strafrechtliche Verfolgungen und Sanktionen» wird entsprechend der Vorgabe in Artikel 5 Buchstabe c nDSG durch «verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen» ersetzt.

Art. 89

Der Verweis wird an das nDSG angepasst.

---

153 SR **745.11**

154 SR **748.132.1**

155 SR **780.11**

156 SR **780.12**

157 SR **784.101.1**

7.90 Verordnung vom 6. Oktober 1997[158] über die Adressierungselemente im Fernmeldebereich

Art. 13l Abs. 2

Der Verweis wird an das nDSG angepasst.

7.91 Verordnung vom 5. November 2014[159] über Internet-Domains

Art. 17 Abs. 2 Bst. f

Der Verweis wird an das nDSG angepasst.

7.92 Fortpflanzungsmedizinverordnung vom 4. Dezember 2000[160]

Art. 19a Abs. 2 zweiter Satz

Der Verweis wird an das nDSG angepasst.

7.93 Verordnung vom 14. Februar 2007[161] über genetische Untersuchungen beim Menschen

Art. 21 Abs. 3

Der Verweis wird an das nDSG angepasst.

7.94 Transplantationsverordnung vom 16. März 2007[162]

Art. 48 Abs. 3, 49 zweiter Satz

Der Verweis wird an das nDSG und die DSV angepasst.

Art. 49c Abs. 1 erster Satz

Der Begriff «Inhaber der Datensammlung» wird gestrichen. Dies bringt keine materiell-rechtliche Änderung mit sich.

7.95 Überkreuz-Lebendspende-Verordnung vom 18. Oktober 2017[163]

Art. 21 Abs. 1 erster Satz

Der Begriff «Inhaber der Datensammlung» wird gestrichen. Dies bringt keine materiell-rechtliche Änderung mit sich.

---

158 SR **784.104**

159 SR **784.104.2**

160 SR **810.112.2**

161 SR **810.122.1**

162 SR **810.211**

163 SR **810.212.3**

7.96 Organzuteilungsverordnung vom 16. März 2007[164]

Art. 34c Abs. 1 erster Satz

Der Begriff «Inhaber der Datenbank» wird gestrichen. Dies bringt keine materiell-rechtliche Änderung mit sich.

Art. 34i Abs. 1 Bst. a

Der Verweis auf die Artikel 20 und 21 VDSG wird durch die Artikel 1–4 und 6 DSV ersetzt.

7.97 Humanforschungsverordnung vom 20. September 2013[165]

Art. 26 Abs. 2

In der deutschen Fassung wird der Begriff «Datensammlung» durch «Personendaten» ersetzt. Ausserdem werden die deutsche und die italienische Fassung an die französische Version angeglichen, indem der Begriff Material mit «biologisch» ergänzt wird.

7.98 Organisationsverordnung HFG vom 20. September 2013[166]

Art. 11 Abs. 2 Bst. a und b

Artikel 11 regelt die Pflicht der Vollzugsbehörde, der betroffenen Person mitzuteilen, wenn sie Personendaten über sie bekanntgibt.

Die Ausnahmen nach Absatz 2 Buchstaben a und b entsprechen nicht den Vorschriften nach Artikel 20 Absatz 1 Buchstaben a und b nDSG. Absatz 2 Buchstabe a muss folglich angepasst werden. Die Ausnahme nach Absatz 2 Buchstabe b muss gestrichen werden, da sie in Artikel 20 nDSG nicht vorgesehen ist.

Art. 12

Diese Bestimmung regelt den Austausch von Daten mit ausländischen Behörden und Institutionen. Die Absätze 1, 2 und 3 tragen den neuen Anforderungen nach den Artikeln 16 Absätze 1 und 2 Buchstabe c und 17 Absatz 1 Buchstaben a und d nDSG Rechnung.

Absatz 4 übernimmt die Regelung von Artikel 19 Absatz 4 nDSG.

7.99 Prüfungsverordnung MedBG vom 26. November 2008[167]

Art. 26 Abs. 2

Die Norm übernimmt die Vorgaben von Artikel 16 Absatz 1 erster Satz und Absatz 3 DSV. Für die Form des Auskunftsbegehrens wird nicht auf Artikel 16 DSV verwiesen, da im Unterschied zu Artikel 16 Absatz 1 zweiter Satz DSV das Auskunftsbegehren aufgrund der Sensibilität der bearbeiteten Personendaten nicht mündlich gestellt werden kann.

---

[164] SR **810.212.4**

[165] SR **810.301**

[166] SR **810.308**

[167] SR **811.113.3**

7.100 Arzneimittel-Bewilligungsverordnung vom 14. November 2018[168]

Art. 66 Bst. b

Diese Änderung betrifft nur die deutsche Fassung. Der Begriff «Daten über administrative und strafrechtliche Verfolgungen und Sanktionen» wird in Artikel 5 Buchstabe c Ziffer 5 nDSG durch «Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen» ersetzt.

Art. 68 Abs. 2

Der erste Satz wird so angepasst, dass alle Zugriffe auf das Informationssystem protokolliert werden. Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.101 Arzneimittelverordnung vom 21. September 2018[169] über die Arzneimittel

Art. 76 Abs. 2 zweiter Satz

In der französischen Fassung wird eine formelle Änderung vorgenommen, um den ersten Satz an die deutsche Version anzugleichen. Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.102 Tierarzneimittelverordnung vom 18. August 2004[170]

Art. 36 Sachüberschrift und Abs. 5

In der Sachüberschrift wird der Begriff «Datensammlung» durch «Datenbearbeitung» ersetzt. In Absatz 5 wird der Verweis an das nDSG angepasst.

7.103 Medizinprodukteverordnung vom 1. Juli 2020[171]

Art. 84 Abs. 1 und 2

Der Verweis wird an die DSV angepasst. In Absatz 2 wird der Verweis auf Artikel 20 und 21 VDSG wird durch Artikel 1-4 und 6 DSV ersetzt.

Art. 92 und Anhang 3, 2 Schweizerisches Recht, Ziff. 13, zweite Spalte

Der Verweis wird an das nDSG angepasst.

---

[168] SR **812.212.1**

[169] SR **812.212.21**

[170] SR **812.212.27**

[171] SR **812.213**

7.104 Verordnung vom 31. Oktober 2018[172] über das Informationssystem Antibiotika in der Veterinärmedizin

Art. 13

In Absatz 1 wird der Verweis an das nDSG angepasst. Absatz 2 verweist für die Form des Auskunftsbegehrens neu auf Artikel 16 DSV.

7.105 Verordnung vom 4. Mai 2022[173] über In-vitro-Diagnostika

Anhang 2, 2 Schweizerisches Recht, Ziff. 7, zweite Spalte

Der Verweis wird an das nDSG angepasst.

7.106 Störfallverordnung vom 27. Februar 1991[174]

Art. 17 Sachüberschrift

In der deutschen Fassung wird «Datensammlung» durch «Datenerhebung» ersetzt.

7.107 Verordnung vom 20. Oktober 2021[175] über die Rückgabe, die Rücknahme und die Entsorgung elektrischer und elektronischer Geräte

Art. 8

Der Verweis wird an das nDSG angepasst.

7.108 Verordnung vom 22. März 2017[176] über das elektronische Patientendossier

Art. 12 Abs. 1 zweiter Satz Bst. b

Nach Absatz 1 Buchstabe b des geltenden Rechts müssen die Gemeinschaften ein risikogerechtes Datenschutz- und Datensicherheitsmanagementsystem betreiben, das insbesondere ein Inventar der Informatikmittel und Datensammlungen umfassen muss. Da die Verantwortlichen im nDSG (Art. 12) neu verpflichtet werden, ein Verzeichnis ihrer Bearbeitungstätigkeiten zu führen, muss die Bestimmung geändert werden.

7.109 Verordnung vom 27. Mai 2020[177] über den Vollzug der Lebensmittelgesetzgebung

Art. 97 Abs. 1–3

Die Absätze 1 und 2 von Artikel 97 müssten an die Terminologie des nDSG angepasst werden. Da sie im Vergleich zum nDSG und zur DSV keinen zusätzlichen normativen Inhalt normieren, werden sie aufgehoben.

---

[172] SR **812.214.4**

[173] SR **812.219**

[174] SR **814.012**

[175] SR **814.620**

[176] SR **814.012**

[177] SR **817.042**

Absatz 3 betrifft nur die deutsche Fassung. Der Begriff «Daten über administrative und strafrechtliche Verfolgungen und Sanktionen» in Artikel 5 Buchstabe c Ziffer 5 nDSG durch «Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen» ersetzt.

Art. 98 Abs. 4

In Absatz 4 wird der Ausdruck «unbedingt» gelöscht, um den Absatz an die Terminologie in Artikel 6 Absatz 4 nDSG anzugleichen. Es sollen nur diejenigen Personendaten bekanntgegeben werden dürfen, die für die Empfängerin bzw. den Empfänger erforderlich sind.

7.110 Epidemienverordnung vom 29. April 2015[178]

Art. 90 Sachüberschrift

Aufgrund der Aufhebung des Begriffs der Datensammlung wird die Sachüberschrift von Artikel 90 angepasst.

Art. 96

Der Verweis auf die Artikel 20 und 21 VDSG wird durch die Artikel 1–4 und 6 DSV ersetzt.

Art. 97 zweiter Satz

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.111 Verordnung vom 29. April 2015[179] über mikrobiologische Laboratorien

Art. 23 Abs. 1 zweiter Satz

Diese Änderung betrifft nur die französische Fassung. Der Begriff «fichier» wird durch «dossier» ersetzt.

7.112 Verordnung 1 vom 10. Mai 2000[180] zum Arbeitsgesetz

Ingress, Art. 89 und 90

Die Verweise werden an das nDSG angepasst.

7.113 Chauffeurverordnung vom 19. Juni 1995[181]

Art. 18 Abs. 6

Die Verweise werden an das nDSG und die DSV angepasst.

---

[178] SR **818.101.1**

[179] SR **818.101.32**

[180] SR **822.111**

[181] SR **822.221**

7.114 Verordnung vom 6. September 2006[182] gegen die Schwarzarbeit

Art. 9 Sachüberschrift und Abs. 1 sowie 9a

Da durch das nDSG der Schutz der Personendaten juristischer Personen aufgehoben wird, wird in Artikel 17*a* des Entwurfs zur Revision des Bundesgesetzes gegen die Schwarzarbeit eine neue Gesetzesgrundlage eingefügt, gestützt auf welche die kantonalen Kontrollorgane und die zuständigen kantonalen Behörden befugt sind, Daten juristischer Personen zu bearbeiten (Ziff. 78 Anhang 1/II nDSG). Gemäss dem Revisionsentwurf werden die Sachüberschrift und Absatz 1 von Artikel 9 der Verordnung gegen die Schwarzarbeit so angepasst, dass die Bestimmung neu ausschliesslich den Schutz von Personendaten regelt. Es wird zudem ein neuer Artikel 9*a* eingefügt, der die Bearbeitung von Daten juristischer Personen regelt. Artikel 9*a* enthält in Absatz 1 eine analoge Regelung zu Artikel 9 Absatz 1. Artikel 9 Absätze 2-4 gelten gemäss Artikel 9*a* Absatz 2 sinngemäss für Daten juristischer Personen.

7.115 Arbeitsvermittlungsverordnung vom 16. Januar 1991[183]

Art. 58 Sachüberschrift und Abs. 1

Artikel 58 der Arbeitsvermittlungsverordnung regelt das Recht der betroffenen Person, von den Diensten, die Daten über sie bearbeiten, Auskunft zu erhalten.

Er wird an die neuen Vorgaben des nDSG angepasst, namentlich an Artikel 19 nDSG (Informationspflicht bei der Beschaffung von Personendaten), 25 nDSG (Auskunftsrecht) und 41 nDSG (Ansprüche und Verfahren).

Die erste Änderung betrifft die Sachüberschrift von Artikel 58, die nicht korrekt ist. Wie im Folgenden dargelegt wird, regelt die Bestimmung verschiedene Rechte der betroffenen Personen, und nicht nur das Auskunftsrecht.

Wie im geltenden Recht regelt Absatz 1 die Pflicht, die betroffene Person zu informieren. Der Katalog der zu liefernden Informationen wird jedoch erweitert. Nach dem neuen Absatz 1 werden Stellensuchende und Arbeitgeber, die sich bei der Arbeitsmarktbehörde melden, neu orientiert über die Identität und die Kontaktdaten des Verantwortlichen (Bst. a). Abgesehen von redaktionellen Anpassungen bleiben die Informationen nach den Buchstaben b, c und e dieselben. Die Information nach Buchstabe d wird dahingehend geändert, dass die betroffene Person nicht mehr über «die regelmässigen Empfänger» orientiert werden muss, sondern über alle Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen die Personendaten bekanntgegeben werden.

Art. 59a

Die Änderung betrifft nur den französischen Text. Der Begriff «fichier» wird durch «registre» ersetzt.

---

[182] SR **822.411**

[183] SR **823.111**

7.116 Zivildienstverordnung vom 11. September 1996[184]

Art. 110 Sachüberschrift, Abs. 1 und 2 Einleitungssatz

Der Begriff «Datensammlung» wird durch «Datenbank» ersetzt.

7.117 Verordnung vom 20. August 2014[185] über das Informationssystem des Zivildienstes

Art. 11 Abs. 1 Bst. a, 13 Abs. 1

Der Verweis wird an die neue Datenschutzgesetzgebung angepasst.

Art. 11 Abs. 4

Die Bestimmung wird an die Protokollierungsanforderungen gemäss DSV angepasst.

7.118 Verordnung vom 11. September 2002[186] über den Allgemeinen Teil des Sozialversicherungsrechts

Art. 8b Abs. 2 dritter Satz, 9 Abs. 2 zweiter Satz

Der Verweis wird an die neue Datenschutzgesetzgebung angepasst.

7.119 Verordnung vom 31. Oktober 1947[187] über die Alters- und Hinterlassenenversicherung

Art. 144 zweiter Satz

Im französischen Text wird der Begriff «fichier» durch «registre» ersetzt.

7.120 Verordnung vom 17. Januar 1961[188] über die Invalidenversicherung

Im französischen Text wird der Begriff «fichiers de données» durch «ensembles de données» ersetzt.

7.121 Verordnung vom 27. Juni 1995[189] über die Krankenversicherung

Art. 30c erster Satz

Der Verweis wird an die neue Nummerierung der DSV angepasst.

Art. 59a Abs. 1 und 3 erster Satz, 6 zweiter Satz und 7 erster Satz

Die Änderungen an den Absätzen 1 und 3 erster Satz betreffen nur den französischen Text. Der Begriff «fichier» wird durch «ensemble» ersetzt. Der französische Text wird so an den deutschen und den italienischen Text angeglichen («Datensatz» bzw. «insieme di dati»).

---

[184] SR **824.01**

[185] SR **824.095**

[186] SR **830.11**

[187] SR **831.101**

[188] SR **831.201**

[189] SR **832.102**

Die Verweise in den Absätzen 6 zweiter Satz und 7 erster Satz werden an die Nummerierung des nDSG angepasst.

Art. 59a Abs. 7

Der Begriff «Beauftragte» wird durch «Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter» und «EDÖB» ersetzt.

Art. 59a[ter] *Abs. 1*

Der Verweis auf die Artikel 21 und 22 VDSG wird durch die Artikel 1–4 und 6 DSV ersetzt, da die Regelung der Datensicherheit im 1. Abschnitt als Einheit zu betrachten ist. Die Bestimmungen zur Auftragsbearbeitung gelten im Rahmen ihres Geltungsbereichs ohnehin.

7.122 Verordnung vom 20. Dezember 1982[190] über die Unfallversicherung

Art. 72a Abs. 2 zweiter Satz

Der Verweis wird an die DSV angepasst.

7.123 Familienzulagenverordnung vom 31. Oktober 2007[191]

Art. 18h Abs. 1 Bst. a

Der Verweis wird an die DSV angepasst.

7.124 Arbeitslosenversicherungsverordnung vom 31. August 1983[192]

Art. 126 Abs. 1

Siehe die Erläuterungen zu Artikel 58 der Arbeitsvermittlungsverordnung vom 16. Januar 1991 (Ziff. 7.114).

Ausserdem wurde in Artikel 126 Absatz 1 der Begriff «Informationssystem» in der Mehrzahl verwendet, da mehrere Informationssysteme bestehen.

7.125 ALV-Informationssystemeverordnungvom 26. Mai 2021[193]

Art. 2 Abs. 2

Der Verweis wird an das nDSG angepasst.

---

[190] SR **832.202**

[191] SR **836.21**

[192] SR **837.02**

[193] SR **837.063.1**

7.126 Verordnung vom 18. Juni 2021[194] über die konsularischen Informationssysteme des Eidgenössischen Departements für auswärtige Angelegenheiten

Ingress

Aufgrund der Änderungen im RVOG (Ziff. 13 Anhang 1/II nDSG) stützt sich die Verordnung neu auf Artikel 57*h*^{ter} RVOG. Der Ingress wird entsprechend angepasst.

Art. 25 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.127 GUB/GGA-Verordnung vom 28. Mai 1997[195]

Art. 19 Abs. 2 Bst. d Ziff. 4, 21b Abs. 2 Bst. d

Der Verweis wird an das nDSG angepasst.

7.128 Bio-Verordnung vom 22. September 1997[196]

Art. 33 Bst. c Ziff. 6

Der Verweis wird an das nDSG angepasst.

7.129 Berg- und Alp-Verordnung vom 25. Mai 2011[197]

Art. 11 Abs. 1 Bst. d Ziff. 4

Der Verweis wird an das nDSG angepasst.

7.130 Verordnung vom 3. November 2021[198] über die Identitas AG und die Tierverkehrsdatenbank

Art. 4 Sachüberschrift und Abs. 4

Im französischen Text wird der Begriff «fichiers» wird durch «ensembles de données» ersetzt.

7.131 Verordnung vom 27. April 2022[199] über Informationssysteme des BLV für die Lebensmittelkette

Art. 25 Bst. a

Der Verweis wird an das nDSG angepasst.

---

[194] SR **852.12**

[195] SR **910.12**

[196] SR **910.18**

[197] SR **910.19**

[198] SR **916.404.1**

[199] SR **916.408**

7.132 Verordnung vom 18. November 2015[200] über die Ein-, Durch- und Ausfuhr von Tieren und Tierprodukten im Verkehr mit Drittstaaten

Art. 102d zweiter Satz

Der Begriff «Betriebsreglement» wird durch «Bearbeitungsreglement» ersetzt.

Art. 102e

Der Verweis wird an das nDSG angepasst. Absatz 2 verweist für die Form des Auskunftsbegehrens neu auf Artikel 16 DSV.

7.133 Verordnung vom 26. Juni 2013[201] über die Meldepflicht und die Nachprüfung der Berufsqualifikationen von Dienstleistungserbringerinnen und -erbringern in reglementierten Berufen

Gliederungstitel vor Art. 9 und Art. 9 Abs. 1

Der Begriff «Datensammlung» wird durch «Datenbearbeitung» und «sammelt» durch «beschafft» ersetzt.

7.134 Verordnung vom 24. Juni 2015[202] über die im Ausland erbrachten privaten Sicherheitsdienstleistungen

Art. 12 Abs. 1 Einleitungssatz, Abs. 3 Einleitungssatz und 4

Die Änderungen in den Absätzen 1 und 3 betreffen nur die deutsche Fassung. Der Begriff «Daten über administrative und strafrechtliche Verfolgungen und Sanktionen» wird entsprechend Artikel 5 Buchstabe c Ziffer 5 nDSG durch «Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen» ersetzt. In Absatz 4 wird der Verweis an das nDSG angepasst.

7.135 Verordnung vom 12. August 2015[203] über das Datenbearbeitungssystem private Sicherheitsdienstleistungen

Ingress

Aufgrund der Änderungen im RVOG (Ziff. 13 Anhang 1/II nDSG) stützt sich die Verordnung neu auf Artikel 57*h*^{ter} RVOG. Der Ingress wird entsprechend angepasst.

Art. 9 Abs. 1 Bst. a

Der Verweis wird an das nDSG angepasst.

---

200 SR **916.443.10**

201 SR **935.011**

202 SR **935.411**

203 SR **935.412**

Art. 10 Abs. 2

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

7.136 Geldspielverordnung vom 7. November 2018[204]

Art. 73 Abs. 3

Der Verweis wird an das nDSG angepasst.

7.137 Sprengstoffverordnung vom 27. November 2000[205]

Gliederungstitel 9a, Art. 117a, 117b, 117f Abs. 2 Einleitungssatz

In der französischen Fassung wird der Begriff «fichier électronique» durch «banque de données» ersetzt.

Art. 117g zweiter Satz

Wie gemäss Artikel 4 Absatz 5 DSV sind die Protokolle getrennt vom System, in dem die Personendaten bearbeitet werden, aufzubewahren.

Art. 117i, 117j Abs. 1 Bst. a und 117k

Der Verweis wird an das nDSG angepasst. Der Begriff «fichier» wird in der französischen Fassung in Artikel 117*i* gestrichen.

Anhang 14 Ziff. 13 Sachüberschrift und Abs. 1

In der französischen Fassung wird der Begriff «fichier» durch «registre» ersetzt.

7.138 Verordnung vom 25. August 2004[206] über die Meldestelle für Geldwäscherei

Art. 13 Abs. 1 Bst. a

Die Formulierung wurde angepasst, da Artikel 13 Absatz 2 ZentG keine Voraussetzungen mehr enthält, sondern auf die Vorgaben im StGB verweist.

Art. 19 Abs. 1 Bst. a, 26 Abs. 1 dritter Satz

Der Verweis wird an das nDSG angepasst. In Artikel 26 Absatz 1 dritter Satz wird der Ausdruck «Bundesamt» ausserdem durch «Staatssekretariat» ersetzt.

Art. 25 Abs. 1 erster Satz

Die Bestimmung wird entsprechend der Vorgabe in Artikel 29 DSV um die «Vollständigkeit» ergänzt.

---

[204] SR **935.511**

[205] SR **941.411**

[206] SR **955.23**