Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht

Totalrevision des Datenschutzgesetzes: Häufig gestellte Fragen

Datum: Februar 2024

Aktenzeichen: 212.9-754/50/4

Das totalrevidierte Datenschutzgesetz (DSG; SR 235.1; Inkrafttreten: 1. September 2023) passt den Datenschutz an die technologischen Entwicklungen und die europäischen Standards an. Im vorliegenden Dokument werden verschiedene grundsätzliche Fragen zusammengestellt, deren Beantwortung durch das Bundesamt für Justiz (BJ) zu einem besseren Verständnis des neuen Gesetzes und des dazugehörigen Ausführungsrechts beitragen und die Umsetzungsarbeiten für private Datenbearbeiter und Bundesorgane erleichtern soll.

Die Fragen und Antworten orientieren sich an der Struktur des Datenschutzgesetzes. Die Antworten stützen sich insbesondere auf die Botschaft des Bundesrates vom 15. September 2017 zur Totalrevision des DSG sowie die Erläuterungen des BJ vom 31. August 2022 zur Verordnung über den Datenschutz (DSV; SR 235.11; Inkrafttreten: 1. September 2023). Ein besonderes Augenmerk liegt aber auch auf jenen Bestimmungen, die erst im Rahmen der parlamentarischen Beratung in das neue DSG aufgenommen worden sind und zu denen deshalb bislang nur wenig Materialien bestehen (z.B. betreffend den Begriff des Profilings mit hohem Risiko oder die Vertretungspflicht für private Verantwortliche mit Sitz oder Wohnsitz im Ausland).

Das vorliegende Dokument ersetzt die «FAQ Datenschutzrecht» des BJ vom 1. Februar 2023. Es wird fortlaufend aktualisiert und ergänzt.

Inhaltsverzeichnis

1. Geltungsbereich des DSG

1.1 Persönlicher und sachlicher Geltungsbereich

1.1.1 **Frage**: *Für wen gilt das DSG (persönlicher Geltungsbereich)?*

Das DSG findet Anwendung, wenn *private Personen* oder *Bundesorgane* Personendaten bearbeiten (Art. 2 Abs. 1 DSG). Bundesorgane sind Behörden oder Dienststellen des Bundes oder Personen, die mit öffentlichen Aufgaben des Bundes betraut sind (Art. 5 Bst. i DSG). Der Begriff der privaten Personen ist im DSG dagegen nicht definiert. Hier ist insbesondere an Unternehmen oder natürliche Personen zu denken (soweit diese nicht in Erfüllung einer öffentlichen Aufgabe Daten bearbeiten).

Die Datenbearbeitung durch *kantonale* (und *kommunale*) *Behörden* untersteht nicht dem DSG, sondern dem kantonalen Datenschutzrecht. Dies gilt unabhängig davon, ob die kantonalen Behörden Personendaten direkt beschaffen oder über einen Online-Zugriff auf eine Datenbank des Bundes abrufen. Die Bearbeitung von Daten durch kantonale Organe beim Vollzug von Bundesrecht untersteht grundsätzlich ebenfalls dem kantonalen Recht. In einigen Bereichen, für die der Bund zuständig ist, besteht eine besondere Datenschutzregelung, die – zum Beispiel im Sozialversicherungswesen – sowohl für die zuständigen Bundesbehörden wie auch für die mit dem Vollzug des Bundesrechts beauftragten kantonalen Behörden anwendbar ist. Allerdings hat der Bund dabei auf das kantonale Organisationsrecht Rücksicht zu nehmen.

Verweise: Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 S. 6953 und 7011 (nachfolgend: «Botschaft zur Totalrevision des DSG»); Bericht des Bundesrates vom 22. Dezember 2010 «Austausch personenbezogener Daten zwischen Behörden des Bundes und der Kantone» in Erfüllung des Postulates Lustenberger 07.3682, BBl 2011 645.

1.1.2 **Frage**: *Welche Daten werden vom DSG geschützt (sachlicher Geltungsbereich)?*

Mit der Totalrevision des DSG wird die Bearbeitung von Daten juristischer Personen vom sachlichen Anwendungsbereich des Datenschutzgesetzes ausgenommen. Das DSG gilt nur noch für die Bearbeitung von Daten *natürlicher Personen* (= Personendaten). Es berechtigt also nur natürliche, nicht aber juristische Personen (Art. 2 Abs. 1 DSG e contrario).

Juristische Personen bleiben über andere Bestimmungen der schweizerischen Rechtsordnung geschützt. So gelten für sie namentlich der Persönlichkeitsschutz gemäss Zivilgesetzbuch (Art. 28 ff. ZGB; SR 210), das Bundesgesetz gegen den unlauteren Wettbewerb (UWG; SR 241), das Urheberrechtsgesetz (URG; SR 231.1) oder die Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen. Ausserdem wird die Privatsphäre der juristischen Personen durch Artikel 13 der Bundesverfassung (BV; SR 101) gewährleistet. Das bedeutet insbesondere, dass Bundesorgane bei der Bearbeitung oder Bekanntgabe von Daten juristischer Personen eine genügende gesetzliche Grundlage benötigen. Mit der Totalrevision des DSG werden deshalb im Regierungs- und Verwaltungsorganisationsgesetz eine Reihe von neuen Bestimmungen eingeführt, welche den Umgang mit Daten juristischer Personen durch Bundesorgane regeln (Art. 57*r* ff. RVOG; SR 172.010). Des Weiteren verhindert die Übergangsbestimmung in Artikel 71 DSG während fünf Jahren mögliche Rechtslücken.

Keine Anwendung findet das DSG auf Sachdaten. Auch anonymisierte Daten sind (nach der Anonymisierung) keine Personendaten mehr und fallen demzufolge nicht in den Geltungsbereich des DSG.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7011 f.; Aktennotiz des BJ von Oktober 2022 zu den wichtigsten Änderungen der Totalrevision des DSG für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane (nachfolgend: «Aktennotiz des BJ über die Totalrevision des DSG), S. 26 ff.

1.1.3 **Frage**: *Welche Ausnahmen vom persönlichen und sachlichen Geltungsbereich sieht das DSG vor?*

Gemäss Artikel 2 Absatz 2 ist das DSG nicht anwendbar auf:

- Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden (Bst. a);
- Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden (Bst. b);
- Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007 (SR 192.12), die in der Schweiz Immunität von der Gerichtsbarkeit geniessen (Bst. c).

  Beispiel: IKRK.

Für *Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren* (ohne erstinstanzliche Verwaltungsverfahren) regelt Artikel 2 Absatz 3 DSG das Verhältnis zwischen Verfahrensrecht und Datenschutzgesetz: Demgemäss bestimmt das jeweils anwendbare Verfahrensrecht darüber, wie Personendaten bearbeitet werden und die Rechte der betroffenen Personen ausgestaltet sind, wenn ein unmittelbarer Zusammenhang zu einem Verfahren besteht. Dabei stellt das Verfahrensrecht den Schutz der Persönlichkeit und der Grundrechte aller Beteiligten sicher. Zu den Ausnahmen von der Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vgl. Artikel 4 Absatz 2 Buchstabe c–e DSG.

Für die *öffentlichen Register des Privatrechtsverkehrs*, die von *Bundesbehörden* geführt werden, sieht Artikel 2 Absatz 4 DSG vor, dass diese Register durch die Spezialbestimmungen des anwendbaren Bundesrechts geregelt werden. Dies gilt insbesondere für den Zugang zu den Registern und die Rechte der betroffenen Personen. Enthalten die Spezialbestimmungen keine Regelung, so ist das DSG anwendbar. Die Register unterstehen im totalrevidierten DSG neu der Aufsicht des EDÖB (Art. 4 Abs. 1 DSG). Betroffen sind das elektronische Zivilstandsregister, Zefix, das Luftfahrzeugbuch des Bundesamts für Zivilluftfahrt und die Register des Eidgenössischen Instituts für Geistiges Eigentum (insbesondere das Marken-, das Patent- und das Designregister).

Die öffentlichen Register des Privatrechtsverkehrs, für welche die *Kantone* zuständig sind, unterstehen dagegen dem kantonalen Datenschutzrecht (vgl. dazu die Frage 1.1.1). Dies gilt auch, wenn Personendaten im Rahmen des Vollzugs von Bundesrecht bearbeitet werden. Allerdings darf das kantonale Datenschutzrecht die korrekte und einheitliche Anwendung des Bundesprivatrechts und insbesondere den Grundsatz der Öffentlichkeit der Register nicht behindern. Zu den kantonalen Registern gehören das Grundbuch, das Schiffsregister, die kantonalen Handelsregister, die Betreibungs- und Konkursregister sowie das öffentliche Register über die Eigentumsvorbehalte.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7012 ff.

1.2 Räumlicher Geltungsbereich

Frage: *Was ist der räumliche Geltungsbereich des DSG?*

Das Parlament hat im Rahmen der Totalrevision des DSG in Artikel 3 neu eine ausdrückliche Regelung zum räumlichen Geltungsbereich aufgenommen. Dabei ist zu unterscheiden:

- Für die *privatrechtlichen* und *strafrechtlichen Datenschutzbestimmungen* verweist Artikel 3 Absatz 2 DSG deklaratorisch auf die schon heute vorhandenen Kollisionsnormen im Bundesgesetz über das Internationale Privatrecht (Art. 139 IPRG; SR 291) und im Strafgesetzbuch (Art. 3 ff. StGB; SR 311.0).

- Für die *öffentlich-rechtlichen Datenschutzbestimmungen*, zu welchen auch die Aufsicht durch den EDÖB gehört, hält Artikel 3 Absatz 1 DSG fest, dass das Datenschutzgesetz für Sachverhalte gilt, die sich in der Schweiz auswirken, selbst wenn sie im Ausland veranlasst werden. Auch dies ist an sich nichts Neues. Bereits heute sind gemäss der Rechtsprechung die öffentlich-rechtlichen Datenschutznormen auf internationale Sachverhalte anwendbar, wenn ein überwiegender Anknüpfungspunkt zur Schweiz besteht. Es handelt sich hier also um eine Kodifizierung der Gerichtspraxis zum Territorialitäts- und Auswirkungsprinzip im öffentlichen Recht.

Verweise: BGE 138 II 346 E. 3.3.

2. Begriffe

2.1 Personendaten und besonders schützenswerte Personendaten

2.1.1 **Frage**: *Was sind Personendaten?*

Bei Personendaten handelt es sich um alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Art. 5 Bst. a DSG). Daten juristischer Personen werden vom totalrevidierten DSG hingegen nicht mehr erfasst (vgl. dazu eingehend Frage 1.1.2).

Im Übrigen entspricht der Begriff der «Personendaten» aber grundsätzlich dem bisherigen Recht. Eine natürliche Person ist bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, beispielsweise über den Hinweis auf Informationen, die sich aus den Umständen oder dem Kontext ableiten lassen (Identifikationsnummer, Standortdaten, spezifische Aspekte, welche die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder gesellschaftliche Identität betreffen). Die Identifizierung kann über eine einzige Information möglich sein (Telefonnummer, Hausnummer, AHV-Nummer, Fingerabdrücke) oder über den Abgleich verschiedener Informationen (Adresse, Geburtsdatum, Zivilstand). Die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, reicht nicht aus, um anzunehmen, dass eine Person bestimmbar sei. Ist der Aufwand für die Bestimmung der betroffenen Personen derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent oder eine Interessentin diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Ob der Einsatz dieser Mittel vernünftig ist, muss mit Blick auf die Umstände, etwa den zeitlichen und finanziellen Aufwand für die Identifizierung, beurteilt werden. Dabei sind die zum Zeitpunkt der Bearbeitung verfügbaren Technologien und deren Weiterentwicklung zu berücksichtigen.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7019; BGE 136 II 508.

2.1.2 **Frage**: *Was sind besonders schützenswerte Personendaten?*

Der Begriff der besonders schützenswerten Personendaten wird in Artikel 5 Buchstabe c DSG abschliessend definiert. Wie bisher handelt es sich dabei um Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten (Ziff. 1), Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse (Ziff. 2), Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (Ziff. 5) sowie Daten über Massnahmen der sozialen Hilfe (Ziff. 6).

Neu gehören im totalrevidierten DSG folgende Kategorien zu den besonders schützenswerten Personendaten:

- *Daten über die Zugehörigkeit zu einer Ethnie (Art. 5 Bst. c Ziff. 2 DSG):* In Anlehnung an die Rechtsprechung des Bundesgerichts zu Art. 261bis StGB ist eine Ethnie «ein Segment der Bevölkerung, das sich selbst als abgegrenzte Gruppe versteht und das vom Rest der Bevölkerung als Gruppe verstanden wird. Sie muss eine gemeinsame Geschichte sowie ein gemeinsames zusammenhängendes System von Einstellungen und Verhaltensnormen (Tradition, Brauchtum, Sitte, Sprache etc.) haben, wobei die genannten Merkmale zur Abgrenzung verwendet werden müssen»[1].

  Beispiele: Kosovo-Albaner, Araber, Palästinenser oder Fahrende.[2]

- *Genetische Daten (Art. 5 Bst. c Ziff. 3 DSG):* Genetische Daten sind Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden. Diese Definition entspricht Artikel 3 Buchstabe k des Bundesgesetzes über genetische Untersuchungen beim Menschen (GUMG; SR 810.12).

  Beispiel: DNA-Profil.

- *biometrische Daten, die eine natürliche Person eindeutig identifizieren (Art. 5 Bst. c Ziff. 4 DSG):* Unter biometrischen Daten i.S.v. Artikel 5 Buchstabe c Ziffer 4 DSG sind Personendaten zu verstehen, die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen. Anders als bei genetischen Daten ist bei biometrischen Daten der technische Prozess, der die eindeutige Identifizierung der betroffenen Person ermöglicht, fester Bestandteil der Qualifikation als besonders schützenswerte Daten. Ohne diese Einschränkung wären sonst auch gewöhnliche Fotografien oder Tonaufnahmen besonders geschützt.

  Beispiele: Gesichtsbilder, die mit einer Gesichtserkennungssoftware bearbeitet werden, Fingerabdruck-, Iris- und Retinascans.

Die Bearbeitung von besonders schützenswerten Personendaten ist nicht verboten. Sie untersteht aber strengeren Anforderungen als andere Datenbearbeitungen, indem zum Beispiel höhere Anforderungen an eine allfällige Einwilligung gestellt werden (Art. 6 Abs. 7 Bst. a DSG), für Bundesorgane in der Regel eine Grundlage in einem Gesetz im formellen Sinn erforderlich ist (Art. 34 Abs. 2 Bst. a und Art. 36 Abs. 1 DSG) oder bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten grundsätzlich eine Datenschutz-Folgenabschätzung zu erstellen ist (Art. 22 Abs. 2 Bst. a DSG).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7020; Aktennotiz des BJ über die Totalrevision des DSG, S. 10 f.

---

1 BGE 143 IV 193 E. 2.3.

2 Diese Beispiele stammen aus FABIENNE ZANNOL, Die Anwendung der Strafnorm gegen Rassendiskriminierung (Studie im Auftrag der EKR), Bern 2007.

2.1.3 **Frage**: *Sind alle genetischen Daten besonders schützenswerte Personendaten?*

Wie im bisherigen Recht werden auch vom totalrevidierten DSG nur diejenigen Daten erfasst, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 5 Bst. a DSG; vgl. Frage 2.1.1). Das bedeutet: Bei genetischen Daten handelt es sich nur dann um besonders schützenswerte Personendaten, wenn sie Angaben enthalten, mit denen sich eine betroffene Person mit verhältnismässigem Aufwand identifizieren lässt. Trifft dies nicht zu, fallen die genetischen Daten nicht in den Anwendungsbereich des DSG. Auch auf anonymisierte Daten findet das DSG keine Anwendung, wenn eine Re-Identifikation durch einen Dritten nicht mehr möglich ist.

Verweise: AB 2019 N 1787 (Votum der Departementsvorsteherin des EJPD zur Beratung der Totalrevision des DSG im Nationalrat am 24. September 2019).

2.2 Datenbearbeitung

2.2.1 **Frage**: *Was gilt als «Bearbeiten» von Personendaten?*

Gemäss Artikel 5 Buchstabe d DSG ist unter «Bearbeiten» jeder Umgang mit Personendaten zu verstehen, unabhängig von den angewandten Mitteln und Verfahren, wie insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten. Der Begriff ist technologieneutral definiert und umfasst sowohl die automatisierte als auch die nichtautomatisierte (manuelle) Datenbearbeitung.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7021.

2.2.2 **Frage**: *Was ist eine «automatisierte» Datenbearbeitung?*

Die «automatisierte» Datenbearbeitung wird im DSG nicht definiert. Verschiedene Bestimmungen des DSG bzw. der DSV beziehen sich aber ausdrücklich darauf (z.B. Art. 5 Bst. f DSG betreffend den Begriff des Profilings, Art. 28 betreffend das Recht auf Datenherausgabe oder -übertragung, Art. 35 DSG betreffend Pilotversuche, Art. 4 Abs. 1 und 2 DSV betreffend Protokollierung oder Art. 5 und 6 DSV betreffend Bearbeitungsreglement). Die automatisierte Datenbearbeitung ist dabei als Gegenstück zur manuellen (bzw. analogen) Bearbeitung (z.B. dem Erstellen einer handschriftlichen Gesprächsnotiz im Rahmen eines Vorstellungsgesprächs) zu verstehen. Sie umfasst jegliche elektronisch durchgeführten Bearbeitungen (z.B. mit Hilfe von Computern, Smartphones, Tablets oder Kameras). Nicht vorausgesetzt ist, dass die Bearbeitung vollautomatisiert – d.h. ohne menschliches Zutun – erfolgt, wie es der Begriff der automatisierten Einzelentscheidung im Sinne von Artikel 21 DSG verlangt (vgl. dazu die Frage 6.2.1).

2.3 Profiling

2.3.1 **Frage***: Was bedeutet «Profiling»?*

Mit der Totalrevision des DSG wird der bisherige Begriff des «Persönlichkeitsprofils» (Art. 3 Bst. d aDSG) durch das «Profiling» (Art. 5 Bst. f DSG) abgelöst. Obwohl die beiden Begriffe Ähnlichkeiten aufweisen, sind sie nicht deckungsgleich. Das Persönlichkeitsprofil ist das Ergebnis eines Bearbeitungsprozesses (= Zusammenstellung von Daten, aus welcher sich ein Bild über wesentliche [Teil-]Aspekte einer natürlichen Person ergibt) und erfasst damit etwas Statisches. Als Profiling gilt dagegen eine bestimmte Art bzw. Methode der Datenbearbeitung (= automatisierte Bewertung bestimmter Aspekte einer natürlichen Person). Es handelt sich dabei mithin um einen dynamischen Prozess.

Als Profiling gilt gemäss Artikel 5 Buchstabe f DSG jede Art der automatisierten Bearbeitung von Personendaten, mit welcher bestimmte persönliche Aspekte einer natürlichen Person

bewertet werden. Das heisst: Es werden z.B. Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person analysiert oder vorhergesagt. Vereinfacht ausgedrückt, geht es beim Profiling um eine Art Einschätzung oder Beurteilung einer Person. Dabei kann es sich um die Analyse von Persönlichkeitsmerkmalen, aber auch um eine Prognose über zukünftige Verhaltensweisen oder Eigenschaften einer Person handeln.

Kein Profiling ist die objektive Feststellung eines Sachverhalts. Auch eine einfache Einteilung von Personen anhand bekannter Merkmale wie Alter, Geschlecht und Grösse führt nicht zu einem Profiling, solange keine Vorhersagen über einzelne Personen getroffen oder Schlussfolgerungen über einzelne Personen gezogen werden.

Die Datenbearbeitung, insbesondere der Bewertungsprozess, erfolgt beim Profiling automatisiert. Anders als beim Begriff der automatisierten Einzelentscheidung (siehe Frage 6.2.1) muss die Datenbearbeitung beim Profiling aber nicht vollständig automatisiert sein. Das Eingreifen eines Menschen schliesst eine Aktivität nicht von der Profiling-Definition aus, solange die Datenbearbeitung im Wesentlichen automatisiert abläuft.

Beispiele[3]:

- *Bewertung der wirtschaftlichen Lage bzw. der Kreditwürdigkeit*: Das Kreditscoring ist ein mathematisch-statistisches Verfahren zur Einschätzung der Kreditwürdigkeit (Zahlungsfähigkeit und Zahlungswilligkeit) einer Person. In das Kreditscoring fliessen beispielsweise Angaben über Betreibungsauskünfte, Verlustscheine, Sperrungen von Bank- und Kreditkarten aufgrund von Zahlungsrückständen, Kreditgesuche, Zahlungs- und Inkassoverfahren oder Erfahrungen aus bisherigen Geschäftsbeziehungen ein. Dabei wird der betroffenen Person eine Bonitätsnote (Score) zugeordnet. Dieser Kreditscore wird z.B. eingesetzt, um über die Gewährung eines Darlehens oder die Zahlungsmodalitäten (Kauf auf Rechnung) zu entscheiden. Erfolgt das Kreditscoring automatisiert (und nicht manuell), liegt ein Profiling vor.
- *Bewertung der Gesundheit*: Werden mit einem Fitness-Tracker lediglich Schritte gezählt, findet grundsätzlich noch keine Bewertung der Gesundheit einer Person und damit auch kein Profiling statt. Wird die Schrittzählung jedoch mit anderen Daten angereichert, wie z.B. Grösse, Gewicht, Geschlecht, Ernährungsverhalten, Schlafrhythmus oder GPS-Daten, können Aussagen über den Gesundheitszustand getroffen werden. Eine solche (automatisierte) Analyse der Gesundheit stellt ein Profiling dar.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7021 f.; Aktennotiz des BJ über die Totalrevision des DSG, S. 12 ff.

2.3.2 **Frage**: *Wann liegt ein «Profiling mit hohem Risiko» vor?*

Der Begriff des Profilings mit hohem Risiko wurde in der parlamentarischen Beratung zur Totalrevision des DSG eingeführt. Das Parlament hat sich für einen risikobasierten Ansatz ausgesprochen: Danach soll bei privaten Datenbearbeitern nicht jedes Profiling, sondern nur ein «Profiling mit hohem Risiko» zu qualifizierten Rechtsfolgen führen. Für Bundesorgane hat die Unterscheidung zwischen dem «gewöhnlichen» Profiling und dem Profiling mit hohem Risiko dagegen eine geringere Tragweite (vgl. dazu Frage 2.3.3)

Als «Profiling mit hohem Risiko» gilt gemäss Artikel 5 Buchstabe g DSG ein Profiling, «das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt». Die Umschreibung des hohen Risikos in Artikel 5 Buchstabe g DSG orientiert sich am bisherigen Begriff des «Persönlichkeitsprofils» nach

[3] Die Beispiele stammen aus Olivier Heuberger, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, Diss. Luzern, 2020 (Rz. 157 ff.).

Artikel 3 Buchstabe d aDSG. Damit bleibt auch die Rechtsprechung zum Persönlichkeitsprofil (insbesondere das Leiturteil des Bundesverwaltungsgerichts A-4232/2015 vom 18. April 2017) massgebend.

Mit anderen Worten liegt ein Profiling mit hohem Risiko dann vor, wenn das Profiling ein Persönlichkeitsprofil nach bisherigem Datenschutzgesetz zum Ergebnis hat. Es werden also Datenbearbeitungsmethode (Profiling) und Resultat der Datenbearbeitung (Persönlichkeitsprofil) kombiniert. Diese Legaldefinition berücksichtigt, dass eine Vielzahl (auch nicht besonders schützenswerter) Daten durch ein Profiling zu einem Bild über die betroffene Person verknüpft werden, das als solches ein erhöhtes Risiko für die Persönlichkeits- und Grundrechte mit sich bringt. Die betroffene Person hat häufig keinen Einfluss auf dieses Bild und kann weder dessen Richtigkeit noch Verwendung kontrollieren.

Beispiele:

- Durch das integrierte GPS lässt sich grundsätzlich jedes Smartphone bis auf wenige Meter genau lokalisieren. Die Bewegungsdaten des Smartphones können automatisiert ausgewertet werden, um Rückschlüsse über dessen Inhaberin oder Inhaber zu gewinnen. Werden diese Daten lediglich über einen beschränkten Zeitraum und einen bestimmten Ort (z.B. kurzer Aufenthalt in einem Bahnhof) analysiert, so liegt normalerweise nur ein «gewöhnliches» Profiling vor. Werden die Bewegungsdaten hingegen über längere Zeit und in einem grösseren geographischen Umfang ausgewertet, so lassen sich Rückschlüsse auf verschiedenste Lebensbereiche einer Person gewinnen. Dies gilt etwa für den Arbeitsort, die Wohnsituation, die Essgewohnheiten, persönliche Beziehungen, allfällige Arztbesuche oder das Konsumverhalten. So entsteht ein Bild über die Person, das eines besonderen Schutzes bedarf. In diesem Fall wäre ein Profiling mit hohem Risiko anzunehmen.
- Ein Profiling zur Prüfung der Kreditwürdigkeit, bei welchem nicht nur Daten zur wirtschaftlichen Situation bzw. zur Zahlungsfähigkeit einer Person, sondern auch Daten zu weiteren Aspekten der Persönlichkeit (wie die private Wohn- und Lebenssituation) herangezogen werden, ist als Profiling mit hohem Risiko zu qualifizieren (vgl. unter bisherigem Recht das Urteil des Bundesverwaltungsgerichts A-4232/2015 vom 18. April 2017).

In der Praxis kann ein Profiling auch aus anderen Gründen zu schwerwiegenden Eingriffen in die Persönlichkeit oder Grundrechte der betroffenen Personen führen. Zu denken ist etwa an das Profiling von minderjährigen und anderen besonders schutzbedürftigen Personen oder an ein Profiling, das zur Verweigerung einer wichtigen Leistung führen kann. Diese Risiken sind z.B. bei der Erstellung einer Datenschutz-Folgenabschätzung nach Artikel 22 DSG (vgl. Frage 6.3.2) mitzuberücksichtigen.

Verweise: Aktennotiz des BJ über die Totalrevision des DSG, S. 15 f.

2.3.3 **Frage**: *Welche Rechtsfolgen sind bei einem Profiling bzw. einem Profiling mit hohem Risiko zu beachten?*

Für private Datenbearbeiter gelten bei der Durchführung eines Profilings mit hohem Risiko strengere Rechtsfolgen als bei anderen Datenbearbeitungen. So gelten beispielsweise höhere Anforderungen an eine allfällige Einwilligung (Art. 6 Abs. 7 Bst. b DSG). Auch muss bei einem geplanten Profiling mit hohem Risiko grundsätzlich eine Datenschutz-Folgenabschätzung erstellt werden (vgl. Art. 22 Abs. 1 und 2 DSG; Frage 6.3.2). Für Bundesorgane kommen strengere Rechtsfolgen schon bei einem «gewöhnlichen» Profiling zum Zug. Insbesondere sind sie grundsätzlich nur dann zu einem Profiling befugt, wenn dies in einer formell-gesetzlichen Grundlage vorgesehen ist (Art. 34 Abs. 2 Bst. b DSG).

2.3.4 **Frage**: *Brauchen private Datenbearbeiter für die Durchführung eines Profilings immer eine Einwilligung? Und wie verhält es sich beim Profiling durch Bundesorgane?*

Wie jede andere Art der Datenbearbeitung ist Profiling für *private Datenbearbeiter* grundsätzlich erlaubt, es sei denn, die Datenbearbeitung führe zu einer widerrechtlichen Persönlichkeitsverletzung (Art. 30 Abs. 1 DSG). Dabei gehört das Profiling nicht zu den Arten der Datenbearbeitung, welche das DSG per se als persönlichkeitsverletzend bezeichnet (Art. 30 Abs. 2 DSG e contrario). Führt ein Profiling aber im konkreten Anwendungsfall zu einer Persönlichkeitsverletzung, weil es die Persönlichkeitsrechte der betroffenen Person mit einer gewissen Intensität beeinträchtigt, kann es durch Einwilligung, überwiegende private oder öffentliche Interessen oder durch Gesetz gerechtfertigt sein (Art. 31 Abs. 1 DSG). Es ist also selbst bei einem persönlichkeitsverletzenden Profiling nicht immer eine Einwilligung erforderlich. Stattdessen können alle genannten Rechtfertigungsgründe zur Anwendung gelangen. Als Rechtfertigungsgrund käme insbesondere auch ein überwiegendes privates oder öffentliches Interesse in Frage (siehe unter anderem Art. 31 Abs. 2 DSG). So könnte z.B. die Betrugsbekämpfung als berechtigtes Interesse für ein Profiling vorgebracht werden, wenn es im Einzelfall die entgegenstehenden Interessen der betroffenen Person überwiegt.

Wird als Rechtfertigungsgrund für ein persönlichkeitsverletzendes Profiling die Einwilligung der betroffenen Person herangezogen, muss diese den Anforderungen von Artikel 6 Absatz 6 DSG bzw. im Fall eines Profilings mit hohem Risiko den Anforderungen von Artikel 6 Absatz 7 Buchstabe b DSG genügen (vgl. zu den Anforderungen an die Einwilligung die Frage 3.4.2).

Anders als private Personen dürfen *Bundesorgane* als Folge des Legalitätsprinzips Personendaten grundsätzlich nicht ohne gesetzliche Grundlage bearbeiten (Art. 34 Abs. 1 DSG). Beim Profiling verlangt Artikel 34 Absatz 2 Buchstabe b DSG sogar eine Grundlage in einem Gesetz im formellen Sinn. Fehlt eine gesetzliche Grundlage für die Datenbearbeitung bzw. das Profiling, sieht das DSG eine Reihe von Ausnahmen vor. Dazu gehört auch die Einwilligung der betroffenen Person im Einzelfall (Art. 34 Abs. 4 Bst. b DSG). Der Einwilligung kommt bei Datenbearbeitungen durch Bundesorgane also eine deutliche geringere Bedeutung zu als im privatrechtlichen Bereich. Denn werden Personendaten regelmässig oder dauerhaft bearbeitet, kann dies nicht durch die Einwilligung der betroffenen Personen gerechtfertigt werden. Vielmehr müssen die notwendigen gesetzlichen Grundlagen geschaffen werden.

3. (Ausgewählte) Grundsätze

3.1 Grundsatz der Transparenz bzw. der Erkennbarkeit

Frage: *Was bedeutet der Grundsatz der Transparenz bzw. Erkennbarkeit?*

Der Grundsatz der Transparenz bzw. der Erkennbarkeit ergibt sich aus Artikel 6 Absatz 3 DSG. Auch wenn der Wortlaut dieser Bestimmung vom bisherigen Recht (Art. 4 Abs. 4 aDSG) etwas abweicht, sind damit – wie in der Botschaft des Bundesrates zur Totalrevision des DSG erläutert– keine materiellen Änderungen beabsichtigt. Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein. Dies ist grundsätzlich der Fall, wenn die betroffene Person informiert wird, die Bearbeitung gesetzlich vorgesehen oder aus den Umständen klar ersichtlich ist.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7024 f.

3.2 Grundsatz der Zweckbindung

Frage: *Was ist das Zweckbindungsprinzip?*

Der Grundsatz der Zweckbindung wird in Artikel 6 Absatz 3 DSG leicht anders formuliert als im bisherigen Recht (Art. 4 Abs. 3 aDSG). Insbesondere wird neu ausdrücklich festgehalten, dass Personendaten nur so bearbeitet werden dürfen, dass es mit dem anfänglichen Zweck, zu welchem sie beschafft worden sind, vereinbar ist. Diese neue Formulierung bringt allerdings keine wesentlichen Änderungen mit sich: Wie bereits heute verstösst eine Weiterbearbeitung von Personendaten gegen den Zweckbindungsgrundsatz, wenn die betroffene Person dies berechtigterweise als unerwartet, unangebracht oder beanstandbar erachten kann.

Beispiele:

- Nicht mit dem anfänglichen Zweck vereinbar ist es, Adressen, die beim Unterschriftensammeln für eine politische Kampagne erfasst worden sind, zu Werbezwecken weiterzuverwenden.
- Übermittelt die betroffene Person ihre Adresse dagegen im Hinblick auf den Erhalt einer Kundenkarte oder für eine Bestellung, so liegt die Weiterbenutzung dieser Adresse durch das betreffende Unternehmen zu Werbezwecken im Rahmen einer anfänglich erkennbaren Zweckbestimmung und kann als mit dem anfänglichen Zweck vereinbar angesehen werden.[4]

Zulässig ist die Änderung des anfänglichen Zwecks, wenn dies gesetzlich vorgesehen ist, durch eine Gesetzesänderung verlangt wird oder durch einen anderen Rechtfertigungsgrund (z.B. durch die Einwilligung der betroffenen Person) legitimiert ist.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7025.

3.3 Grundsatz der Richtigkeit

Frage: *Was verlangt der Grundsatz der Richtigkeit der Daten?*

Jede Person, die Daten bearbeitet, hat sich über deren Richtigkeit zu vergewissern (Art. 6 Abs. 5 erster Satz DSG). Sie hat alle angemessenen Massnahmen zu treffen, damit die Daten, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind, berichtigt, gelöscht oder vernichtet werden (Art. 6 Abs. 5 zweiter Satz DSG). In Artikel 6 Absatz 5 dritter Satz des totalrevidierten DSG hat das Parlament neu präzisiert, dass die Angemessenheit der zu treffenden Massnahmen namentlich von der Art und dem Umfang der Datenbearbeitung sowie vom Risiko, das die Datenbearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Person mit sich bringt, abhängt. Mit dieser Ergänzung werden die bisherige Lehre und Praxis (insbesondere des Bundesverwaltungsgerichts) zur Datenrichtigkeit ausdrücklich im Gesetz festgehalten. Materiell führt sie aber zu keinen Änderungen.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7026 f.

3.4 Einwilligung

3.4.1 **Frage**: *Braucht es für die Bearbeitung von Personendaten eine Einwilligung der betroffenen Person?*

Die Bearbeitung von Personendaten ist für *private Datenbearbeiter* grundsätzlich ohne Einwilligung der betroffenen Person zulässig. Eine Einwilligung ist nur dort erforderlich, wo sie der Rechtfertigung einer persönlichkeitsverletzenden Datenbearbeitung dient (Art. 30 f. DSG). Dies kann zum Beispiel bei der Bekanntgabe von besonders schützenswerten Personendaten (wie

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

Gesundheitsdaten; vgl. Frage 2.1.2) an Dritte der Fall sein (Art. 30 Abs. 2 Bst. c DSG). Braucht es eine Einwilligung, muss diese die Anforderungen von Artikel 6 Absätze 6 und 7 DSG erfüllen (siehe Frage 3.4.2). Wenn die Einwilligung der betroffenen Person nicht eingeholt werden kann oder die Einwilligung nicht gültig ist oder widerrufen wird, ist eine persönlichkeitsverletzende Datenbearbeitung nicht automatisch unzulässig. Denn auch die anderen Rechtfertigungsgründe können noch geltend gemacht werden. So kann eine gesetzliche Grundlage oder ein überwiegendes privates oder öffentliches Interesse an der persönlichkeitsverletzenden Datenbearbeitung bestehen.

Bei Datenbearbeitungen durch *Bundesorgane* ist die Einwilligung weniger wichtig als im privatrechtlichen Bereich. Hier ist vor allem das Erfordernis der gesetzlichen Grundlage von Bedeutung (Art. 34 ff. DSG). Die Einwilligung kann dagegen nur ausnahmsweise und im Einzelfall Grundlage für eine Datenbearbeitung durch Bundesorgane sein (Art. 34 Abs. 4 Bst. b und Art. 36 Abs. 2 Bst. b DSG).

Zur Bedeutung der Einwilligung beim Profiling vgl. Frage 2.3.4.

3.4.2 **Frage**: *Welche Anforderungen muss eine Einwilligung erfüllen?*

Sofern eine Einwilligung der betroffenen Person erforderlich ist (vgl. dazu Frage 3.4.1), ist sie gemäss Artikel 6 Absatz 6 DSG nur gültig, wenn sie für eine oder mehrere bestimmte Datenbearbeitungen nach angemessener Information freiwillig erteilt wird. Dass das Parlament das im Entwurf des Bundesrates noch vorgesehene Erfordernis der «Eindeutigkeit» der Einwilligung gestrichen hat, bedeutet keine materielle Änderung. Denn schon nach den allgemeinen Grundsätzen der schweizerischen Rechtsordnung muss eine Einwilligung hinreichend bestimmt sein, damit sie gültig ist.

Artikel 6 Absatz 7 DSG regelt diejenigen Konstellationen, in welchen die Einwilligung – wiederum nur, sofern sie erforderlich ist – erhöhte Anforderungen erfüllen und deshalb «ausdrücklich» erteilt werden muss. Dies ist bei der Bearbeitung von besonders schützenswerten Personendaten (Bst. a), beim Profiling mit hohem Risiko durch eine private Person (Bst. b) und beim Profiling durch ein Bundesorgan (Bst. c) der Fall. Ausdrücklich ist eine Einwilligung grundsätzlich dann, wenn sie durch eine aktive Handlung und nicht nur stillschweigend bzw. konkludent erfolgt. Sie muss unmittelbar Klarheit über den Willen der betroffenen Person schaffen.

Beispiele:

- Ausdrücklich sind beispielsweise schriftliche oder mündliche Einwilligungserklärungen, aber auch Gesten wie Kopfnicken oder eindeutige Handzeichen. Im Internetkontext kann eine ausdrückliche Einwilligung ausserdem durch das aktive Anklicken eines Kästchens erteilt werden.
- Nicht ausdrücklich ist dagegen eine konkludente Einwilligung wie etwa die weitere Inanspruchnahme eines Dienstens nach der Mitteilung einer Änderung der Allgemeinen Geschäftsbedingungen.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7027 f.

3.4.3 **Frage**: *Sieht das totalrevidierte Datenschutzgesetz ein Koppelungsverbot vor?*

Die EU hat in Artikel 7 Absatz 4 der Datenschutz-Grundverordnung (vgl. Frage 12.2.1) das sogenannte «Koppelungsverbot» verankert. Das heisst: Wird ein Vertrag von der Einwilligung in eine Datenbearbeitung abhängig gemacht, die für die Vertragserfüllung nicht nötig ist, so wird grundsätzlich davon ausgegangen, dass die Einwilligung nicht freiwillig erfolgt und damit ungültig ist.

Anders als in der EU ist im DSG kein ausdrückliches Koppelungsverbot vorgesehen. Allerdings muss die Einwilligung auch nach schweizerischen Datenschutzrecht freiwillig erteilt werden. Als unfreiwillig gilt eine Einwilligung insbesondere dann, wenn bei einer Verweigerung Nachteile drohen, die keinen Bezug zum Zweck der Datenbearbeitung haben oder unverhältnismässig sind. Damit ist die Stossrichtung des Koppelungsverbots an sich abgedeckt. Auch in der Schweiz sind Koppelungssachverhalte bei der Beurteilung der Freiwilligkeit einer Einwilligung besonders sorgfältig und streng zu prüfen.

Verweise: BGE 138 I 331 E. 7.4.1.

3.5 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Frage: *Was ist unter Datenschutz durch Technik («Privacy by Design») und datenschutzfreundlichen Voreinstellungen («Privacy by Default») zu verstehen?*

Datenschutz durch Technik («Privacy by Design»; Art. 7 Abs. 1 und 2 DSG) bedeutet, dass der Verantwortliche bereits ab dem Zeitpunkt der Planung verpflichtet ist, eine Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden. Mit anderen Worten: Die gesetzlichen Anforderungen an eine datenschutzkonforme Bearbeitung werden technisch so umgesetzt, dass die Gefahr von Verstössen gegen Datenschutzvorschriften reduziert oder ausgeschlossen wird.

Beispiel: Eine Applikation wird technisch so ausgestaltet, dass sie Daten in regelmässigen Abständen löscht oder standardmässig anonymisiert.

Verantwortliche haben zudem die Pflicht, mittels geeigneter Voreinstellungen («Privacy by Default»; Art. 7 Abs. 3 DSG) dafür zu sorgen, dass nur so viele Personendaten bearbeitet werden, wie im Hinblick auf den Verwendungszweck nötig sind, soweit die von der Datenbearbeitung betroffene Person nicht etwas anderes bestimmt.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7028 ff.

3.6 Datensicherheit

3.6.1 Allgemeines

3.6.1.1 **Frage**: *Was ist eine Verletzung der Datensicherheit?*

Gemäss Artikel 8 Absatz 1 DSG müssen die verantwortlichen Datenbearbeiter und Auftragsbearbeiter durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten. Diese Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden (Art. 8 Abs. 2 DSG).

Was unter einer Verletzung der Datensicherheit zu verstehen ist, wird in Artikel 5 Buchstabe h DSG definiert: Es handelt sich dabei um eine «Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden». Massgebend ist dabei alleine, ob der fragliche Vorgang geschieht. Irrelevant für das Vorliegen einer Verletzung der Datensicherheit ist dagegen, ob lediglich die Möglichkeit bestand, dass die Personendaten Unbefugten offengelegt oder zugänglich gemacht wurden, oder ob ein solcher Zugang tatsächlich stattgefunden hat.

Zur Meldepflicht bei Verletzungen der Datensicherheit siehe die Fragen unter Ziff. 6.4.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7022 f. und 7031.

3.6.1.2 **Frage**: *Was müssen die verantwortlichen Datenbearbeiter und die Auftragsbearbeiter tun, um eine angemessene Datensicherheit zu gewährleisten?*

Gestützt auf Artikel 8 Absatz 3 DSG hat der Bundesrat in den Artikeln 1 bis 6 DSV Bestimmungen über die Mindestanforderungen an die Datensicherheit erlassen:

Ganz allgemein müssen die Verantwortlichen und Auftragsbearbeiter zur Gewährleistung einer angemessene Datensicherheit den *Schutzbedarf der Personendaten* bestimmen und die im Hinblick auf das *Risiko* für die Persönlichkeit oder die Grundrechte der betroffenen Personen geeigneten *technischen und organisatorischen Massnahmen* festlegen (Art. 1 Abs. 1 DSV).

- Um den *Schutzbedarf der Personendaten* zu bestimmen, müssen die Art der bearbeiteten Daten sowie Zweck, Art, Umfang und Umstände der Datenbearbeitung beurteilt werden (Art. 1 Abs. 2 DSV).
- Bei der Beurteilung des *Risikos für die Persönlichkeit oder die Grundrechte der betroffenen Personen* sind die Ursachen des Risikos, die hauptsächlichen Gefahren, die ergriffenen oder vorgesehenen Massnahmen sowie die Wahrscheinlichkeit und Schwere einer Verletzung der Datensicherheit trotz der ergriffenen oder vorgesehenen Massnahmen als Kriterien heranzuziehen (Art. 1 Abs. 3 DSV).
- Bei der *Festlegung der technischen und organisatorischen Massnahmen*, die zu ergreifen sind, werden ausserdem der Stand der Technik und die Implementierungskosten berücksichtigt (Art. 1 Abs. 4 DSV).

Artikel 2 DSV nennt die Ziele der zur Gewährleistung der Datensicherheit zu treffenden organisatorischen und technischen Massnahmen: Die von den Verantwortlichen und Auftragsbearbeiten bearbeiteten Daten müssen ihrem Schutzbedarf entsprechend:

- nur Berechtigten zugänglich sein (*Vertraulichkeit*);
- verfügbar sein, wenn sie benötigt werden (*Verfügbarkeit*);
- nicht unberechtigt oder unbeaufsichtigt verändert werden (*Integrität*); sowie
- nachvollziehbar bearbeitet werden (*Nachvollziehbarkeit*).

Artikel 3 DSV nennt eine Reihe von Massnahmen, um die Ziele nach Artikel 2 DSV zu erreichen.

Zur Protokollierung gemäss Artikel 4 DSV vgl. die Fragen unter Ziff. 3.6.2.

Zum Bearbeitungsreglement gemäss Artikel 5 f. DSV vgl. die Fragen unter Ziff. 3.6.3.

Verweise: Erläuternder Bericht des Bundesamts für Justiz vom 31. August 2022 zur Verordnung über den Datenschutz (nachfolgend: «Erläuternder Bericht zur DSV»), S. 17 ff.

3.6.2 Protokollierung

3.6.2.1 **Frage**: *Was ist der Sinn und Zweck der Protokollierungspflicht?*

Die Protokollierung ist eine Massnahme zur Gewährleistung der Datensicherheit im Sinne von Artikel 3 DSV. Ausserdem handelt es sich bei der Protokollierung um ein klassisches, präventives Mittel zur Gewährleistung der Cybersicherheit.

Der Zweck der Protokollierung besteht darin, dass die Bearbeitung von Personendaten nachträglich überprüfbar wird. Mit anderen Worten: Es soll im Nachhinein festgestellt werden können, ob Personendaten abhandengekommen sind oder gelöscht, vernichtet, verändert oder offengelegt bzw. zugänglich gemacht wurden. Ausserdem können sich aus der Protokollierung Hinweise ergeben, ob Personendaten zweckkonform bearbeitet wurden. Weiter kann die

Protokollierung dazu dienen, Verletzungen der Datensicherheit (vgl. Frage 3.6.1.1) aufzudecken und aufzuklären. Die Protokollierung hat hingegen *nicht* zum Ziel, die Nutzerinnen und Nutzer, die Personendaten bearbeiten, zu überwachen.

Verweise: Erläuternder Bericht zur DSV, S. 26 ff.

3.6.2.2 **Frage**: *In welchen Fällen müssen Private ihre Datenbearbeitungen protokollieren?*

Private Datenbearbeitungsverantwortliche und Auftragsbearbeiter müssen zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren, wenn sie besonders schützenswerte Personendaten (vgl. Frage 2.1.2) in grossem Umfang (vgl. Frage 3.6.2.3) automatisiert (vgl. Frage 2.2.2) bearbeiten oder ein Profiling mit hohem Risiko (vgl. Frage 2.3.2) durchführen und die präventiven Massnahmen den Datenschutz nicht gewährleisten können (Art. 4 Abs. 1 erster Satz DSV). 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 (Art. 4 Abs. 1 zweiter Satz DSV).

Verweise: Erläuternder Bericht zur DSV, S. 26.

3.6.2.3 **Frage**: *Was bedeutet die Bearbeitung von besonders schützenswerten Personendaten «in grossem Umfang»?*

Der Ausdruck «in grossem Umfang» in Artikel 4 Absatz 1 DSV (sowie weiteren Bestimmungen wie z.B. Art. 22 Abs. 2 Bst. a DSG betreffend Datenschutz-Folgenabschätzung oder Art. 5 Abs. 1 Bst. a DSV betreffend Bearbeitungsreglement und Art. 24 Bst. a DSV betreffend Verzeichnis der Bearbeitungstätigkeiten) bezieht sich auf Fälle, in denen besonders schützenswerte Personendaten nicht bloss vereinzelt bearbeitet werden. Dies betrifft zum Beispiel die Bearbeitung von Daten von Patientinnen und Patienten durch eine Arztpraxis oder ein Spital. Hingegen fällt die vereinzelte Bearbeitung von Daten zu krankheitsbedingten Abwesenheiten von Mitarbeitenden durch ein Unternehmen nicht unter den Begriff. Eine umfangreiche Bearbeitung liegt unter anderem vor, wenn es sich bei der Bearbeitung der besonders schützenswerten Personendaten um eine Haupttätigkeit der datenbearbeitenden Person oder Stelle handelt.

3.6.2.4 **Frage**: *In welchen Fällen müssen Bundesorgane ihre Datenbearbeitungen protokollieren?*

Bundesorgane und ihre Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten (vgl. Frage 2.2.2) zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten (Art. 4 Abs. DSV). Es handelt sich also um dieselben Bearbeitungsvorgänge, welche auch die privaten Verantwortlichen protokollieren müssen (vgl. Frage 3.6.2.2). Allerdings ist der Anwendungsbereich weiter: Die Protokollierungspflicht gilt ungeachtet dessen, ob es sich um besonders schützenswerte Personendaten oder ein Profiling mit hohem Risiko handelt oder nicht. Damit wird den Anforderungen von Artikel 25 der EU-Richtlinie 2016/680 (vgl. Frage 12.1) Rechnung getragen. Für Datenbearbeitungen, die nicht in den Anwendungsbereich der EU-Richtlinie 2016/680 fallen, sieht Artikel 46 Absatz 1 DSV eine Übergangsfrist von drei Jahren ab Inkrafttreten der DSV oder spätestens nach Ende des Lebenszyklus des Systems vor. Während der Übergangszeit gelten die Vorgaben für private Verantwortliche nach Artikel 4 Absatz 1 DSV.

Verweise: Erläuternder Bericht zur DSV, S. 27 und 60.

3.6.2.5 **Frage**: *Welche Besonderheiten gelten bei allgemein öffentlich zugänglichen Personendaten?*

Gemäss Artikel 4 Absatz 3 DSV muss bei Personendaten, welche allgemein öffentlich zugänglich sind, zumindest das Speichern, Verändern, Löschen und Vernichten der Daten protokolliert werden, *nicht* aber das Lesen und Bekanntgeben.

Beispiel: Die Konsultation bzw. das Lesen des Staatskalenders, der allgemein öffentlich zugänglich ist, muss nicht zwingend protokolliert werden.

Verweise: Erläuternder Bericht zur DSV, S. 27.

3.6.2.6 **Frage**: *Was muss protokolliert werden?*

Die Protokollierung muss 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 (Art. 4 Abs. 4 DSV).

Verweise: Erläuternder Bericht zur DSV, S. 27.

3.6.2.7 **Frage**: *Wie lange und auf welche Weise müssen die Protokolle aufbewahrt werden?*

Die Protokolle müssen während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden (Art. 4 Abs. 5 erster Satz DSV). Vorbehalten bleiben spezialrechtliche Vorschriften (z.B. Art. 4 Abs. 1 Bst. b der Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes; SR 172.010.442). Die Aufbewahrungsdauer muss stets in einem angemessenen Verhältnis zu den Zielen der Datensicherheit stehen. Die getrennte Aufbewahrung vom System ist notwendig, da ansonsten bei Cyberangriffen auch die Protokolle selber manipuliert oder verschlüsselt werden könnten.

Die Protokolle dürfen des Weiteren ausschliesslich den Organen und Personen zugänglich sein, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung bzw. Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen (dazu gehören z.B. auch Sicherheitsverantwortliche oder Systemadministratoren, wenn sie den Verdacht haben, dass eine Sicherheitslücke besteht). Die Protokolle dürfen nur für diesen Zweck verwendet werden (Art. 4 Abs. 5 zweiter Satz DSV). Sie dürfen nicht zur Überwachung der Nutzerinnen und Nutzer verwendet werden. Vorbehalten bleibt die Verwendung für spezialgesetzlich vorgesehene Zwecke, wie etwa eine allfällige Verwendung in einem Strafverfahren.

Verweise: Erläuternder Bericht zur DSV, S. 27 f.

3.6.3 Bearbeitungsreglement

3.6.3.1 **Frage**: *Wann müssen private Verantwortliche und Bundesorgane ein Bearbeitungsreglement erstellen?*

Der private Datenbearbeitungsverantwortliche und sein privater Auftragsbearbeiter müssen ein Bearbeitungsreglement für automatisierte Datenbearbeitungen erstellen, wenn sie besonders schützenswerte Personendaten in grossem Umfang bearbeiten (vgl. Frage 3.6.2.3) oder ein Profiling mit hohem Risiko (vgl. Frage 2.3.2) durchführen (Art. 5 Abs. 1 DSV).

Verweise: Erläuternder Bericht zur DSV, S. 28 f.

3.6.3.2 **Frage**: *Wann müssen Bundesorgane ein Bearbeitungsreglement erstellen?*

Bundesorgane und ihre Auftragsbearbeiter müssen nach Artikel 6 Absatz 1 DSV ein Bearbeitungsreglement für automatisierte Bearbeitungen erstellen, wenn sie besonders schützenswerte Personendaten bearbeiten (Bst. a; vgl. Frage 2.1.2); ein Profiling durchführen (Bst. b; vgl. Frage 2.3.1); wenn der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen können (Bst. c); wenn sie Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen Personendaten zugänglich machen (Bst. d); Datenbestände miteinander verknüpfen (Bst. e) oder mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften (Bst. f).

Verweise: Erläuternder Bericht zur DSV, S. 29 f.

3.6.3.3 **Frage**: *Was muss das Bearbeitungsreglement beinhalten?*

Das Bearbeitungsreglement muss insbesondere Angaben zur internen Organisation (z.B. Umschreibung der Systemarchitektur), zum Datenbearbeitungs- und Kontrollverfahren (z.B. betreffend Datenminimierung, Datenbekanntgaben und das Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung) sowie zu den Massnahmen zur Gewährleistung der Datensicherheit beinhalten (Art. 5 Abs. 2 und Art. 6 Abs. 2 DSV). Das Reglement muss zudem regelmässig aktualisiert werden und (im privatrechtlichen Bereich: wenn vorhanden) der Datenschutzberaterin oder dem Datenschutzberater zur Verfügung gestellt werden (Art. 5 Abs. 3 und Art. 6 Abs. 3 DSV; vgl. die Fragen unter Ziff. 3.7).

Wie unter bisherigem Recht ist das Bearbeitungsreglement als eine Dokumentation oder ein Handbuch auszugestalten.

Verweise: Erläuternder Bericht zur DSV, S. 28 ff.

3.6.3.4 **Frage**: *Was ist der Unterschied zwischen dem Bearbeitungsreglement nach Artikel 5 f. DSV und dem Verzeichnis der Bearbeitungstätigkeiten nach Artikel 12 DSG?*

Vgl. dazu Frage 3.8.2.

3.7 Datenschutzberaterinnen und -berater

3.7.1 **Frage**: *Wer muss eine Datenschutzberaterin oder einen Datenschutzberater einsetzen?*

Für *private Datenbearbeitungsverantwortliche* besteht keine Pflicht, eine Datenschutzberaterin oder einen Datenschutzberater zu ernennen. Sie können dies aber freiwillig tun (Art. 10 Abs. 1 DSG) und – wenn gewisse Voraussetzungen erfüllt sind (vgl. dazu die Frage 3.7.3) – von einer Erleichterung bei der Datenschutz-Folgenabschätzung profitieren (Verzicht auf die Konsultation des EDÖB [vgl. dazu Frage 6.3.3]; Art. 10 Abs. 3 i.V.m. Art. 23 Abs. 4 DSG).

Bundesorgane sind dagegen verpflichtet, eine Datenschutzberaterin oder einen Datenschutzberater zu ernennen (Art. 10 Abs. 4 DSG i.V.m. Art. 25 DSV). Dabei können mehrere Bundesorgane eine gemeinsame Datenschutzberaterin oder einen gemeinsamen Datenschutzberater einsetzen. Diese Regelung soll es insbesondere kleineren Bundesorganen oder Departementen mit zentralisierter Organisationstruktur ermöglichen, Synergien zu nutzen und Ressourcen zu sparen.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7032 ff.; Erläuternder Bericht zur DSV, S. 51.

3.7.2 **Frage**: *Was sind die Aufgaben der Datenschutzberaterin oder des Datenschutzberaters?*

Die Datenschutzberaterin oder der Datenschutzberater wirkt bei der Anwendung der Datenschutzvorschriften mit. Sie bzw. er prüft unter anderem die Datenbearbeitungen und empfiehlt Korrekturmassnahmen, wenn eine Verletzung der Datenvorschriften festgestellt wird. Ausserdem schult und berät sie oder er die Mitarbeitenden in Fragen des Datenschutzes (z.B. bei der Erstellung einer Datenschutz-Folgenabschätzung; vgl. Frage 6.3.1). Des Weiteren ist die Datenschutzberaterin oder der Datenschutzberater Anlaufstelle für die von den Datenbearbeitungen betroffenen Personen und für die für den Datenschutz zuständigen Behörden (namentlich für den EDÖB; vgl. zum Ganzen betreffend private Verantwortliche Art. 10 Abs. 2 DSG und betreffend Bundesorgane Art. 10 Abs. 4 DSG i.V.m. Art. 26 Abs. 2 sowie Art. 28 DSV). Die Verantwortung dafür, dass die Personendaten datenschutzkonform bearbeitet werden, trifft nicht die Datenschutzberaterin oder den Datenschutzberater, sondern liegt alleine beim Datenbearbeitungsverantwortlichen.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7032 ff.; Erläuternder Bericht zur DSV, S. 51 ff.

3.7.3 **Frage**: *Was sind die Anforderungen an eine Datenschutzberaterin oder einen Datenschutzberater?*

Für *Bundesorgane* schreibt Artikel 26 Absatz 1 DSV vor, dass die Datenschutzberaterin oder der Datenschutzberater über die erforderlichen Fachkenntnisse verfügen muss (Bst. a) und ihre oder seine Funktion gegenüber dem Bundesorgan fachlich unabhängig und weisungsungebunden ausüben muss (Bst. b). Es muss also gewährleistet sein, dass die Datenschutzberaterin oder der Datenschutzberater ihre bzw. seine Empfehlungen frei aussprechen kann, ohne Nachteile befürchten zu müssen. Die Unabhängigkeit der Datenschutzberaterin oder des Datenschutzberaters ist vor allem durch organisatorische Massnahmen sicherzustellen: Dazu gehört unter anderem, dass sich die Tätigkeit als Datenschutzberaterin oder -berater nicht negativ auf das Mitarbeitergespräch auswirkt.

Falls *private Datenbearbeitungsverantwortliche* von einer Erleichterung bei der Datenschutz-Folgenabschätzung profitieren wollen (Verzicht auf die Konsultation des EDÖB [vgl. dazu Frage 6.3.3; Art. 10 Abs. 3 i.V.m. Art. 23 Abs. 4 DSG], muss ihre Datenschutzberaterin oder ihr Datenschutzberater dieselben Voraussetzungen erfüllen, wie sie für Bundesorgane vorgesehen sind (Art. 10 Abs. 3 Bst. a und b DSG). Ausdrücklich vorgeschrieben ist ausserdem, dass die Datenschutzberaterin oder der Datenschutzberater keine Tätigkeiten ausüben darf, die mit ihren oder seinen Aufgaben unvereinbar sind (Art. 10 Abs. 3 Bst. b DSG). Dies könnte beispielsweise der Fall sein, wenn die Datenschutzberaterin oder der Datenschutzberater Mitglied der Geschäftsleitung ist, Funktionen in Bereichen der Personalführung oder der Informationssystemverwaltung ausübt oder zu einer Dienststelle gehört, die selbst besonders schützenswerte Personendaten bearbeitet. Hingegen ist es durchaus denkbar, die Aufgabe der Datenschutzberaterin oder des Datenschutzberaters mit derjenigen der oder des Informationssicherheitsbeauftragten zu kumulieren. Die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters müssen veröffentlicht und dem EDÖB mitgeteilt werden (Art. 10 Abs. 3 Bst. d DSG).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, 7032 ff.; Erläuternder Bericht zur DSV, S. 51 ff.

3.7.4 **Frage**: *Welche Pflichten treffen die Datenbearbeitungsverantwortlichen gegenüber ihren Datenschutzberaterinnen und -berater?*

Bundesorgane müssen der Datenschutzberaterin oder dem Datenschutzberater Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten (vgl. dazu Frage 3.8.1) und Personendaten, die sie zur Aufgabenerfüllung benötigen, gewähren (Art. 27 Abs. 1 Bst. a DSV). Vorbehalten bleiben spezialgesetzliche Grundlagen, welche diesem Zugang entgegenstehen. Ausserdem müssen die Bundesorgane – z.B. mittels Weisung – dafür sorgen, dass ihre Datenschutzberaterin oder ihr Datenschutzberater über eine Verletzung der Datensicherheit (vgl. dazu Frage 3.6.1.1) informiert wird (Art. 27 Abs. 1 Bst. b DSV). Diese Pflicht betrifft nicht nur Verletzungen, die dem EDÖB gestützt auf Artikel 24 DSG gemeldet werden müssen, sondern bezieht sich auf jegliche Verletzungen der Datensicherheit. Die Datenschutzberaterin oder der Datenschutzberater berät das Bundesorgan bei der Frage, ob die Verletzung einer Meldepflicht im Sinne von Artikel 24 DSG unterliegt (vgl. dazu die Fragen 6.4.2 und 6.4.5). Die Meldung an sich liegt aber in der Verantwortung des Bundesorgans bzw. der für dieses handelnden Personen: Sie entscheiden darüber, ob und – falls ja – welche Verletzungen dem EDÖB gemeldet werden. Schliesslich muss das Bundesorgan die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters im Internet veröffentlichen und dem EDÖB mitteilen (Art. 27 Abs. 2 DSV). Für die Veröffentlichung im Internet genügt es, eine E-Mail-Adresse der fachlich zuständigen Stelle anzugeben. Die Datenschutzberaterin oder der Datenschutzberater muss nicht mit Namen genannt werden.

Für *private Datenbearbeitungsverantwortliche* sieht Artikel 23 DSV ebenfalls verschiedene Pflichten vor: Sie müssen ihrer Datenschutzberaterin oder ihrem Datenschutzberater die notwendigen Ressourcen zur Verfügung stellen (Bst. a); Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten (vgl. dazu Frage 3.8.1) und Personendaten gewähren, welche die Beraterinnen und Berater zur Erfüllung ihrer Aufgaben benötigen (Bst. b) sowie das Recht einräumen, in wichtigen Fällen das oberste Leitungs- oder Verwaltungsorgan zu informieren (Bst. c).

Verweise: Erläuternder Bericht zur DSV, S. 49 und 52.

3.8 Verzeichnis der Bearbeitungstätigkeiten

3.8.1 **Frage**: *Was ist das Verzeichnis der Bearbeitungstätigkeiten?*

Gemäss Artikel 12 Absatz 1 DSG führen die verantwortlichen Datenbearbeiter und die Auftragsdatenbearbeiter je ein Verzeichnis ihrer Bearbeitungstätigkeiten. Das Verzeichnis enthält die wesentlichen Informationen zu den Datenbearbeitungen eines Verantwortlichen oder Auftragsbearbeiters. Vereinfacht gesagt handelt es sich dabei um eine generelle Beschreibung der Datenbearbeitungstätigkeiten. Das Verzeichnis lässt wichtige Rückschlüsse darauf zu, ob eine Datenbearbeitung dem Grundsatz nach datenschutzkonform ausgestaltet ist oder nicht. Das Verzeichnis ist hingegen *kein* Journal, in welchem protokollartig einzelne Daten oder Handlungen aufgeführt werden müssen.

Die Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten ersetzt die bisherige Meldepflicht von Datensammlungen (Art. 11*a* aDSG).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7035 ff.

3.8.2 **Frage**: *Was ist der Unterschied zwischen dem Verzeichnis der Bearbeitungstätigkeiten nach Artikel 12 DSG und dem Bearbeitungsreglement nach Artikel 5 f. DSV?*

Das Bearbeitungsreglement (als Massnahmen zur Gewährleistung der Datensicherheit nach Art. 5 f. DSV; vgl. dazu die Fragen in Ziff. 3.6.3) ist vom Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG) zu unterscheiden. Während das Verzeichnis der Bearbeitungstätigkeiten eine allgemeine Zusammenstellung bzw. einen Überblick über die Datenbearbeitungen eines privaten Datenbearbeiters oder Bundesorgans enthält, regelt das Bearbeitungsreglement die interne Organisation (wie z.B. die Architektur und den Betrieb der Informationssysteme oder die Gewährleistung der Rechte der betroffenen Personen), die Datenbearbeitungs- und -kontrollverfahren (wie z.B. die Zugriffsberechtigungen) sowie die (technischen und organisatorischen) Massnahmen zur Gewährleistung der Datensicherheit (vgl. dazu Frage 3.6.3.3).

3.8.3 **Frage**: *Was muss im Verzeichnis der Bearbeitungstätigkeiten aufgeführt werden?*

Artikel 12 Absatz 2 DSG nennt die Mindestangaben, die das Verzeichnis der Bearbeitungstätigkeiten des verantwortlichen Datenbearbeiters enthalten muss.

Dazu gehören zunächst die Identität (Name bzw. Firma und Adresse) des Verantwortlichen (Bst. a) und der Bearbeitungszweck (Bst. b). Des Weiteren sind die Kategorien betroffener Personen (z.B. «Konsumentinnen und Konsumenten» oder «Arbeitnehmerinnen und Arbeitnehmer») und die Kategorien bearbeiteter Personendaten (z.B. «Kontaktdaten» oder «Zahlungsdaten») zu beschreiben (Bst. c). Aufgeführt werden müssen ebenfalls die Kategorien von Empfängern, denen die Personendaten gegebenenfalls bekanntgegeben werden (Bst. d). Auch hier sind wiederum typisierte Gruppen mit gemeinsamen Merkmalen gemeint, wie z.B. «Aufsichtsbehörden», «Lieferanten» oder «IT-Dienstleister». Befinden sich diese Empfänger im Ausland, müssen im Verzeichnis auch die entsprechenden Staaten sowie allfällige Garantien nach Artikel 16 Absatz 2 DSG (wie Standardvertragsklauseln; vgl. Frage 5.3.2) angegeben werden (Bst. g). Sodann muss das Verzeichnis die Aufbewahrungsdauer der Personendaten enthalten (Bst. e). Sind genaue Angaben nicht möglich, muss das Verzeichnis zumindest die Kriterien enthalten, nach denen diese Dauer festgelegt wird. Gemäss Artikel 12 Absatz 2 Buchstabe f DSG muss das Verzeichnis ausserdem eine allgemeine Beschreibung der Massnahmen zur der Datensicherheit nach Artikel 8 DSG enthalten (vgl. dazu die Fragen unter Ziff. 3.6. Die Wendung «wenn möglich» macht deutlich, dass diese Beschreibung nur erfolgen soll, wenn die Vorkehrungen hinreichend konkret umschrieben werden können.

Artikel 12 Absatz 3 DSG enthält eine kürzere Liste von Mindestangaben, die das Verzeichnis der Bearbeitungstätigkeiten des Auftragsbearbeiters vorsehen muss.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7035 ff.

3.8.4 **Frage**: *Muss das Verzeichnis der Bearbeitungstätigkeiten dem EDÖB gemeldet werden?*

Gemäss Artikel 12 Absatz 4 DSG müssen die *Bundesorgane* ihre Verzeichnisse dem EDÖB melden. Dieser führt ein Meldeportal bzw. Register der Bearbeitungstätigkeiten, welches veröffentlicht wird (Art. 56 DSG; <https://datareg.edoeb.admin.ch>).

Die Meldepflicht an den EDÖB gilt (anders als im bisherigen Recht) nicht für *private Datenbearbeiter*. Die privaten Datenbearbeiter sind allerdings im Rahmen ihrer Mitwirkungspflicht gehalten, dem EDÖB ihre Bearbeitungsverzeichnisse bei einer Untersuchung (auf Anfrage) vorzulegen, damit dieser die Einhaltung des Datenschutzrechts kontrollieren kann (vgl. Art. 49 Abs. 3 und Art. 50 Abs. 1 Bst. a DSG).

3.8.5 **Frage**: *Ist der Betrieb einer Videoüberwachungsanlage durch ein Bundesorgan auch eine Datenbearbeitungstätigkeit, welche im Verzeichnis der Bearbeitungstätigkeiten zu erfassen und dem EDÖB zu melden ist?*

Die Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten nach Artikel 12 DSG bezieht sich auf alle Bearbeitungstätigkeiten eines Verantwortlichen oder Auftragsbearbeiters. Soweit auf den Videoaufnahmen bestimmte oder bestimmbare Personen zu erkennen sind, untersteht also auch die Videoüberwachung durch Bundesorgane dem DSG und somit den Vorschriften zum Verzeichnis der Bearbeitungstätigkeiten (unter Vorbehalt von spezialgesetzlichen Ausnahmen). Das bedeutet, dass dem EDÖB beispielsweise Videokameras zur Überwachung des Eingangsbereichs eines Bundesgebäudes gemeldet werden müssen.

3.8.6 **Frage**: *Gibt es Ausnahmen von der Pflicht, ein Verzeichnis der Bearbeitungstätigkeiten zu führen?*

Gemäss Artikel 12 Absatz 5 DSG i.V.m. Artikel 24 DSV sind Unternehmen und andere privatrechtliche Organisationen, die am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter (unabhängig vom Beschäftigungsgrad) beschäftigen, sowie natürliche Personen von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen. Diese Ausnahme gilt jedoch nicht, wenn (a) besonders schützenswerte Personendaten (wie z.B. Gesundheitsdaten; vgl. zum Begriff die Frage 2.1.2) in grossem Umfang bearbeitet werden oder (b) ein Profiling mit hohem Risiko (vgl. zum Begriff die Frage 2.3.2) durchgeführt wird. Für diese Datenbearbeitungen (nicht aber für die anderen Datenbearbeitungen) ist ein Verzeichnis der Bearbeitungstätigkeiten zu führen.

Zur Frage, wann eine umfangreiche Bearbeitung besonders schützenswerter Personendaten vorliegt vgl. Ziff. 3.6.2.3.

Datenbearbeiter, die von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten ausgenommen sind, können natürlich freiwillig ein solches Verzeichnis erstellen. Gerade wenn jemand regelmässig Personendaten bearbeitet, ist es ein nützliches und einfaches Instrument, um einen Überblick über die Bearbeitungstätigkeiten zu behalten. Dadurch kann auch die Einhaltung anderer Verpflichtungen, wie etwa der Informationspflicht bei der Beschaffung von Personendaten (vgl. Frage 6.1.1), erleichtert werden.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7037; Erläuternder Bericht zur DSV, S. 50.

4. Vertretungspflicht für private Verantwortliche mit Sitz oder Wohnsitz im Ausland

4.1 Voraussetzungen der Vertretungspflicht

4.1.1 **Frage**: *Welche ausländischen Datenbearbeitungsverantwortlichen müssen eine Vertretung in der Schweiz bezeichnen?*

In Artikel 14 Absatz 1 DSG werden neu gewisse ausländische Verantwortliche verpflichtet, eine Vertretung in der Schweiz zu bezeichnen. Diese Verpflichtung trifft private Datenbearbeitungsverantwortliche mit Sitz oder Wohnsitz im Ausland, die Personendaten von Personen in der Schweiz bearbeiten (Einleitungssatz) und die folgenden Voraussetzungen – kumulativ – erfüllen:

- Die Datenbearbeitung steht im Zusammenhang mit dem *Angebot von Waren und Dienstleistungen* oder der *Beobachtung des Verhaltens von Personen in der Schweiz* (Bst. a): Dies ist beispielsweise dann der Fall, wenn der verantwortliche Datenbearbeiter einen Online-Handel betreibt und sein Angebot in Schweizer Franken ausschreibt oder eine Lieferung

in die Schweiz vorsieht. Allein die Tatsache, dass eine Website oder eine elektronische Adresse von der Schweiz aus zugänglich ist, genügt dagegen nicht. Um eine Beobachtung des Verhaltens von Personen in der Schweiz handelt es sich unter anderem dann, wenn der verantwortliche Datenbearbeiter die Aktivitäten dieser Personen im Internet verfolgt. Diese Voraussetzung zielt insbesondere auf soziale Netzwerke ab.

- Es handelt sich um eine *umfangreiche Datenbearbeitung* (Bst. b; vgl. dazu Frage 3.6.2.3).
- Es handelt sich um eine *regelmässige Datenbearbeitung* (Bst. c): Diese Voraussetzung dürfte z.B. im Bereich des Online-Handels erfüllt sein. Auch wenn Personendaten sozusagen den «Rohstoff» einer Tätigkeit bilden – wie z.B. für soziale Netzwerke – liegt eine regelmässige Datenbearbeitung vor. Keine regelmässige Datenbearbeitung ist es dagegen, wenn die Daten nur während einer beschränkten Zeitdauer oder nur gelegentlich bearbeitet werden.
- Die Datenbearbeitung bringt ein *hohes Risiko für die Persönlichkeit der betroffenen Personen* mit sich (Bst. d): Ob eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich bringt, ist jeweils im Einzelfall zu prüfen. Das hohe Risiko kann sich insbesondere aus der Menge und der Art der bearbeiteten Daten (namentlich bei besonders schützenswerten Personendaten), dem Zweck der Datenbearbeitung, der Art und Weise der Datenbearbeitung (z.B. beim Einsatz neuer Technologien), einer allfälligen Datenbekanntgabe ins Ausland sowie der Zugriffsberechtigung auf die Daten (z.B. bei Zugriffen durch eine grosse oder gar unbegrenzte Anzahl Personen) ergeben.

Von der Pflicht, eine Vertretung in der Schweiz zu bezeichnen, sind voraussichtlich insbesondere grosse Internetplattformen und soziale Netzwerke mit Sitz im Ausland betroffen.

Gemäss Artikel 14 Absatz 3 DSG muss der ausländische Datenbearbeitungsverantwortliche den Namen und die Adresse seiner Vertretung veröffentlich. Dies kann er zum Beispiel auf seiner Webseite tun.

4.1.2 **Frage**: *Was passiert, wenn ein ausländischer Datenbearbeitungsverantwortlicher keine Vertretung in der Schweiz bestimmt?*

Der EDÖB kann einen ausländischen Verantwortlichen, der die Voraussetzungen von Artikel 14 Absatz 1 DSG erfüllt, mittels Verfügung dazu verpflichten, eine Vertretung in der Schweiz zu bezeichnen (Art. 51 Abs. 4 DSG). Da es sich dabei um ein amtliches Dokument handelt, muss die Verfügung des EDÖB auf diplomatischem Weg zugestellt werden (ausser ein internationales Abkommen würde die direkte Zustellung vorsehen). Der EDÖB kann dem ausländischen Verantwortlichen zusammen mit seiner Anordnung auch eine Strafe wegen Missachtens von Verfügungen androhen (Art. 63 DSG). Falls gestützt darauf eine Busse angeordnet wird, kann diese grundsätzlich nur rechtshilfeweise vollstreckt werden bzw. muss auf diplomatischem Weg um Hilfe bei der Vollstreckung der Busse ersucht werden.

4.2 Aufgaben und Pflichten der Vertretung

Frage: *Welche Aufgaben bzw. Pflichten hat die Vertretung in der Schweiz?*

Die Vertretung dient in der Schweiz als Anlaufstelle für die betroffenen Personen und den EDÖB (Art. 14 Abs. 2 DSG). Ihr kommt also die Rolle einer Ansprechperson zu. Hingegen kann die Vertretung nicht für allfällige Datenschutzverstösse des Datenbearbeiters verantwortlich gemacht werden.

Gemäss Artikel 15 DSG hat die Vertretung drei Pflichten:

- Sie führt ein Verzeichnis der Bearbeitungstätigkeiten des verantwortlichen Datenbearbeiters (Abs. 1): Dieses Verzeichnis muss dieselben Angaben enthalten, wie es allgemein in Artikel 12 Absatz 2 DSG vorgegeben ist (vgl. Frage 3.8.3). Dabei geht es im Wesentlichen um eine generelle Beschreibung der Bearbeitungstätigkeiten. Personendaten enthält das Verzeichnis hingegen grundsätzlich keine.
- Die Vertretung teilt dem EDÖB auf dessen Anfrage hin alle im Verzeichnis enthaltenen Angaben mit (Abs. 2): Allerdings kann der EDÖB von der Vertretung keine Informationen oder Personendaten verlangen, die sich im Ausland befinden. Dies wäre mit Blick auf die Souveränität des ausländischen Staates problematisch. Benötigt der EDÖB solche Informationen, muss er den Rechtshilfeweg beschreiten.
- Auf Anfrage erteilt die Vertretung den betroffenen Personen Auskünfte darüber, wie diese ihre Rechte ausüben können (Abs. 3): Das können beispielsweise die Adresse des Verantwortlichen oder die Kontaktangaben seiner Datenschutzberaterin oder seines Datenschutzberaters sein. Obwohl die Vertretung als Anlaufstelle für die betroffenen Personen fungiert, bleibt der für die Datenbearbeitung Verantwortliche verpflichtet, der gesetzlich vorgeschriebenen Informationspflicht bei der Beschaffung von Personendaten (vgl. Frage 6.1.1) gegenüber den betroffenen Personen nachzukommen. Auch das Auskunftsrecht (vgl. Frage 7.2.1) kann die betroffene Person einzig beim Verantwortlichen selber und nicht bei dessen Vertretung geltend machen.

5. Bekanntgabe von Personendaten ins Ausland

5.1 Übersicht

Frage: *Wann dürfen Personendaten ins Ausland bekanntgegeben werden?*

Personendaten dürfen gemäss Artikel 16 Absatz 1 DSG ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet (vgl. Ziff. 5.2).

Liegt keine Angemessenheitsbeurteilung des Bundesrates vor, so dürfen Personendaten nur in den Fällen von Artikel 16 Absätze 2 und 3 DSG (Liste von Garantien, mit welchen ein geeigneter Datenschutz gewährleistet werden kann; vgl. Ziff. 5.3) oder von Artikel 17 DSG (Ausnahmetatbestände; vgl. Ziff. 0) ins Ausland bekanntgegeben werden.

Zu den Garantien für einen geeigneten Datenschutz gehören:

- völkerrechtliche Verträge (Art. 16 Abs. 2 Bst. a DSG);
- Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden (Art. 16 Abs. 2 Bst. b DSG);
- spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat (Art. 16 Abs. 2 Bst. c DSG);
- Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat (Art. 16 Abs. 2 Bst. d DSG);

- verbindliche unternehmensinterne Datenschutzvorschriften («Binding Corporate Rules»), die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden (Art. 16 Abs. 2 Bst. e DSG);
- Verhaltenskodizes und Zertifizierungen (Art. 16 Abs. 3 DSG i.V.m. Art. 12 DSV).

Siehe zur Bekanntgabe von Personendaten ins Ausland auch die Informationen und Unterlagen des EDÖB: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html>.

5.2 Angemessenheitsbeurteilung des Bundesrates

5.2.1 **Frage**: *Wo finde ich die Staaten und internationalen Organe, die über einen angemessenen Datenschutz verfügen?*

Gemäss dem totalrevidierten DSG legt der Bundesrat und nicht (mehr) der EDÖB fest, welche Staaten oder internationalen Organe einen angemessenen Datenschutz gewährleisten.

Die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe, die gemäss dem Bundesrat über einen angemessenen Datenschutz verfügen, werden in Anhang 1 zur DSV aufgeführt und sind auf der Webseite des Bundesamts für Justiz einsehbar: <https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales/anerkennung-staaten.html>.

5.2.2 **Frage***: Nach welchen Kriterien beurteilt der Bundesrat, ob ein Staat oder ein internationales Organ über ein angemessenes Datenschutzniveau verfügt?*

Artikel 8 Absatz 2 DSV legt mehrere Kriterien fest, die der Bundesrat bei seinen Angemessenheitsbeurteilungen besonders zu berücksichtigen hat, nämlich:

- die internationalen Verpflichtungen des Staates oder internationalen Organs, insbesondere im Bereich des Datenschutzes (Bst. a);
- die Rechtsstaatlichkeit und die Achtung der Menschenrechte (Bst. b);
- die geltende Gesetzgebung insbesondere zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung (Bst. c);
- die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes (Bst. d);
- das wirksame Funktionieren einer oder mehrerer unabhängiger Behörden, die im betreffenden Staat für den Datenschutz zuständig sind oder denen ein internationales Organ untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen (Bst. e).

Der EDÖB wird bei jeder Beurteilung konsultiert. Zudem können die Einschätzungen von internationalen Organen oder ausländischen Behörden, die für den Datenschutz zuständig sind, berücksichtigt werden (Art. 8 Abs. 3 DSV).

Die Angemessenheitsbeurteilungen des Bundesrates werden periodisch überprüft (Art. 8 Abs. 4 DSV). Sie werden veröffentlicht (Art. 8 Abs. 5 DSG) und sind über den nachfolgenden Link abrufbar: <https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales.html>.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7038 f.; Erläuternder Bericht zur DSV, S. 31 ff.

5.3 Garantien für einen geeigneten Datenschutz

5.3.1 **Frage**: *Welche Anforderungen gelten für vertragliche Datenschutzklauseln (Art. 16 Abs. 2 Bst. b DSG) und für spezifische Garantien (Art. 16 Abs. 2 Bst. c DSG)?*

Fehlt eine positive Angemessenheitsbeurteilung des Bundesrates (vgl. Ziff. 5.2) kann der geeignete Datenschutz im privatrechtlichen Bereich durch *Datenschutzklauseln* in einem Vertrag zwischen dem Datenbearbeitungsverantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner gewährleistet werden (Art. 16 Abs. 2 Bst. b nDSG). Analog dazu kann das zuständige Bundesorgan im öffentlich-rechtlichen Bereich *spezifische Garantien* erarbeiten (Art. 16 Abs. 2 Bst. c DSG).

Anders als Standarddatenschutzklauseln (siehe Frage 5.3.2) gelten die vertraglichen Datenschutzklauseln nur für die Datenbekanntgabe, die im entsprechenden Vertrag vorgesehen ist.

Artikel 9 Absatz 1 DSV regelt den Mindestinhalt der vertraglichen Datenschutzklauseln und der spezifischen Garantien. Folgende Punkte müssen enthalten sein:

- 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 sowie der betroffenen Personen (Bst. b);
- die Art und der 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);
- die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten (Bst. e);
- die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger (Bst. f);
- die Massnahmen zur Gewährleistung der Datensicherheit (Bst. g; siehe die Fragen unter Ziff. 3.6);
- die Pflicht, Verletzungen der Datensicherheit zu melden (Bst. h; siehe die Fragen unter Ziff. 6.4);
- falls die Empfängerinnen und Empfänger Verantwortliche sind: die Pflicht, die betroffenen Personen über die Bearbeitung zu informieren (Bst. i; siehe die Fragen unter Ziff. 6.1);
- die Rechte der betroffenen Person, insbesondere das Auskunftsrecht und das Recht auf Datenherausgabe oder -übertragung, das Recht, der Datenbekanntgabe zu widersprechen, das Recht auf Berichtigung, Löschung oder Vernichtung der Daten sowie das Recht, eine unabhängige Behörde um Rechtsschutz zu ersuchen (Bst. j; siehe die Fragen unter Ziff. 7).

Anders als die Standarddatenschutzklauseln (vgl. Frage 5.3.2) oder die verbindlichen unternehmensinternen Datenschutzvorschriften (vgl. Frage 5.3.3) müssen die vertraglichen Datenschutzklauseln und die spezifischen Garantien nicht vom EDÖB genehmigt werden. Eine

(der Datenbekanntgabe vorangehende) Mitteilung an den EDÖB reicht aus (Art. 16 Abs. 2 Bst. b und c DSG und Art. 9 Abs. 3 DSV).

Der Verantwortliche und der Auftragsbearbeiter (nur im Fall von vertraglichen Datenschutzklauseln) müssen angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die vertraglichen Datenschutzklauseln oder die spezifischen Garantien einhält (Art. 9 Abs. 2 DSV).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7039 f.; Erläuternder Bericht zur DSV, S. 33 ff.

5.3.2 **Frage**: *Welche Anforderungen gelten für Standarddatenschutzklauseln (Art. 16 Abs. 2 Bst. d DSG)?*

Fehlt eine positive Angemessenheitsbeurteilung des Bundesrates (vgl. Ziff. 5.2), kann ein geeigneter Datenschutz durch *Standarddatenschutzklauseln* (Art. 16 Abs. 2 Bst. d DSG) gewährleistet werden.

Standarddatenschutzklauseln können von Privaten, interessierten Kreisen oder Bundesorganen erarbeitet werden. Solche Klauseln müssen vorgängig vom EDÖB genehmigt werden. Es dürfen keine Daten ins Ausland bekanntgegeben werden, bis der EDÖB seinen Entscheid zu den Klauseln gefällt hat, ausser die Datenbekanntgabe kann sich auf anderen Garantien nach Artikel 16 Absatz 2 DSG (vgl. die Fragen 5.3.1 und 5.3.3) oder einen Ausnahmetatbestand nach Artikel 17 DSG (vgl. die Frage 5.4) stützen. Der EDÖB entscheidet innerhalb von 90 Tagen (Art. 10 Abs. 2 DSV).

Standarddatenschutzklauseln können aber auch vom EDÖB selber ausgestellt oder anerkannt werden. Die Liste dieser Klauseln wird vom EDÖB unter <https://www.edoeb.admin.ch/edoeb/de/home/deredoeb/infothek/infothek-ds.html> veröffentlicht.

Beispiel: Der EDÖB hat die Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss [EU] 2021/914 vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäss der Verordnung [EU] 2016/679 des Europäischen Parlaments und des Rates) anerkannt.

Gibt der Verantwortliche oder der Auftragsbearbeiter Personendaten mittels Standarddatenschutzklauseln ins Ausland bekannt, muss er angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet (Art. 10 Abs. 1 DSV).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7040 f.; Erläuternder Bericht zur DSV, S. 35.

5.3.3 **Frage**: *Welche Anforderungen gelten für verbindliche unternehmensinterne Datenschutzvorschriften (Art. 16 Abs. 2 Bst. e DSG)?*

Fehlt eine positive Angemessenheitsbeurteilung des Bundesrates (vgl. Ziff. 5.2), kann die Bekanntgabe von Personendaten an ein ausländisches Unternehmen, das zum selben Konzern gehört (vgl. Art. 11 Abs. 1 DSV), auf *verbindliche unternehmensinterne Datenschutzvorschriften* (sog. «Binding Corporate Rules») gestützt werden (Art. 16 Abs. 2 Bst. e DSG).

Die «Binding Corporate Rules» (BCR) müssen vorgängig durch den EDÖB oder durch eine ausländische Datenschutzbehörde eines Staates mit angemessenem Datenschutzniveau genehmigt worden sein. Erst wenn ein Entscheid des EDÖB vorliegt, können die Personendaten gestützt auf die BCR ins Ausland bekanntgegeben werden. Der EDÖB teilt das Ergebnis seiner Prüfung der BCR innerhalb von 90 Tagen mit (Art. 11 Abs. 3 DSV). Wurden die BCR bereits von einer ausländischen Datenschutzbehörde eines Staates mit angemessenem Datenschutz genehmigt, ist keine separate Genehmigung des EDÖB mehr erforderlich.

Der Mindestinhalt der BCR wird in Artikel 11 DSV geregelt. Die BCR müssen mindestens dieselben Angaben wie die vertraglichen Datenschutzklauseln bzw. spezifischen Garantien nach Artikel 9 Absatz 1 DSV umfassen (vgl. dazu die Frage 5.3.1). Zusätzlich müssen sie die folgenden Angaben enthalten (Art. 11 Abs. 2 DSV):

- die Organisation und die Kontaktdaten des Konzerns und seiner Unternehmen;
- die innerhalb des Konzerns getroffenen Massnahmen zur Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7041 f.; Erläuternder Bericht zur DSV, S. 35 f.

5.3.4 **Frage**: *Gibt es weitere Garantien, um im Ausland einen geeigneten Datenschutz zu gewährleisten und die Datenbekanntgabe ins Ausland zu ermöglichen?*

Ja. Nach Artikel 16 Absatz 3 DSG i.V.m. Artikel 12 Absatz 1 DSV dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein *Verhaltenskodex* oder eine *Zertifizierung* einen geeigneten Datenschutz gewährleistet. Der Verhaltenskodex muss vorgängig dem EDÖB zur Genehmigung unterbreitet werden (Art. 12 Abs. 2 DSV). Der Verhaltenskodex oder die Zertifizierung muss ausserdem mit einer verbindlichen und durchsetzbaren Verpflichtung des Verantwortlichen oder des Auftragsbearbeiters im Drittstaat verbunden werden, die darin enthaltenen Massnahmen anzuwenden (Art. 12 Abs. 3 DSV).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7042; Erläuternder Bericht zur DSV, S. 36.

5.4 Ausnahmen

Frage: *Dürfen Personaldaten ausnahmsweise ohne Angemessenheitsbeurteilung des Bundesrates oder Gewährleistung eines geeigneten Datenschutzes ins Ausland bekannt gegeben werden?*

Ja. Personendaten dürfen gemäss Artikel 17 Absatz 1 DSG in den nachfolgenden Fällen *ausnahmsweise* ohne Angemessenheitsbeurteilung (vgl. Ziff. 5.2) oder besondere Garantien für einen geeigneten Datenschutz (vgl. Ziff. 5.3) ins Ausland bekanntgegeben werden:

- Die betroffene Person hat ausdrücklich in die Bekanntgabe eingewilligt (Bst. a).
- Die Bekanntgabe steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person oder zwischen dem Verantwortlichen und seiner Vertragspartnerin oder seinem Vertragspartner im Interesse der betroffenen Person (Bst. b). In letzterem Fallt muss der EDÖB auf Anfrage informiert werden (Art. 17 Abs. 2 DSG).
- Die Bekanntgabe ist notwendig für die Wahrung eines überwiegenden öffentlichen Interesses oder die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde (Bst. c). Der EDÖB muss auf Anfrage informiert werden (Art. 17 Abs. 2 DSG).
- Die Bekanntgabe ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen (Bst. d). Der EDÖB muss auf Anfrage informiert werden (Art. 17 Abs. 2 DSG)
- Die betroffene Person hat die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt (Bst. e).

- Die Daten stammen aus einem gesetzlich vorgesehenen Register, das öffentlich oder Personen mit einem schutzwürdigen Interesse zugänglich ist, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind (Bst. f).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7042 f.

6. Pflichten des Verantwortlichen und des Auftragsbearbeiters

6.1 Informationspflicht des Verantwortlichen bei der Beschaffung von Personendaten

6.1.1 **Frage**: *Was bedeutet die Informationspflicht bei der Beschaffung von Personendaten?*

Nach Artikel 19 Absatz 1 DSG muss der verantwortliche Datenbearbeiter die betroffene Person angemessen über die Beschaffung ihrer Personendaten informieren. Dies ist ein zentraler Grundsatz des Datenschutzrechts. Denn nur wenn eine Person weiss, dass Daten über sie bearbeitet werden, kann sie auch entscheiden, wie mit diesen Daten umgegangen werden soll.

Mit der Totalrevision des DSG wird die Informationspflicht auf die Beschaffung aller Arten von Personendaten ausgedehnt (Art. 19 Abs. 1 DSG). Für Bundesorgane ist dies nichts Neues. Die Änderung betrifft vor allem private Datenbearbeitungsverantwortliche, die unter dem alten Recht nur über die Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen informieren mussten. Damit wird die Transparenz von Datenbearbeitungen erhöht und die informationelle Selbstbestimmung der Bürgerinnen und Bürger gestärkt.

Wie bisher gilt die Informationspflicht auch dann, wenn die Daten nicht bei der betroffenen Person, sondern bei Dritten beschafft werden (Art. 19 Abs. 1 zweiter Teilsatz DSG).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7050 f.

6.1.2 **Frage**: *Gibt es Ausnahmen von der Informationspflicht bei der Beschaffung von Personendaten?*

Ja. Artikel 20 DSG sieht Ausnahmen, bei welchen die Informationspflicht gänzlich entfällt (Abs. 1 und 2), und Einschränkungen der Informationspflicht, bei welchen eine Interessenabwägung durchgeführt werden muss (Abs. 3 und 4), vor.

Eine *Ausnahme* von der Informationspflicht gilt unter anderem, wenn:

- die betroffene Person bereits über die entsprechenden Informationen verfügt (Art. 20 Abs. 1 Bst a DSG);

  Beispiel: Die betroffene Person hat vorgängig ihre Einwilligung in die Datenbearbeitung gegeben.

- die Datenbearbeitung gesetzlich vorgesehen ist (Art. 20 Abs. 1 Bst. b DSG);

  Unter diese Ausnahme können sowohl Datenbearbeitungen durch Bundesorgane als auch durch private Verantwortlich fallen. In diesem Fall sind die Eckwerte der Datenbearbeitung für die betroffenen Personen aus der gesetzlichen Grundlage erkennbar.

- die Personendaten bei Dritten beschafft werden und die Information der betroffenen Person nicht möglich ist oder einen unverhältnismässigen Aufwand erfordert (Art. 20 Abs. 2 DSG).

Der verantwortliche Datenbearbeiter kann die Information unter anderem dann einschränken, aufschieben oder darauf verzichten, wenn

- überwiegende Interessen Dritter dies erfordern (Art. 20 Abs. 3 Bst. a DSG);

- überwiegende Interessen des privaten Verantwortlichen dies erfordern und der Verantwortliche die Personendaten nicht Dritten (ausserhalb eines Konzerns; vgl. Art. 20 Abs. 4 DSG) bekannt gibt (Art. 20 Abs. 3 Bst. c DSG);

- – bei Bundesorganen – überwiegende öffentliche Interessen, insbesondere der inneren oder der äusseren Sicherheit der Schweiz dies erfordern (Art. 20 Abs. 3 Bst. d Ziff. 1 DSG).

Die Information sollte nur soweit eingeschränkt werden, als dies wirklich unerlässlich ist. Dabei müssen der Grund für die Einschränkung der Informationspflicht und das Interesse an einer transparenten Datenbearbeitung zueinander in Beziehung gesetzt werden. Grundsätzlich sollte die für die betroffene Person günstigste Lösung gewählt werden, sodass eine transparente Datenbearbeitung soweit als möglich gewährleistet wird.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7052 ff.

6.1.3 **Frage**: *Welche Informationen muss der verantwortliche Datenbearbeiter der betroffenen Person mitteilen?*

Gemäss Artikel 19 Absatz 2 Einleitungssatz DSG müssen der betroffenen Person grundsätzlich all diejenigen Informationen mitgeteilt werden, die erforderlich sind, damit sie ihre Rechte nach dem DSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Artikel 19 Absatz 2 Buchstaben a – c sowie die Absätze 3 und 4 DSG konkretisieren diesen Grundsatz durch verschiedene Mindestangaben, welche der betroffenen Person mitgeteilt werden müssen. Mit diesem Konzept lässt sich die Informationspflicht flexibel und risikobasiert handhaben. Je nach der Art der bearbeiteten Daten, der Natur und dem Umfang der fraglichen Datenbearbeitung muss der Verantwortliche verstärkt informieren oder nicht.

Zu den Mindestangaben gehören: die Identität (d.h. der Name oder die Firma) und die Kontaktdaten des Verantwortlichen (Art. 19 Abs. 2 Bst. a DSG), der Zweck der Datenbearbeitung (Art. 19 Abs. 2 Bst. b DSG) und gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen die Personendaten bekanntgegeben werden (Art. 19 Abs. 2 Bst. c). Unter die Empfängerinnen und Empfänger im Sinne dieser Bestimmung fallen auch Auftragsbearbeiter. Der Verantwortliche muss die betroffene Person bei der Beschaffung von Personendaten also darüber informieren, dass die Daten an einen Auftragsbearbeiter bekanntgegeben werden. Werden die Daten nicht bei der betroffenen Person selbst, sondern bei einem Dritten beschafft, muss der verantwortliche Datenbearbeiter zudem die Kategorien der bearbeiteten Personendaten mitteilen (Art. 19 Abs. 3 DSG). Werden die Personendaten ins Ausland bekanntgegeben, muss schliesslich auch über den jeweiligen Staat oder das jeweilige internationale Organ und gegebenenfalls die Garantien nach Artikel 16 Absatz 2 DSG (vgl. dazu die Fragen unter Ziff. 5.3) oder die Anwendung einer Ausnahme nach Artikel 17 DSG (vgl. dazu die Fragen unter Ziff. 5.4) informiert werden (Art. 19 Abs. 4 DSG).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7051 f.

6.1.4 **Frage**: *Auf welche Weise muss die betroffene Person bei der Beschaffung ihrer Personendaten informiert werden? Genügt es, die notwendigen Informationen auf einer Webseite zu veröffentlichen?*

Das DSG legt nicht genau fest, auf welche Weise die betroffene Person informiert werden muss. Artikel 19 Absatz 1 DSG gibt einzig vor, dass die Information «angemessen» erfolgen muss. Artikel 13 DSV konkretisiert, dass der verantwortliche Datenbearbeiter der betroffenen Person die Information über die Beschaffung von Personendaten in präziser, transparenter, verständlicher und leicht zugänglicher Form mitteilen muss.

Weder das DSG noch die DSV geben Formvorschriften für die Information vor. In Frage kommen also z.B. Datenschutzerklärungen, Allgemeine Geschäftsbedingungen, separate Schreiben oder Piktogramme. Der verantwortliche Datenbearbeiter muss allerdings gewährleisten, dass die betroffene Person die Information tatsächlich zur Kenntnis nehmen kann. Dies gilt insbesondere, wenn die Daten nicht bei der betroffenen Person beschafft werden. In diesem Fall reicht es möglicherweise nicht aus, lediglich Informationen auf einer Webseite zur Verfügung zu stellen. Denn die betroffene Person muss wissen, dass sie die Informationen auf einer bestimmten Website findet, und muss aktiv darüber informiert werden.

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.

Der Verantwortliche muss 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 Webseite, 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.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7050 f.; Erläuternder Bericht zur DSV, S. 37.

6.2 Automatisierte Einzelentscheidung

6.2.1 **Frage***: Was ist eine automatisierte Einzelentscheidung?*

Eine automatisierte Einzelentscheidung liegt vor, wenn die Entscheidung ausschliesslich auf einer automatisierten Datenbearbeitung beruht und wenn sie für die betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (Art. 21 Abs. 1 DSG). Im Einzelnen:

- *Vollautomatisation*: Bei einer automatisierten Einzelentscheidung werden sowohl die inhaltliche Beurteilung eines Sachverhalts als auch die darauf basierende Entscheidung durch eine Maschine bzw. einen Algorithmus getroffen, ohne dass eine natürliche Person mitwirkt. Ob die Programmierung des Algorithmus durch einen Menschen erfolgt, ist hingegen nicht massgeblich. Von einer automatisierte Einzelentscheidung ist im Übrigen auch dann auszugehen, wenn die Entscheidung zwar von einer natürlichen Person mitgeteilt wird, von dieser aber nicht vorgenommen worden ist oder lediglich in formellen Aspekten kontrolliert worden ist. Keine automatisierte Einzelentscheidung ist es dagegen, wenn ein Entscheid automatisiert vorbereitet, aber von einer natürlichen Person getroffen wird.

- *Komplexität*: Die automatisierte Einzelentscheidung im Sinne des totalrevidierten DSG muss eine gewisse Komplexität aufweisen. Aus dem Schutzzweck der einschlägigen Bestimmungen (namentlich Art. 21, Art. 25 Abs. 2 Bst. f und Art. 34 Abs. 2 Bst. c DSG) lässt sich schliessen, dass insbesondere Entscheidungsprozesse im Fokus stehen, die für die betroffenen Personen nicht nachvollziehbar sind. Im Sinne einer teleologischen Reduktion von Artikel 21 Absatz 1 DSG sollten deshalb triviale Wenn-Dann-Entscheidungen bzw. simple Ja/Nein-Abfragen objektiver Kriterien, die auf Bedingungen beruhen, welche für die betroffene Person offensichtlich sind, nicht vom Begriff der automatisierten Einzelentscheidung erfasst werden.

Beispiele: Keine automatisierten Einzelentscheidungen i.S.v. Artikel 21 Absatz 1 DSG sind der Bezug von Geld aus einem bestehenden Guthaben am Bancomaten oder die chipkartenbasierte Zutrittskontrolle anhand vorgegebener Listen zutrittsberechtigter Personen. Aber auch simple mathematische Operationen (wie z.B. das reine Zusammenzählen von Werten) dürften in der Regel die für eine automatisierte Einzelentscheidung erforderliche Komplexität nicht erreichen.

- *Wirkung*: Vom Begriff der automatisierten Einzelentscheidung nach Artikel 21 Absatz 1 DSG sind nur Entscheidungen erfasst, die für die betroffene Person mit einer Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen.

  Die Entscheidung ist *mit einer Rechtsfolge verbunden*, wenn sie unmittelbare, rechtlich vorgesehene Konsequenzen für die betroffene Person nach sich zieht. Dies ist im privatrechtlichen Bereich namentlich beim Abschluss eines Vertrags oder dessen Kündigung der Fall. Der Nichtabschluss eines Vertrags entfaltet hingegen in der Regel keine rechtliche Wirkung, (eine besondere Ausgangslage besteht indessen im Bereich von Kontrahierungspflichten). Allerdings kann ein nicht abgeschlossener Vertrag eine erhebliche Beeinträchtigung darstellen (zweite Variante; siehe nachfolgend). Im öffentlich-rechtlichen Bereich liegt eine Rechtsfolge insbesondere dann vor, wenn eine Verfügung vollautomatisiert erlassen wird.

  Eine *erhebliche Beeinträchtigung* der betroffenen Person ist anzunehmen, wenn diese auf nachhaltige Weise z.B. in ihren wirtschaftlichen oder persönlichen Belangen eingeschränkt wird. Eine blosse Belästigung reicht dafür nicht aus. Massgebend sind die konkreten Umstände des Einzelfalls. Zu berücksichtigen ist insbesondere, wie bedeutsam das fragliche Gut für die betroffene Person ist, wie dauerhaft sich die Entscheidung auswirkt und ob allenfalls Alternativen zugänglich sind. Handelt es sich um ein wichtiges Gut (z.B. Wohnung oder Arbeitsstelle), sollte der Umstand, dass Alternativen vorhanden sind, restriktiv ausgelegt werden.

  Beispiel: Eine erhebliche Beeinträchtigung kann vorliegen, wenn medizinische Leistungen auf der Basis automatisierter Entscheidungen zugeteilt werden.

Die automatisierte Einzelentscheidung ist vom Profiling zu unterscheiden, auch wenn sich die beiden Vorgänge überschneiden können. Die der automatisierten Einzelentscheidung zugrundeliegende Datenbearbeitung kann ein Profiling sein, zwingend ist dies jedoch nicht. Umgekehrt kann ein Profiling zu einer automatisierten Einzelentscheidung führen, muss es aber nicht (z.B. wenn das Profiling lediglich eine Vorprüfung für einen Entscheid darstellt, der durch einen Menschen getroffen wird). Die Streichung des Einschubs «einschliesslich Profiling» durch das Parlament in Artikel 19 Absatz 1 des Entwurfs des Bundesrates zur Totalrevision des DSG hat – wie die Departementsvorsteherin des EJPD im Ständerat am 18. Dezember 2019 ausführte – materiell keine Änderung zur Folge. Das Profiling hatte in diesem Bestimmungsentwurf keine selbstständige Bedeutung. Es fällt mit oder ohne ausdrückliche Erwähnung in den Anwendungsbereich von Artikel 21 Absatz 1 DSG, sofern es zu einer automatisierten Einzelentscheidung führt.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7056 ff.; Aktennotiz des BJ über die Totalrevision des DSG, S. 20 ff.; AB 2019 S 1241 (Votum der Departementsvorsteherin des EJPD zur Beratung der Totalrevision des DSG im Ständerat am 18. Dezember 2019).

6.2.2 **Frage**: *Welche Rechte hat die betroffene Person im Falle einer automatisierten Einzelentscheidung?*

Das neue Datenschutzrecht schreibt vor, dass die betroffene Person über eine automatisierte Einzelfallentscheidung informiert werden muss (Art. 21 Abs. 1 DSG). Ergeht die automatisierte Einzelentscheidung durch ein Bundesorgan, so muss es die Entscheidung entsprechend kennzeichnen (Art. 21 Abs. 4 erster Satz DSG). Ausserdem wird der betroffenen Person das Recht eingeräumt, auf Antrag ihren Standpunkt darzulegen und zu verlangen, dass der Entscheid von einer natürlichen Person überprüft wird (Art. 21 Abs. 2 DSG).

Die Pflicht des verantwortlichen Datenbearbeiters zur Information und das Recht der betroffenen Person auf Anhörung entfallen gemäss Artikel 21 Absatz 3 DSG, wenn die automatisierte Einzelentscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und deren Begehren stattgegeben wird (Bst. a) oder wenn die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt (Bst. b; zu den Anforderungen an die Einwilligung vgl. die Frage 3.4.2). Für Bundesorgane ist Artikel 21 Absatz 2 DSG zum Anhörungsrecht der betroffenen Person zudem nicht anwendbar, wenn diese nach Artikel 30 Absatz 2 des Verwaltungsverfahrensgesetzes (VwVG; SR 172.021) oder nach einem anderen Bundesgesetz vor dem Entscheid nicht angehört werden muss (z.B. wenn die automatisierte Einzelentscheidung in einem nicht automatisierten Einspracheverfahren überprüft werden kann). Auf diese Weise wird das DSG mit dem Verwaltungsverfahrensrecht des Bundes koordiniert.

Schliesslich müssen der betroffenen Person im Rahmen ihres Auskunftsrechts gemäss Artikel 25 Absatz 2 Buchstabe f DSG Angaben über das Vorliegen einer automatisierten Einzelentscheidung sowie zur Logik, auf der die Entscheidung beruht, gemacht werden (zum Auskunftsrecht vgl. die Fragen unter Ziff. 7.2.

Verweise: Zu den Anforderungen an die Rechtsgrundlagen für Bundesorgane zum Erlass von automatisierten Einzelentscheidungen vgl. die Aktennotiz des BJ über die Totalrevision des DSG, S. 22.

6.3 Datenschutz-Folgenabschätzung

6.3.1 **Frage**: *Was ist eine Datenschutz-Folgenabschätzung?*

Wer eine Datenbearbeitung plant, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann, muss grundsätzlich eine Datenschutz-Folgenabschätzung erstellen (Art. 22 Abs. 1 DSG). Die Datenschutz-Folgeabschätzung ist ein Instrument zur Risikobewertung. In der Datenschutz-Folgenabschätzung müssen die geplante Bearbeitung beschrieben, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen bewertet sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte aufgezeigt werden (Art. 22 Abs. 3 DSG). Dabei dient die Datenschutz-Folgenabschätzung nicht nur dem Schutz der von einer möglicherweise besonders riskanten Datenbearbeitung betroffenen Personen. Auch für den Datenbearbeitungsverantwortlichen ist eine solche Abschätzung hilfreich, weil sie ihm erlaubt, allfällige datenschutzrechtliche Probleme präventiv anzugehen.

Die Datenschutz-Folgenabschätzung muss nach Beendigung der zugrundeliegenden Datenbearbeitung noch mindestens zwei Jahre aufbewahrt werden (Art. 14 DSV).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7059 ff.; Erläuternder Bericht zur DSV, S. 37 f.

6.3.2 **Frage**: *Wann muss eine Datenschutz-Folgenabschätzung erstellt werden?*

Eine Datenschutz-Folgenabschätzung muss erstellt werden, wenn eine (geplante) Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann (Art. 22 Abs. 1 DSG). Ob ein solches hohes Risiko besteht, ist anhand von verschiedenen Risikofaktoren zu beurteilen. Gemäss Artikel 22 Absatz 2 DSG ergibt sich das hohe Risiko, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Das DSG führt beispielhaft zwei Konstellationen auf, in welchen ein hohes Risiko geben ist: die umfangsreiche Bearbeitung besonders schützenswerter Personendaten (vgl. dazu Frage 3.6.2.3) und die systematische Überwachung umfangreicher öffentlicher Bereiche (Art. 22 Abs. 2 Bst. a und b DSG).

Von der Datenschutz-Folgenabschätzung *ausgenommen* sind private Verantwortliche, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind (Art. 22 Abs. 4 DSG). In diesem Fall ist davon auszugehen, dass der Gesetzgeber allfällige Risiken für die betroffene Person abgewogen und gegebenenfalls die notwendigen Schutzvorschriften erlassen hat.

Ausserdem kann der private Verantwortliche von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn er ein System, ein Produkt oder eine Dienstleistung einsetzt, das oder die für die vorgesehene Verwendung nach Artikel 13 DSG zertifiziert ist, oder wenn er einen Verhaltenskodex nach Artikel 11 DSG einhält, der verschiedene Voraussetzungen erfüllen muss (Art. 22 Abs. 5 DSG).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7059 ff.

Dokumentation zur Datenschutz-Folgenabschätzung (DSFA) für Bundesorgane:

- Richtlinien des Bundesrates für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung (BBl 2023 1882)
- Instrument für die Risikovorprüfung
- DSFA-Leitfaden

6.3.3 **Frage**: *Wann muss der EDÖB konsultiert werden?*

Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der geplanten Bearbeitung *trotz* der vom Datenbearbeitungsverantwortlichen vorgesehenen Massnahmen ein *hohes Restrisiko* für die Persönlichkeit oder die Grundrechte der betroffenen Person *bleibt*, so muss grundsätzlich eine Stellungnahme des EDÖB eingeholt werden (Art. 23 Abs. 1 DSG). Mit anderen Worten: Nur in denjenigen Fällen, in denen es dem für die Datenbearbeitung Verantwortlichen nicht gelingt, die ermittelten Risiken hinreichend zu bewältigen, muss er den EDÖB konsultieren.

Wird der EDÖB konsultiert, so teilt er dem Verantwortlichen innerhalb von zwei Monaten seine Einwände gegen die geplante Bearbeitung mit. Diese Frist kann um einen Monat verlängert werden, wenn es sich um eine komplexe Datenbearbeitung handelt (Art. 23 Abs. 2 DSG). Hat der EDÖB Einwände gegen die geplante Bearbeitung, so schlägt er dem Verantwortlichen geeignete Massnahmen vor (Art. 23 Abs. 3 DSG).

Von der Konsultation des EDÖB *absehen* kann ein privater Verantwortlicher dann, wenn er die Datenschutzberaterin oder den Datenschutzberater nach Artikel 10 DSG konsultiert hat (vgl. dazu die Fragen 3.7.1 und 3.7.3).

6.4 Meldung von Verletzungen der Datensicherheit

6.4.1 **Frage**: *Was ist eine Verletzung der Datensicherheit?*

Vgl. dazu Frage 3.6.1.1.

6.4.2 **Frage**: *Müssen dem EDÖB alle Verletzungen der Datensicherheit gemeldet werden?*

Nein. Eine Meldung an den Beauftragten ist gemäss Artikel 24 Absatz 1 DSG nur dann vorgeschrieben, wenn die Verletzung der Datensicherheit voraussichtlich zu einem *hohen Risiko* für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Der Datenbearbeitungsverantwortliche muss deshalb eine Prognose zu den möglichen Auswirkungen der Verletzung

für die betroffene Person stellen. Meldepflichtig sind nur eingetretene Verletzungen der Datensicherheit, nicht aber erfolgreich abgewehrte oder untaugliche Cyberangriffe. Freiwillige Meldungen einer Verletzung der Datensicherheit, deren Risiko der Verantwortliche nicht als hoch einschätzt, sind möglich.

Die Meldung an den EDÖB kann über ein speziell für diesen Zweck entwickeltes Portal eingereicht werden («Databreach-Portal»: <https://databreach.edoeb.admin.ch/report>). Der Verantwortliche kann die Meldung aber auch in einer anderen Form abgeben.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941 S. 7064.

6.4.3 **Frage**: *Welche Angaben muss die Meldung an den EDÖB enthalten?*

Artikel 24 Absatz 2 DSG enthält die Mindestanforderungen zur Meldung von Verletzungen der Datensicherheit an den EDÖB: Dazu gehört die Art der Verletzung der Datensicherheit, deren Folgen sowie die ergriffenen oder vorgesehenen Massnahmen. Der Inhalt der Meldung an den EDÖB wird in Artikel 15 Absatz 1 DSV weiter präzisiert: Neben den erwähnten Mindestangaben muss der EDÖB soweit als möglich auch über den Zeitpunkt und die Dauer der Verletzung der Datensicherheit sowie die Kategorien und die ungefähre Anzahl der von der Sicherheitsverletzung betroffenen Personendaten (z. B. Adressen, Kreditkartenformationen, Gesundheitsdaten) und betroffenen Personen informiert werden. Diese Informationen sind wichtig, damit der EDÖB das Ausmass der Sicherheitsverletzung abschätzen kann. Ausserdem muss der Datenbearbeitungsverantwortliche den Namen und die Kontaktdaten einer Ansprechperson melden, welche als Anlaufstelle für die Kommunikation mit dem EDÖB als auch gegebenenfalls mit den betroffenen Personen (vgl. dazu Frage 6.4.5) fungiert.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7064 f.; Erläuternder Bericht zur DSV, S. 38.

6.4.4 **Frage**: *In Artikel 24 Absatz 1 DSG heisst es, dass eine Verletzung der Datensicherheit dem EDÖB «so rasch als möglich» gemeldet werden muss. Was bedeutet das?*

Die Meldung der Sicherheitsverletzung hat ab dem Zeitpunkt der Kenntnisnahme so rasch als möglich zu erfolgen. Der Datenbearbeitungsverantwortliche muss grundsätzlich schnell handeln, aber er verfügt über einen gewissen Ermessensspielraum. Massgebend ist dabei unter anderem das Ausmass der Gefährdung der betroffenen Personen. Je erheblicher die Gefährdung und je grösser die Anzahl der betroffenen Personen, umso schneller muss der Verantwortliche den EDÖB informieren.

Artikel 15 Absatz 2 DSV ermöglicht es dem Verantwortlichen, dem EDÖB die Informationen schrittweise zur Verfügung zu stellen, falls es nicht möglich sein sollte bei Entdeckung der Verletzung der Datensicherheit bereits alle Informationen gleichzeitig zu liefern. Er kann in einem ersten Schritt bei der Entdeckung der Verletzung nur die ihm bekannten Grundangaben liefert. Für die Nachmeldung der weiteren Angaben gilt – wie gemäss Artikel 24 Absatz 1 DSG –, dass diese «so rasch als möglich» erfolgen muss (vgl. Art. 24 Abs. 1 DSG; Frage 6.4.4).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7064; Erläuternder Bericht zur DSV, S. 38 f.

6.4.5 **Frage**: *In welchen Fällen müssen die betroffenen Personen über eine Verletzung der Datensicherheit informiert werden?*

Der Verantwortliche muss die betroffenen Personen über eine Verletzung der Datensicherheit informieren, wenn es zu deren Schutz erforderlich ist oder wenn der EDÖB es verlangt (Art. 24 Abs. 4 DSG). Dabei besteht ein gewisser Ermessensspielraum. Wichtig ist, ob durch die Information die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen

reduziert werden können. Dies ist insbesondere dann der Fall, wenn die betroffenen Personen Vorkehren zu ihrem Schutz treffen müssen, zum Beispiel indem sie ihre Zugangsdaten oder Passwörter ändern.

Artikel 15 Absatz 3 DSV regelt, welche Angaben die betroffenen Personen erhalten müssen. Diese Angaben müssen möglichst einfach und verständlich sein.

Der Datenbearbeitungsverantwortliche kann die Information an die betroffenen Personen in gewissen Fällen einschränken, aufschieben oder sogar darauf verzichten, z.B. wenn eine gesetzliche Geheimhaltungspflicht die Information verbietet oder die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert. Diese Ausnahmen sind in Artikel 24 Absatz 5 DSG geregelt.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7065; Erläuternder Bericht zur DSV, S. 39.

7. Rechte der betroffenen Person

7.1 Übersicht

Frage: *Welche Rechte haben die von einer Datenbearbeitung betroffenen Personen?*

Mit der Totalrevision des DSG wird die Transparenz von Datenbearbeitungen erhöht. Das ist für die Stärkung der Rechte der betroffenen Personen zentral. Denn erst wenn eine Person überhaupt weiss, dass Daten über sie bearbeitet werden, kann sie ihre datenschutzrechtlichen Ansprüche wahrnehmen. Neben der Pflicht des verantwortlichen Datenbearbeiters, die betroffenen Personen über die Beschaffung ihrer Personendaten zu informieren (Art. 19 f. DSG; vgl. dazu die Fragen unter Ziff. 6.1), kommt deshalb dem Auskunftsrecht der betroffenen Personen grundlegende Bedeutung zu (Art. 25 ff. DSG; vgl. dazu die Frage 7.2). Damit können die betroffenen Personen vom verantwortlichen Datenbearbeiter wichtige Angaben über die Bearbeitung ihrer Daten verlangen. Neu sieht das DSG ausserdem einen Anspruch auf Datenherausgabe oder -übertragung vor (Art. 28 f. DSG; vgl. dazu die Frage 7.3).

Des Weiteren stehen den betroffenen Personen verschiedene Ansprüche zu, mit welchen sie auf die Bearbeitung ihrer Daten Einfluss nehmen können. Dazu gehören insbesondere das Recht, einer Datenbearbeitung oder Datenbekanntgabe ganz oder teilweise zu widersprechen (Art. 30 Abs. 2 Bst. b i.V.m. Art. 32 Abs. 2 sowie Art. 37 DSG), das Recht auf Berichtigung von unrichtigen Personendaten (Art. 32 Abs. 1 und Art. 41 Abs. 2 Bst. a DSG) sowie das Recht auf Löschung oder Vernichtung von widerrechtlich bearbeiteten Personendaten (Art. 32 Abs. 2 Bst. c und Art. 41 Abs. 2 Bst. a DSG).

Zur Durchsetzung ihrer Rechte können sich die betroffenen Personen im Rahmen eines Zivil- oder Verwaltungsverfahrens an unabhängige Gerichte wenden (Art. 32 und Art. 41 DSG). Ausserdem können sie einen Verstoss gegen die Datenschutzvorschriften beim EDÖB anzeigen (Art. 49 Abs. 1 DSG). Zwar haben die betroffenen Personen in einer allfälligen Untersuchung des EDÖB keine Parteistellung (Art. 52 Abs. 2 DSG e contrario). Der EDÖB muss sie aber über die gestützt auf eine Anzeige unternommenen Schritte und das Ergebnis einer allfälligen Untersuchung informieren (Art. 49 Abs. 4 DSG). Schliesslich besteht die Möglichkeit, gewisse Verhaltensweisen (z.B. die Verletzung von Informations- und Auskunftspflichten) den Strafverfolgungsbehörden zur Anzeige bringen (Art. 60 ff. DSG; vgl. dazu die Fragen unter Ziff. 11).

7.2 Auskunftsrecht

7.2.1 **Frage**: *Was ist das Auskunftsrecht?*

Nach Artikel 25 Absatz 1 DSG kann jede Person vom verantwortlichen Datenbearbeiter Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Dieses Auskunftsrecht wurde im Rahmen der Totalrevision des DSG ausgebaut. Die betroffene Person muss diejenigen Auskünfte erhalten, die erforderlich sind, damit sie ihre Rechte nach dem DSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist (Art. 25 Abs. 2 Einleitungssatz DSG). Das Auskunftsrecht ermöglicht es der betroffenen Person, die Bearbeitung ihrer Daten zu kontrollieren und sich gegen einen allfällige widerrechtliche Datenbearbeitung zur Wehr zu setzen (vgl. Frage. 7.1)

Artikel 25 Absatz 2 DSG enthält eine nicht abschliessende Liste von Angaben, die der betroffenen Person in jedem Fall mitgeteilt werden müssen: Die betroffene Person muss über Identität und Kontaktdaten des Verantwortlichen, über die bearbeiteten Personendaten als solche und über den Bearbeitungszweck informiert werden (Bst. a – c). Weiter müssen ihr die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer mitgeteilt werden (Bst. d). Zudem muss sie die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden, erhalten (Bst. e). Sie muss gegebenenfalls über das Vorliegen einer automatisierten Einzelentscheidung (vgl. dazu die Fragen 6.2.1 und 6.2.2) sowie über die Logik, auf der die Entscheidung beruht, informiert werden (Bst. f). Auch muss sie Angaben über die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben wurden, erhalten. Falls sich diese im Ausland befinden, muss die betroffene Person über den Staat sowie die vorgesehenen Garantien oder die Anwendung einer der Ausnahmen informiert werden (Bst. g; vgl. dazu die Ziff. 5).

Hinweis: Einen Musterbrief sowie weitere Information zum Vorgehen bei einem Auskunftsgesuch finden Sie auf der Webseite des EDÖB:
<https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/grundlagen/auskunftsrecht.html>.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7066 ff.; Erläuternder Bericht zur DSV, S. 40 ff.

7.2.2 **Frage**: *Kann das Auskunftsrecht beschränkt werden?*

In gewissen Fällen kann der verantwortliche Datenbearbeiter die Auskunft verweigern, einschränken oder aufschieben (Artikeln 26 und 27 DSG). Solche Beschränkungen des Auskunftsrechts sind insbesondere aufgrund überwiegender privater oder öffentlicher Interessen möglich. Sie entsprechen weitgehend dem bisherigen Recht.

Neu kann der Verantwortliche die Auskunft ausserdem auch dann verweigern, einschränken oder aufschieben, wenn das Auskunftsgesuch offensichtlich unbegründet ist, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist (Art. 26 Abs. 1 Bst. c DSG). Diese Ausnahme muss eng ausgelegt werden. Denn grundsätzlich darf das Auskunftsrecht voraussetzungslos und ohne Interessensnachweis geltend gemacht werden. In einem Leitentscheid zur datenschutzwidrigen Verwendung des Auskunftsrechts anerkennt das Bundesgericht jedoch, dass das Motiv des Auskunftsbegehrens ausnahmsweise berücksichtigt werden kann, wenn das Auskunftsrecht rechtsmissbräuchlich – also zu datenschutzwidrigen Zwecken – eingesetzt wird (BGE 138 III 425 E. 5.5). Rechtsmissbrauch fällt gemäss dem Bundesgericht beispielsweise dann in Betracht, wenn die Gesuchstellerin oder der Gesuchsteller das Auskunftsbegehren einzig aus dem Grund stellt, um eine (spätere) Gegenpartei auszuforschen und Beweise zu beschaffen, an welche sie bzw. er sonst nicht

gelangen könnte, oder wenn sie bzw. er damit Kosten sparen will, die sie bzw. er für die Datenbeschaffung sonst bezahlen müsste. An eine schikanöse Rechtsausübung zu denken ist ausserdem auch dann, wenn eine Auskunft nur deshalb verlangt wird, um den Auskunftspflichtigen zu schädigen. Angesichts der zentralen Bedeutung des Auskunftsrechts für die Persönlichkeits- und Grundrechte der betroffenen Personen (vgl. Frage 7.2.1), muss jedoch immer offenkundig sein, dass das Auskunftsgesuch aus Gründen gestellt wurde, die mit datenschutzrechtlichen Zwecken nichts zu tun haben.

Wenn das Auskunftsrecht verweigert, eingeschränkt oder aufgeschoben wird, muss der Verantwortliche dies begründen (Art. 26 Abs. 4 DSG). Anhand der Begründung muss die betroffene Person überprüfen können, ob die Beschränkung ihres Auskunftsrechts gerechtfertigt ist.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7068 ff.; Erläuternder Bericht zur DSV, S. 40 ff.; BGE 138 III 425.

7.3 Recht auf Datenherausgabe oder -übertragung

Frage: *Was ist das Recht auf Datenherausgabe oder -übertragung?*

Das Recht auf Datenherausgabe und -übertragung wurde vom Parlament im Rahmen der Beratungen der Totalrevision des DSG eingeführt: Gemäss Artikel 28 DSG hat eine betroffene Person neu die Möglichkeit, ihre Personendaten, die sie einem privaten Datenbearbeitungsverantwortlichen bekanntgegeben hat, in einem gängigen elektronischen Format herauszuverlangen oder einem anderen Verantwortlichen übertragen zu lassen. Die Voraussetzungen hierzu sind, dass der Verantwortliche die Daten automatisiert (vgl. die Frage 2.2.2) und mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person bearbeitet. Sollen die Daten auf einen weiteren Verantwortlichen übertragen werden, darf dies zudem keinen unverhältnismässigen Aufwand erfordern (Art. 28 Abs. 2 DSG).

Die nach Artikel 28 DSG herausverlangten Personendaten können für verschiedene Zwecke verwendet werden: beispielsweise für den rein persönlichen Gebrauch (etwa um die Daten auf einem persönlichen Speicherplatz zu speichern) oder um sie an einen anderen Onlinedienste-Anbieter weiterzuleiten. Der neue Anspruch auf Datenherausgabe oder -übertragung soll die Kontrolle der betroffenen Personen über ihre Personendaten sowie über deren Weiterverwendung zu stärken. Er erleichtert den Wechsel zwischen verschiedenen digitalen Dienstleistungsangeboten und fördert innovative Lösungen sowie den Wettbewerb unter den verschiedenen Anbietern.

Beschränkungen des Rechts auf Datenherausgabe oder -übertragung sind in Artikel 29 DSG geregelt. Dabei wird weitgehend auf die Bestimmungen des Auskunftsrechts verwiesen (vgl. Frage 7.2.2).

Verweise: Eingehende Ausführungen zum Recht auf Datenherausgabe oder -übertragung finden sich im Erläuternden Bericht zur DSV, S. 43 ff.

8. Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Frage: *Brauchen private Datenbearbeiter einen Rechtfertigungsgrund für die Bearbeitung von Personendaten?*

In der Schweiz ist das Bearbeiten von Personendaten durch private Personen (insbesondere Unternehmen oder natürliche Personen) grundsätzlich erlaubt. Nur wenn eine Datenbearbeitung im konkreten Anwendungsfall zu einer Persönlichkeitsverletzung führt, muss sie gerechtfertigt werden. Ansonsten gilt sie als widerrechtlich (Art. 30 Abs. 1 und Art. 31 Abs. 1 DSG).

Damit folgt das Datenschutzgesetz demselben Konzept, welches in allgemeiner Weise schon für den Persönlichkeitsschutz gemäss Zivilgesetzbuch (Art. 28 ff. ZGB; SR 210) gilt.

Nicht jede Bearbeitung von Personendaten stellt eine Persönlichkeitsverletzung dar. Nur wenn die Datenbearbeitung eine Beeinträchtigung von einer gewissen Intensität verursacht, liegt eine Persönlichkeitsverletzung vor. Artikel 30 Absatz 2 DSG enthält eine beispielhafte Aufzählung von Handlungen, die zu einer Persönlichkeitsverletzung führen. Eine Persönlichkeitsverletzung ist demnach insbesondere dann gegeben, wenn:

- Personendaten entgegen den allgemeinen Grundsätzen von Artikel 6 und 8 DSG bearbeitet werden (Art. 30 Abs. 2 Bst. a DSG; z.B. wenn Personendaten länger als notwendig bearbeitet werden oder entgegen dem Zweck, zu welchem sie ursprünglich beschafft worden sind);
- Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden (Art. 30 Abs. 2 Bst. b DSG); oder
- Dritten besonders schützenswerte Personendaten bekanntgegeben werden (Art. 30 Abs. 2 Bst. c DSG).

Keine Persönlichkeitsverletzung liegt dagegen in der Regel vor, wenn die betroffene Person ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 30 Abs. 3 DSG).

Ist eine Persönlichkeitsverletzung erstellt, heisst das noch nicht, dass die Datenbearbeitung unzulässig ist. Eine Persönlichkeitsverletzung ist dann nicht widerrechtlich, wenn ein genügender Rechtfertigungsgrund für die Datenbearbeitung besteht (Art. 31 Abs. 1 DSG). Dabei sind drei Rechtfertigungsgründe möglich:

- *Gesetzliche Grundlage* für die Datenbearbeitung.
- *Überwiegendes privates oder öffentliches Interesse an der Datenbearbeitung*: Dieser Rechtfertigungsgrund erfordert eine Interessenabwägung. Dabei erwähnt das DSG in Artikel 31 Absatz 2 eine Reihe von Beispielen, bei welchen ein überwiegendes Interesse des Datenbearbeiters in Betracht fällt.
- *Einwilligung*: Bildet die Einwilligung der betroffenen Person den Rechtfertigungsgrund für eine persönlichkeitsverletzende Datenbearbeitung, muss diese die Anforderungen von Artikel 6 Absätze 6 und 7 DSG erfüllen (vgl. dazu die Frage 3.4.2).

Kann eine persönlichkeitsverletzende Datenbearbeitung nicht gerechtfertigt werden, hat die betroffene Person verschiedene zivilrechtliche Ansprüche. Dabei verweist Artikel 32 Absatz 2 DSG wie im bisherigen Recht auf die Klagen nach Artikel 28 ff. ZGB. Der betroffenen Person stehen damit die gleichen Ansprüche zu wie bei anderen Persönlichkeitsverletzungen. Der Klarheit halber hält das DSG ausserdem einzelne spezifische Ansprüche ausdrücklich fest. Dazu gehört gemäss Artikel 32 Absatz 2 Buchstabe c DSG insbesondere das Recht auf Löschung oder Vernichtung von Personendaten, die widerrechtlich bearbeitet werden (vgl. dazu die Frage 7.1).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7070 ff.

9. Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane

Hinweis: Anders als private Datenbearbeiter (vgl. Frage 8) benötigen Bundesorgane in der Regel eine Rechtgrundlage für die Bearbeitung von Personendaten. Für die Erarbeitung dieser Rechtsgrundlagen hat das BJ zwei Hilfsmittel veröffentlicht:

- Gesetzgebungsleitfaden Datenschutz
- Aktennotiz «Totalrevision des Datenschutzgesetzes (DSG) - Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane»

10. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Frage: *Wie stärkt das totalrevidierte DSG die Unabhängigkeit und die Aufsichtskompetenzen des EDÖB?*

Die Leiterin oder der Leiter des EDÖB wird neu von der Vereinigten Bundesversammlung gewählt (Art. 43 Abs. 1 DSG). Ausserdem verfügt der EDÖB inskünftig über ein eigenes Budget (Art. 43 Abs. 5 erster Satz und Art. 45 DSG). Damit wird seine Unabhängigkeit gestärkt.

Auch die Aufsichtskompetenz des EDÖB wird erweitert. Gemäss dem neuen Datenschutzgesetz eröffnet der EDÖB grundsätzlich von Amtes wegen oder auf Anzeige hin eine Untersuchung, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte (Art. 49 Abs. 1 DSG). Von der Eröffnung einer Untersuchung kann er dann absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist (Art. 49 Abs. 2 DSG). Die Untersuchungsbefugnisse des EDÖB werden ebenfalls gestärkt (Art. 50 DSG). Kommt der EDÖB zum Schluss, dass eine Verletzung der Datenschutzvorschriften vorliegt, so kann er nicht nur eine Empfehlung, sondern neu eine anfechtbare Verfügung erlassen (Art. 51 DSG). Er kann zum Beispiel die Anpassung, den Unterbruch oder den Abbruch einer Datenbearbeitung oder die Löschung oder Vernichtung von Personendaten verfügen. Hat die betroffene Person eine Anzeige beim EDÖB erstattet, muss der EDÖB sie über die gestützt darauf unternommenen Schritte und das Ergebnis einer allfälligen Untersuchung informieren (Art. 49 Abs, 4 DSG).

Weitere Informationen zur Stellung und zu den Aufgaben des EDÖB finden Sie auf dessen Webseite: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/grundlagen/rolle-edoeb.html>.

11. Strafbestimmungen

11.1 Übersicht

Frage: *Was ändert sich mit dem totalrevidierten DSG bei den Strafbestimmungen?*

Neben einer starken Datenschutzaufsicht sollen strengere Strafbestimmungen für eine bessere Einhaltung des Datenschutzgesetzes sorgen. Im neuen DSG werden deshalb die bisherigen Straftatbestände erweitert und die bisherige Bussenobergrenze für Verstösse wird von 10 000 Franken auf 250 000 Franken erhöht (Art. 60 ff. DSG).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7098 ff.

11.2 Adressaten der Strafbestimmungen

Frage: *Warum werden von den Strafbestimmungen des DSG nicht die Unternehmen, sondern die natürlichen Personen innerhalb des Unternehmens erfasst?*

Es stimmt, dass die Strafbestimmungen im DSG in erster Linie natürliche Personen erfassen. Dies ist aber keine Besonderheit des Datenschutzrechts. Die Adressaten von Strafbestimmungen sind im schweizerischen Strafrecht primär Menschen und nicht Unternehmen.

Allerdings sorgt insbesondere Artikel 6 des Bundesgesetzes über das Verwaltungsstrafrecht (VStrR; SR 313.0) i.V.m. Artikel 64 Absatz 1 DSG dafür, dass bei der Verletzung von Pflichten, welche nur das Unternehmen treffen, gerade nicht die einfachen Mitarbeitenden, sondern die Leitungspersonen strafrechtlich verantwortlich gemacht werden. Das bedeutet: Verantwortlich sind vor allem der Geschäftsherr, die Organe oder die Mitglieder eines Organs, die geschäftsführenden Gesellschafter sowie die tatsächlich leitenden Personen. Es braucht in jedem Fall eine selbstständige Entscheidungsbefugnis in einem bestimmten Unternehmensbereich.

Beispiele: Die Pflicht, sich über das Datensicherheitsniveau bei einem Auftragsbearbeiter ins Bild zu setzen (Art. 61 Bst. b DSG), ist eine Pflicht von Leitungspersonen und nicht von «einfachen Mitarbeitenden». Verstösst hingegen ein Mitarbeiter gegen seine persönliche berufliche Schweigepflicht (Art. 62 DSG), wird er selbst zur Rechenschaft gezogen.

Die zuständige Strafverfolgungsbehörde kann von der Verfolgung der natürlichen Person absehen und stattdessen das Unternehmen (bzw. den Geschäftsbetrieb) zur Bezahlung der Busse verurteilen, wenn höchstens eine Busse von 50 000 Franken in Betracht fällt und die Ermittlung der strafbaren natürlichen Person unverhältnismässig wäre (Art. 64 Abs. 2 DSG).

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7098 ff.

11.3 Zuständigkeit für die Strafverfolgung

Frage: *Wer ist zuständig für die Strafverfolgung?*

Die Verfolgung und die Beurteilung strafbarer Handlungen nach dem DSG obliegt nicht dem EDÖB. Der EDÖB hat also anders als die (meisten) Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten keine Sanktionsbefugnisse. Zuständig sind – wie bisher – die kantonalen Strafverfolgungsbehörden (Polizei, Staatsanwaltschaft, Strafgerichte; Art. 65 Abs. 1 DSG). Allerdings kann der EDÖB bei der zuständigen Strafverfolgungsbehörde Anzeige erstatten und im Verfahren die Rechte einer Privatklägerschaft wahrnehmen (Art. 65 Abs. 2 DSG). Ausserdem kann er seine Verfügungen mit einem Hinweis auf die Strafdrohung nach Art. 63 DSG versehen: Danach werden private Personen mit einer Busse bis zu 250'000 Franken bestraft, wenn sie der Verfügung des EDÖB vorsätzlich nicht Folge leisten. Für die Strafverfolgung sind aber auch in dieser Konstellation die kantonalen Strafverfolgungsbehörden zuständig.

Verweise: Botschaft zur Totalrevision des DSG, BBl 2017 6941, S. 7104 ff.

12. Internationale Entwicklungen des Datenschutzes

12.1 EU-Richtlinie 2016/680

Frage: *Welche Bedeutung hat die EU-Richtlinie 2016/680 für die Schweiz?*

Die EU-Richtlinie 2016/680 stellt eine Weiterentwicklung des Schengen-Besitzstands dar, welche die Schweiz aufgrund des Schengen-Assoziierungsabkommens übernehmen musste. Sie hat einen spezifischen Geltungsbereich und regelt Datenbearbeitungen durch Behörden zum Zweck der Strafverfolgung, Strafvollstreckung und der Abwehr von Gefahren für die öffentliche Sicherheit.

12.2 EU-Datenschutz-Grundverordnung und Angemessenheitsbeschluss

12.2.1 **Frage**: *Welche Bedeutung hat die Datenschutz-Grundverordnung der EU für die Schweiz?*

Die EU-Datenschutz-Grundverordnung regelt allgemein den Schutz von Daten, die von privaten Personen oder Behörden der EU-Mitgliedstaaten bearbeitet werden. Anders als die EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen (vgl. Frage 12.1) ist die EU-Datenschutz-Grundverordnung keine Weiterentwicklung des Schengen-Besitzstandes und ist für die Schweiz nicht direkt verbindlich. Allerdings gilt die EU-Datenschutz-Grundverordnung auch für Unternehmen in der Schweiz, wenn sie Personen in der EU Waren oder Dienstleistungen anbieten oder wenn sie das Verhalten von Personen in der EU beobachten. Zudem ist es für die Schweiz wichtig, dass sie von der EU auch unter der Datenschutz-Grundverordnung weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkannt wird.

12.2.2 **Frage**: *Erfüllt das schweizerische Datenschutzrecht die europäischen Standards?*

Die Schweiz verfügt bereits seit dem Jahre 2000 über einen Angemessenheitsbeschluss der EU, der ein gleichwertiges Datenschutzniveau anerkennt. Die Angemessenheit gegenüber den europäischen Datenschutzvorschriften wird regelmässig überprüft. Das neue Recht ermöglicht eine Annäherung des Schweizer Schutzniveaus an den EU-Standard und trug dazu bei, dass die EU der Schweiz ein angemessenes Datenschutzniveau bestätigte (siehe dazu den Bericht der Europäischen Kommission vom 15. Januar 2024 sowie das dazugehörige Arbeitsdokument mit den Länderberichten; letzteres ist nur auf Englisch verfügbar).

12.2.3 **Frage**: *Was sind die Folgen, wenn die EU-Kommission das Datenschutzniveau der Schweiz mehr nicht als angemessen anerkennt?*

Fehlt ein Angemessenheitsbeschluss vonseiten der EU, so sind Datenbekanntgaben in die Schweiz nur möglich, sofern geeignete Garantien vorgesehen sind oder bestimmte Ausnahmetatbestände vorliegen. Dies führt zu hohen administrativen Hürden, die den freien Datenfluss und die damit einhergehende Innovation hemmen und somit nachteilige Konsequenzen für den Schweizer Wirtschaftsstandort haben. Die EU hat am 15. Januar 2024 bestätigt, dass die Schweiz ein angemessenes Datenschutzniveau bietet (siehe dazu den Bericht der Europäischen Kommission vom 15. Januar 2024 sowie das dazugehörige Arbeitsdokument mit den Länderberichten; letzteres ist nur auf Englisch verfügbar).

12.3 Datenschutz-Konvention 108+ des Europarates

Frage: *Warum ist die Schweiz der modernisierten Datenschutz-Konvention 108+ des Europarates beigetreten?*

Bis heute haben rund 50 Staaten die Datenschutz-Konvention 108 des Europarats ratifiziert, darunter auch die Schweiz. Es ist das erste verbindliche völkerrechtliche Instrument im Bereich des Datenschutzes und datiert aus dem Jahr 1981. Der Europarat hat nun auch diese Konvention dem digitalen Zeitalter angepasst. Die Schweiz hat die revidierte Konvention bzw. die modernisierte Datenschutz-Konvention 108 (Datenschutz-Konvention 108+) am 7. September 2023 ratifiziert. Die Datenschutz-Konvention 108+ wird jedoch erst in Kraft treten, wenn 38 Vertragsstaaten sie ratifiziert haben

Die Schweiz kann mit der Ratifizierung der Datenschutz-Konvention 108+ gegenüber ihren internationalen Vertragspartnern ein gutes Datenschutzniveau behalten und damit den Wirtschaftsstandort stärken. Mit der Totalrevision des DSG werden die Anforderungen der Datenschutz-Konvention 108+ erfüllt.