GESETZGEBUNGSLEITFADEN DATENSCHUTZ

Auswirkungen des neuen Datenschutzgesetzes auf die Erarbeitung von Rechtsgrundlagen

Bern, August 2022, aktualisiert im März 2024

Inhaltsverzeichnis

Einleitung

A) Kontext

Das vorliegende Dokument ersetzt den Leitfaden für die Erarbeitung der Rechtsgrundlagen für den Betrieb eines Systems zur automatisierten Bearbeitung von Personendaten vom 16. Dezember 2010, der nicht mehr aktuell ist. Ziel ist es, die Auswirkungen der Totalrevision des Bundesgesetzes über den Datenschutz (DSG; vgl. nachfolgend Ziff. 2.1)[1] auf die Schaffung der Rechtsgrundlagen, die Bundesorgane für die Bearbeitung von Personendaten von natürlichen Personen benötigen, in zusammengefasster Form darzustellen und die Grundprinzipien des Datenschutzes, die unverändert bleiben, aufzuzeigen. Von der Form her handelt es sich um eine Zusammenfassung; das vorliegende Dokument basiert auf einer ausführlichen Aktennotiz des Bundesamts für Justiz (BJ) zur Totalrevision des Datenschutzgesetzes mit dem Titel *Totalrevision des Datenschutzgesetzes: Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane* (nachfolgend: *«Aktennotiz des BJ über die Totalrevision des DSG»*), und verweist darauf.

Wie der vorhergehende Leitfaden ist auch das vorliegende Dokument ein Hilfsmittel unter vielen für die Juristinnen und Juristen, die mit der Ausarbeitung von Rechtsgrundlagen beauftragt sind, die Bundesorgane zur Bearbeitung von Personendaten natürlicher Personen benötigen. Dieses Hilfsmittel konzentriert sich auf die Elemente, die bei der Ausarbeitung der betreffenden Rechtsgrundlagen zu berücksichtigen sind. Es deckt nicht alle Aspekte des Datenschutzes ab. Es erfasst namentlich sehr wichtige Bereiche wie die Datensicherheit nicht, die zwar insbesondere die Einführung technischer und organisatorischer Massnahmen im Sinne von Artikel 3 der Datenschutzverordnung vom 31. August 2022[2] (DSV) erfordert, aber nicht unbedingt die Ausarbeitung spezifischer Gesetzesbestimmungen.

[1] Die Revision ist am 1. September 2023 in Kraft getreten.

[2] SR **235.11** – Verordnung vom 31. August 2022 über den Datenschutz (Datenschutzverordnung, DSV) (admin.ch)

B) Verbindungen zum Gesetzgebungsleitfaden, zur Projektmanagementmethode HERMES und zur Datenschutz-Folgenabschätzung (DSFA)

Die Datenschutzbedürfnisse müssen bereits in der Anfangsphase eines Projekts analysiert werden. Sehr häufig müssen gesetzliche Grundlagen geändert oder neu geschaffen werden. Das vorliegende Dokument stellt die wichtigsten Fragen zu diesem Thema dar und ergänzt in dieser Hinsicht das Vorgehen, das Juristinnen und Juristen im Gesetzgebungsleitfaden vorgeschlagen wird[3].

Darüber hinaus sieht die Projektmanagementmethode HERMES, die insbesondere im Bereich der Informatik des Bundes eingesetzt wird,[4] die Erarbeitung eines ISDS-Konzepts[5] vor (Informationssicherheits- und Datenschutzkonzept). Dieses Dokument kann sich als hilfreich erweisen, um die Anforderungen an den Datenschutz zu bestimmen, Risiken zu bewerten und Massnahmen für die Entwicklung dieses Konzepts festzulegen.

Eine Datenschutz-Folgenabschätzung (DSFA) ist erforderlich, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann (Art. 22 Abs. 1 DSG). Der Bundesrat hat am 28. Juni 2023 die Richtlinien[6] für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung (DSFA-Richtlinien) erlassen. Andere praktische Hilfsmittel werden auf der Website des BJ zur Verfügung gestellt, wie zum Beispiel das Instrument für die Risikovorprüfung[7], der DSFA-Leitfaden[8] und das Dokument FAQ Datenschutzrecht[9].

I Verfassungsrechtlicher Rahmen

1.1 Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 der Bundesverfassung sowie gemäss Art. 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten

Das Recht auf informationelle Selbstbestimmung ist in Artikel 13 Absatz 2 der Bundesverfassung (BV)[10] und Artikel 8 der Europäischen Menschenrechtskonvention

---

[3] Die elektronische Version von Kapitel 14 des Gesetzgebungsleitfadens (BJ, Gesetzgebungsleitfaden, 4. Aufl., 2019) über den Datenschutz wurde im Oktober 2023 aktualisiert: Legistische Hauptinstrumente (admin.ch).

[4] https://www.hermes.admin.ch/, Methodenübersicht (admin.ch)

[5] ISDS-Konzept erarbeiten (admin.ch)

[6] BBl **2023** 1882 – Richtlinien des Bundesrates für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung (DSFA-Richtlinien)

[7] Instrument für die Risikovorprüfung: https://www.bj.admin.ch/dam/bj/de/data/staat/datenschutz/instrument-risikovorpruefung.xlsx.download.xlsx/instrument-risikovorpruefung-d.xlsx

[8] DSFA-Leitfaden: https://www.bj.admin.ch/dam/bj/de/data/staat/datenschutz/dsfa-leitfaden.pdf.download.pdf/dsfa-leitfaden-d.pdf

[9] FAQ Datenschutzrecht, BJ, September 2023

[10] SR **101** – Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (admin.ch)

(EMRK)[11] verankert. Es verleiht der einzelnen Person eine Art Herrschaft über ihre Personendaten.[12] Artikel 13 Absatz 2 BV schützt also nicht nur die einzelne Person vor dem *«Missbrauch»* ihrer Daten, wie es der Wortlaut zu erklären scheint. Er erfasst jede Tätigkeit des Staates zur Bearbeitung von Personendaten, z. B. die Erhebung, Aufbewahrung oder Bekanntgabe von Personendaten.[13] *«Im Bereich des Datenschutzes garantiert das verfassungsmässig geschützte Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV und Art. 8 Ziff. 1 EMRK), dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen sind, dem Einzelnen die Herrschaft über seine Personendaten zusteht»*[14]. Es handelt sich um ein Grundrecht. Einschränkungen dieses Rechts müssen daher die verfassungsmässigen Anforderungen der gesetzlichen Grundlage, des öffentlichen Interesses, der Verhältnismässigkeit und der Wahrung des Kerngehalts der Grundrechte erfüllen (Art. 36 BV).[15] Schwerwiegende Einschränkungen von Grundrechten müssen in einem Gesetz im formellen Sinn vorgesehen sein (Art. 36 Abs. 1, zweiter Satz BV). Personen, die mit der Ausarbeitung eines Erlasses betraut sind, der eine Bearbeitung von Personendaten nach sich zieht oder regelt, sind verpflichtet, auf die Einhaltung dieser verfassungsrechtlichen Anforderungen und der aus Artikel 8 EMRK folgenden konventionsrechtlichen Anforderungen zu achten[16] (dies selbst wenn das Bundesgesetz über den Datenschutz nicht anwendbar ist, wie bei der Datenbearbeitung durch kantonale öffentliche Organe).[17]

1.2 Verfassungsrechtliche Kompetenzaufteilung

Die Bundesverfassung enthält keine Bestimmung, die den Bund ausdrücklich zur Gesetzgebung im Bereich des Datenschutzes ermächtigt. Der Bund kann Datenschutzbestimmungen nur auf der Grundlage von Verfassungsnormen erlassen, die ihm die Gesetzgebungskompetenz auf einem bestimmten Gebiet übertragen, z. B. im Bereich der Sozialversicherungen (Alters-, Hinterlassenen- und Invalidenversicherung, Arbeitslosenversicherung, Kranken- und Unfallversicherung). Wo derweil die Bundesverfassung dem Bund die Zuständigkeit für die Gesetzgebung auf einem bestimmten Gebiet überträgt, kann sich die Verpflichtung des Bundesgesetzgebers ergeben, spezifische Datenschutzbestimmungen zu erlassen, die auch für die mit dem Vollzug von Bundesrecht betrauten kantonalen Behörden gelten, z. B. im Bereich der Sozialversicherungen.

---

[11] SR **0.101** – Konvention vom 4. November 1950 zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) (admin.ch)

[12] Pascal MAHON, *Le droit à l'intégrité numérique: réelle innovation ou simple évolution du droit? Le point de vue du droit constitutionnel*, in: Le droit à l'intégrité numérique, Helbing Lichtenhahn, 2021, S. 44–63 [47–48] und die zitierte Rechtsprechung.

[13] BGE **128** II 259 E. 3.2

[14] BGE **138** II 346 E. 8.2 (D) oder BGE **140** I 381 E. 4.1 (F); vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1.

[15] Betreffend die Einschränkung von Grundrechten vgl. Gesetzgebungsleitfaden, Rz. 688.

[16] Im Zusammenhang mit der Dauer der Aufbewahrung von Personendaten vgl. EGMR-Urteil *Catt v. Vereinigtes Königreich* vom 24. Januar 2019, Nr. 43514/15.

[17] Vgl. die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1, sowie die zitierten Verweise auf Lehre und Rechtsprechung zu den verfassungsmässigen Rechten, die sich aus Art. 13 Abs. 2 BV ergeben, insbesondere das Recht, von der Existenz von Personendaten Kenntnis zu haben, diese einzusehen und unrichtige Daten berichtigen zu lassen.

Es obliegt den Kantonen, in ihren Kompetenzbereichen Gesetze zum Datenschutz zu erlassen.[18] Vorbehaltlich von Bestimmungen in Spezialgesetzen des Bundes werden Datenbearbeitungen kantonaler (und kommunaler) Organe durch das kantonale Recht geregelt. Dies gilt auch, wenn die betreffenden Organe Bundesrecht vollziehen oder die Daten über einen Online-Zugriff auf eine Datenbank des Bundes beschafft haben.[19]

II Gesetzlicher Rahmen, Begriffe, Grundsätze

2.1 Vorbemerkungen

Das Bundesgesetz über den Datenschutz vom 25. September 2020 (DSG) ersetzt das Bundesgesetz über den Datenschutz von 1992 (aDSG oder Gesetz von 1992).[20] Ziel der Revision ist es, besser auf die mit den neuen Technologien verbundenen Herausforderungen reagieren zu können; die Transparenz der Datenbearbeitung soll verbessert[21] und das verfassungsmässige Recht auf informationelle Selbstbestimmung gestärkt werden. Das DSG übernimmt die bewährten Begriffe und Grundsätze. Es schafft keine neuen Kompetenzen zugunsten des Bundes, sodass die Kantone vorbehaltlich der oben erwähnten bereichsspezifischen materiellen Bundesbestimmungen (vgl. Ziff. 1.2) souverän bleiben.

Das Schweizer Recht muss die Anforderungen der Weiterentwicklung des Schengen-Besitzstands erfüllen, insbesondere der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung im Rahmen des Schengen-Besitzstands.[22]

---

[18] Austausch personenbezogener Daten zwischen Behörden des Bundes und der Kantone. Bericht des Bundesrates in Erfüllung des Postulates Lustenberger 07.3682 vom 5. Oktober 2007 *«Erleichterter Datenaustausch zwischen Bundes- und Kantonsbehörden»*, BBl **2011** 645.

[19] 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 (nachfolgend: «Botschaft über die Totalrevision des DSG»); vgl. auch die Aktennotiz des BJ über die Totalrevision des Datenschutzgesetzes, Ziff. 4.5, sowie den obgenannten Bericht des Bundesrates in Erfüllung des Postulates Lustenberger, Ziff. 2.1, BBl **2011** 645.

[20] Es ersetzt auch das Schengen-Datenschutzgesetz vom 28. September 2018, SR **235.3**, vgl. nachfolgend Fussnote 22.

[21] Botschaft über die Totalrevision des DSG, BBl **2017** 6943, siehe jedoch: Bertil COTTIER, Transparence des traitements de données personnelles opérés par les organes fédéraux: un pas en avant, deux en arrière, SZW 2021 S. 65 ff., 65), wo festgehalten ist: *«‹Le présent projet de loi vise à renforcer la protection des données, au travers notamment d'une amélioration de la transparence des traitements et du contrôle que les personnes concernées peuvent exercer sur leurs données.› Autant dire qu'à l'entame de son message à la révision totale de la loi sur la protection des données, le Conseil fédéral exprime sans détours ses intentions: une des priorités de la nouvelle loi sera d'accroitre la visibilité des traitements de données personnelles. La révision de la loi fédérale sur la protection des données enfin sous toit, il y a lieu de se demander si cet objectif fondamental a réellement été atteint. C'est sans ambages que l'on répondra oui s'agissant des traitements opérés par des personnes privées; et ce, en raison avant tout de l'ampleur du devoir d'information désormais à la charge du responsable du traitement. Pour ce qui concerne les traitements opérés par des organes fédéraux, la réponse est en revanche mitigée. Certes, des coups de projecteurs bienvenus ont été apportés ici ou là: intelligibilité des décisions automatisées, extension du droit d'accès et annonce des violations de la sécurité des données notamment. Ces avancées ponctuelles ne sauraient toutefois masquer un recul majeur: la révision a affaibli le devoir d'information des autorités fédérales».*

[22] Das Parlament hat den ursprünglichen Vorschlag des Bundesrates für eine Totalrevision des DSG in zwei Etappen aufgeteilt. In einem ersten Schritt wurde nur die EU-Richtlinie 2016/680 über den Datenschutz in Strafsachen umgesetzt (vgl. zum Beispiel den erläuternden Bericht zum Bundesgesetz über die Umsetzung der Richtlinie [EU] 2016/690 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung im Rahmen der Weiterentwicklung des Schengen-Besitzstands). Das Bundesgesetz über den Schutz von Personendaten im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-

Im Übrigen müssen die bereichsspezifischen Rechtsgrundlagen im Bereich des Datenschutzes auch die Anforderungen der modernisierten Datenschutzkonvention 108+ des Europarates erfüllen[23], die von der Schweiz am 7. September 2023 ratifiziert wurde und in Kraft tritt, wenn sie von 38 Vertragsstaaten ratifiziert worden ist.[24]

Darüber hinaus profitiert die Schweiz von einem Angemessenheitsbeschluss der EU, der die Schweiz als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt, wodurch ohne Hindernisse Daten mit der Schweiz ausgetauscht werden können.[25] Es ist daher wichtig, dass die Schweizer Datenschutzgesetzgebung, einschliesslich des bereichsspezifischen Rechts, den Datenschutzstandard der Datenschutz-Grundverordnung der Europäischen Union (Verordnung (EU) 2016/679, DSGVO) einhält. So hat die Europäische Kommission in ihrem Bericht vom 15. Januar 2024 bestätigt, dass das Datenschutzrecht der Schweiz nach wie vor dem europäischen Standard entspricht.[26]

2.2 Persönlicher und sachlicher Geltungsbereich

Das DSG bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden (Art. 1 DSG).

Der Geltungsbereich des DSG wurde auf Daten über natürliche Personen beschränkt. Wie im aDSG ist in Artikel 2 DSG ein Katalog von Ausnahmen bezüglich des Geltungsbereichs des DSG vorgesehen. Der Katalog umfasst beispielsweise die Bearbeitung von Personendaten im Rahmen von Gerichtsverfahren.

Hingegen umfasst der Geltungsbereich des DSG die Daten über juristische Personen nicht mehr. Die Bearbeitung von Personendaten über juristische Personen ist nunmehr im Regierungs- und Verwaltungsorganisationsgesetz (RVOG)[27] geregelt, wie es durch Anhang 1/II des DSG angepasst wurde. Juristische Personen können sich auf Artikel 13 Absatz 2 BV berufen. Das bedeutet insbesondere, dass Bundesorgane Daten juristischer Personen nur bearbeiten oder bekanntgeben dürfen, wenn dafür eine ausreichende gesetzliche Grundlage besteht. Mit der Totalrevision des DSG werden im Regierungs- und Verwaltungsorganisationsgesetz eine Reihe von neuen Bestimmungen eingeführt, welche den Umgang mit Daten juristischer Personen durch Bundesorgane regeln (Art. 57*r* ff.

Datenschutzgesetz, SDSG) ist am 1. März 2019 in Kraft getreten, während das Parlament die Beratung über die Totalrevision des DSG fortgesetzt hat. Das DSG hebt das SDSG auf, der Inhalt des letzteren wird in das DSG übernommen.

[23] Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 10. Oktober 2018 (CETS Nr. 223).

[24] La Suisse ratifie le Protocole d'amendement à la Convention 108 – Protection des données (coe.int), 31 Staaten haben bis am 6. Februar 2024 das oben genannte Protokoll ratifiziert.

[25] Verfahren für den Angemessenheitsbeschluss, vgl. Art. 45 DSGVO.

[26] Die Europäische Kommission hat am 15. Januar 2024 ihren Bericht über die Angemessenheit des Datenschutzniveaus von mehreren Drittstaaten veröffentlicht. Darin anerkennt sie, dass die Schweiz weiterhin ein angemessenes Schutzniveau für Personendaten bietet: EU bestätigt angemessenen Datenschutz in der Schweiz (admin.ch)

[27] SR **172.010** – Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG)

RVOG). Des Weiteren soll die Übergangsbestimmung von Artikel 71 DSG mögliche Rechtslücken verhindern [28].

Beabsichtigt ein Bundesorgan die Bearbeitung von Daten, die keine Informationen enthalten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, muss den Anforderungen des DSG nicht Rechnung getragen werden. Das Bundesorgan berücksichtigt bei seiner Beurteilung das Risiko, dass Sachdaten mit anderen Daten oder technischen Prozessen verknüpft werden, die einen Personenbezug herstellen können.

2.3 Begriffe

Gemäss den Anforderungen an die Einschränkung von Grundrechten und dem Legalitätsprinzip (Art. 5 BV) müssen Bundesorgane über eine gesetzliche Grundlage verfügen, um Personendaten bearbeiten zu können[29] – unabhängig davon, ob die Daten besonders schützenswert sind oder nicht.

Diese gesetzliche Grundlage ist in den bereichsspezifischen Erlassen zu schaffen. Das DSG legt die Anforderungen fest, die diese bereichsspezifischen Rechtsgrundlagen erfüllen müssen (Art. 34 und 36 DSG). Im Vergleich zum Gesetz von 1992 ändert es bestimmte Begriffe wie den der besonders schützenswerten Daten oder führt neue Begriffe wie z. B. jenen des Profilings ein.[30]

2.3.1 Personendaten

Der Begriff der Personendaten bleibt unverändert (Art. 5 Bst. a DSG). Er umfasst alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Der Begriff ist nach wie vor in einem weiten Sinne zu verstehen, z. B. kann eine IP-Adresse (IP für Internet Protocol, d. h. die Identifikationsnummer, die jedem Rechner zugewiesen wird, der auf das Internet zugreift) unter bestimmten Voraussetzungen ausreichen, um unter den Begriff der Personendaten zu fallen.[31]

---

[28] Vgl. Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 3 (insbesondere Ziff. 3.2).

[29] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2. (insbesondere Ziff. 2.1).

[30] Vgl. insbesondere folgende Kommentare zum DSG: Bruno BAERISWYL, Kurt PÄRLI, Dominika BLONSKI, Stämpflis Handkommentar SHK, Datenschutzgesetz (DSG), Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG), 2. Auflage, 2023; Philippe MEIER, Sylvain MÉTILLE, Commentaire romand sur la loi fédérale sur la protection des données, Helbing Lichtenhahn, 2023; Yaniv BENHAMOU, Bertil COTTIER, Petit commentaire LPD, Loi sur la protection des données, Helbing Lichtenhahn, 2023; Adrian BIERI, Julian POWELL, Orell Füssli Kommentar (OFK), DSG Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, 2023; David VASELLA, Gabor P. BLECHTA, Basler Kommentar (BSK) zum Datenschutzgesetz und Öffentlichkeitsgesetz, 4. Auflage, Basel 2024; Thomas STEINER, Anne-Sophie MORAND, Daniel HÜRLIMANN (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version: 25.08.2023: https://onlinekommentar.ch/de/kommentare/dsg43 (besucht am 12. Dezember 2023), DOI: 10.17176/20230825-103609-0.

[31] BGE **136** II 508 E. 3; Philippe MEIER / Nicolas TSCHUMY, *L'adresse IP: une donnée personnelle? Ou quand la CJUE rejoint le TF!*, in: Jusletter vom 23. Januar 2017, Rz. 22 ff.

Ein Bundesorgan ist grundsätzlich[32] nur dann zur Bearbeitung und Bekanntgabe von Personendaten berechtigt, wenn eine gesetzliche Grundlage besteht (Art. 5 Abs. 1 BV; Art. 34 Abs. 1 DSG).

2.3.2 Besonders schützenswerte Personendaten

Der Katalog mit den besonders schützenswerten Personendaten wird erweitert (Art. 5 Bst. c DSG). Er umfasst alle Kategorien von Daten, die im Sinne des aDSG als besonders schützenswert gelten, d. h. Personendaten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, administrative oder strafrechtliche Verfolgungen und Sanktionen sowie Massnahmen der sozialen Hilfe.

Der Katalog umfasst künftig auch die folgenden Kategorien[33]:

– die Daten über die Zugehörigkeit zu einer Ethnie;

– genetische Daten;

– biometrische Daten, die eine natürliche Person eindeutig identifizieren.

Grundsätzlich muss ein Gesetz im formellen Sinn die Bearbeitung von besonders schützenswerten Daten vorsehen (Art. 34 Abs. 2 Bst. a DSG; vgl. nachfolgend Ziff. 3.2.1).

2.3.3 Profiling

Das DSG definiert den Begriff des Profilings als eine besondere Form der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten (Art. 5 Bst. f DSG). Durch den Einsatz statistischer und mathematischer Methoden, insbesondere von Algorithmen, können aus einer grossen Menge von Daten, die für sich genommen möglicherweise nicht sehr informativ sind, neue Informationen über Einzelpersonen generiert werden. Der Begriff des Profilings ersetzt den Begriff des Persönlichkeitsprofils gemäss dem Gesetz von 1992, unterscheidet sich allerdings von diesem. Während ein Persönlichkeitsprofil das Ergebnis eines Bearbeitungsprozesses darstellt, beschreibt Profiling eine Methode zur Bearbeitung von Daten[34], d. h. eine automatisierte Bewertung bestimmter Aspekte einer natürlichen Person.[35]

---

[32] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1 (insbesondere *Ausnahmen vom Erfordernis der gesetzlichen Grundlage*).

[33] Vgl. dazu Bericht des BJ über die Totalrevision des DSG, Ziff. 2 (insbesondere Ziff. 2.2 sowie Ziff. 2.2.1, Bst. a).

[34] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2.1, Bst. b.

[35] Das Profiling stellt somit eine Technik zur Analyse und Vorhersage des menschlichen Verhaltens dar. Es beruht auf der Auswertung von Daten durch mathematische Modelle, sogenannte Algorithmen, die statistische, datenanalytische und wahrscheinlichkeitstheoretische Techniken anwenden. Diese Modelle bezwecken die Herstellung einer Korrelation zwischen bestimmten persönlichen und faktischen Merkmalen (Input) einerseits und einem bestimmten vorherzusagenden, zu beeinflussenden oder sogar zu erzwingenden Zustand oder Verhalten (Output) andererseits, vgl. Michael MONTAVON, Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyenne-s et des autorités de contrôle, Genf – Zürich – Basel 2021, S. 639.

Darüber hinaus hat das Parlament den Begriff des Profilings mit hohem Risiko eingeführt (Art. 5 Bst. g DSG). Diese Art von Profiling bringt ein hohes Risiko für die Persönlichkeit mit sich, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.[36] Diese Unterscheidung hat jedoch kaum Auswirkungen für Bundesorgane. Die Rechtsgrundlage, die Profiling (mit oder ohne hohes Risiko) durch Bundesorgane vorsieht, muss grundsätzlich ein Gesetz im formellen Sinn sein (Art. 34 Abs. 2 Bst. b DSG; vgl. nachfolgend Ziff. 3.2.2). Die Bearbeitung, einschliesslich der Bekanntgabe von Daten, die auf Profiling beruhen (vgl. nachfolgend Ziff. 3.2.4), sollte ebenfalls besonderen Anforderungen unterliegen.[37]

2.3.4 Automatisierte Einzelentscheidung

Das DSG definiert eine automatisierte Einzelentscheidung als eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung von Personendaten beruht und Rechtsfolgen für die betroffene Person hat oder diese erheblich beeinträchtigt (Art. 21 DSG).

Das bedeutet, dass die Beurteilung eines Sachverhalts und die daraus resultierende individuelle Entscheidung durch eine Maschine bzw. einen Algorithmus erfolgt, ohne dass eine natürliche Person mitwirkt.[38] In diesem Fall ist die Maschine nicht nur ein Werkzeug oder ein Hilfsmittel für die Entscheidung (vgl. nachfolgend Ziff. 2.3.5).[39]

Nur automatisierte Einzelentscheidungen, die eine gewisse Komplexität aufweisen, werden als solche betrachtet (und nicht z. B. die Kontrolle des Zugangs zu einem Gebäude auf der Grundlage einer Legitimationskarte).[40]

Der Einsatz der automatisierten Entscheidung kann (muss aber nicht) einen Fall von Artikel 34 Absatz 2 Buchstabe c DSG darstellen (d. h. als eine Bearbeitungsform angesehen werden, die die Grundrechte der betroffenen Person in schwerwiegender Weise beeinträchtigen kann). In diesem Fall muss ein Gesetz im formellen Sinn dies vorsehen.

2.3.5 Automatisierte Unterstützung der individuellen Entscheidfindung durch künstliche Intelligenz

Die automatisierte Unterstützung der individuellen Entscheidungsfindung durch Algorithmensysteme («***künstliche Intelligenz***»[41]) ist als solche im DSG nicht geregelt. Es liegt

---

[36] Sylvain MÉTILLE, *Le traitement des données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données vom 25. September 2021*, Sonderdruck der Semaine judiciaire 2021 II 1, S. 26.

[37] Zur Problematik der Bearbeitung von (nicht zwingend besonders schützenswerten) Daten, die auf Profiling beruhen, vgl. die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.1, Bst. b/dd).

[38] Zur Problematik der Zulässigkeit von automatisierten Einzelentscheidungen für den Fall, dass die Behörde über einen Ermessensspielraum verfügt, vgl. die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.1, Bst. c/cc [vgl. insbesondere *Fallgruppe 1: Automatisierte Einzelentscheidungen*]).

[39] *Ebd*.

[40] *Ebd*.

[41] Das schweizerische Recht definiert nicht, was künstliche Intelligenz ist. Auf internationaler Ebene geht die Tendenz eher dahin, den Begriff «Systeme der künstlichen Intelligenz» zu verwenden. Dabei handelt es sich laut dem Entwurf des Rahmenübereinkommens des Europarats über künstliche Intelligenz, Menschenrechte, Demokratie und Rechtsstaatlichkeit vom

keine automatisierte Einzelentscheidung im Sinne von Artikel 21 DSG vor, wenn diese zwar automatisiert vorbereitet, aber von einem Menschen getroffen wird.[42] Die rechtlichen Fragen, die oben im Zusammenhang mit automatisierten Einzelentscheidungen angesprochen wurden, können sich jedoch in analoger Weise stellen, wenn es um die automatisierte Unterstützung individueller Entscheidungen durch «künstliche Intelligenz» geht.[43]

Im gleichen Sinne wie vorstehend beschrieben kann (muss aber nicht) der Einsatz von *«künstlicher Intelligenz»* einen Fall von Artikel 34 Absatz 2 Buchstabe c DSG darstellen (d. h. als eine Bearbeitungsform angesehen werden, die die Grundrechte der betroffenen Person in schwerwiegender Weise beeinträchtigen kann). In diesem Fall muss ein Gesetz im formellen Sinn dies vorsehen.

2.3.6 Datenbearbeitung

Die Definition der Datenbearbeitung im Sinne von Artikel 5 Buchstabe d DSG wird inhaltlich nicht geändert, auch wenn sie nun ausdrücklich das Speichern und das Löschen mitumfasst.[44]

2.3.7 Verantwortlicher

Beim Verantwortlichen im Sinne von Artikel 5 Buchstabe j DSG handelt es sich um die private Person oder das Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet. Gemeint sind hier Faktoren und Risiken, die nach dem DSG relevant sind (z. B. welche Daten aus welchen Quellen, wie lange und auf welche Art und Weise bearbeitet werden[45]).

Dieser Begriff ersetzt jenen des Inhabers der Datensammlung. Wie der frühere Begriff des Inhabers der Datensammlung muss der Verantwortliche im bereichsspezifischen Gesetz genau bestimmt werden, da er für die Einhaltung der Datenschutzvorschriften verantwortlich ist und die betroffene Person bei ihm ihr Auskunftsrecht – ein Schlüsselelement des Datenschutzrechts – ausüben kann.[46]

---

14. März 2024 um *« un système informatique qui déduit, à partir des données qu'il reçoit et en fonction d'objectifs explicites ou implicites, comment générer des résultats tels que des prévisions, des contenus, des recommandations ou des décisions susceptibles d'influer sur des environnements matériels ou virtuels. Les différents systèmes d'intelligence artificielle varient dans leurs niveaux d'autonomie et d'adaptabilité après leur déploiement* ». Dieser Text basiert auf der überarbeiteten Definition des Begriffs «System der künstlichen Intelligenz», die von der OECD am 8. November 2023 angenommen wurde (siehe Empfehlung des Rates zur künstlichen Intelligenz). Die Definition entspricht weitgehend der Definition im Entwurf der EU-Verordnung über künstliche Intelligenz (KOM [2021] 206 final). Da es im schweizerischen Recht keine eigene Definition gibt, kann man sich an diesen Umschreibungen orientieren.

[42] Vgl. Bericht des BJ über die Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.1, Bst. c/cc [vgl. insbesondere: *Fallgruppe 2: Unterstützender Einsatz von künstlicher Intelligenz*]).

[43] *Ebd*.

[44] Botschaft über die Totalrevision des DSG, S. 7021.

[45] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4 (insbesondere Ziff. 4.1).

[46] *« L'obligation d'information est complétée par le droit d'accès. Le droit d'accès est un élément clé du droit de la protection des données car il permet à la personne concernée de faire valoir les droits que lui octroie la loi »,* vgl. Sylvain MÉTILLE, *Le*

Artikel 3 des Bundesgesetzes über die Informationssysteme des Bundes im Bereich Sport[47] sieht beispielsweise Folgendes vor:

> *«Das BASPO ist für die Sicherheit der Informationssysteme und die Rechtmässigkeit der Bearbeitung der Daten verantwortlich.»*

Der Bundesrat regelt in einer Verordnung die Kontrollverfahren und die Verantwortung für den Datenschutz, wenn ein verantwortliches Bundesorgan Personendaten zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit privaten Personen bearbeitet (Art. 33 DSG).

Das DSG erweitert bestimmte Pflichten des Verantwortlichen oder auferlegt ihm neue Pflichten (Art. 19–24 DSG)[48], insbesondere die Pflicht, eine Folgenabschätzung durchzuführen, wenn die geplante Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann.[49]

2.3.8 Auftragsbearbeiter

Auftragsbearbeiter im Sinne von Artikel 5 Buchstabe k DSG ist die private Person oder das Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

Bundesorgane können die Bearbeitung von Personendaten vertraglich oder durch die Gesetzgebung auf einen Auftragsbearbeiter übertragen (Art. 9 DSG). Dies entbindet sie nicht von der Pflicht, die datenschutzrechtliche Verantwortung wahrzunehmen.[50]

Die Auftragsbearbeitung kann sich im Übrigen auch auf IT-Dienste für die Datenbearbeitung in der Cloud beziehen, die mit besonderen Risiken verbunden ist[51] und insbesondere Garantien sowie technische und organisatorische Massnahmen voraussetzt.

2.3.9 Dritte

Der Begriff des Dritten wird im DSG nicht ausdrücklich definiert. Es handelt sich beim Dritten um eine private Person, ein Bundesorgan oder ein kantonales Organ, welche bzw. welches

---

traitement des données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données vom 25. September 2021, Sonderdruck der Semaine judiciaire 2021 II 1, S. 30.

[47] SR **415.1** – Bundesgesetz vom 19. Juni 2015 über die Informationssysteme des Bundes im Bereich Sport (IBSG) (admin.ch)

[48] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 1.2.

[49] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4.3, sowie vgl. Buchstabe B der Einführung oben und die Richtlinien des Bundesrates vom 28. Juni 2023 für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung (DSFA-Richtlinien), BBl **2023** 1882.

[50] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4 (insbesondere Ziff. 4.1).

[51] Vgl. Sylvain MÉTILLE, Utilisation de l'informatique en nuage par l'administration publique, AJP/PJA 6/2019, S. 609 f.; siehe auch Cloud Computing, Datenschutzrechtliche Rahmenbedingungen am Beispiel des Kantons Zürich, in: Künstliche Intelligenz und Datenschutz, Schulthess, 2021 S. 65 ff.

weder Verantwortlicher noch Auftragsbearbeiter ist. Anders als im Gesetz von 1992 (vgl. Art. 10*a* aDSG) gilt der Auftragsbearbeiter nicht mehr als Dritter (Art. 9 DSG *e contrario*).[52]

2.3.10 Bearbeitungstätigkeit

Der Begriff der Bearbeitungstätigkeit ersetzt im DSG (Art. 12 DSG) jenen der Datensammlung im Gesetz von 1992 (Art. 11*a* aDSG). Die Bundesorgane müssen Verzeichnisse ihrer Bearbeitungstätigkeiten führen und diese dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten melden (Art. 12 DSG).

2.4 Grundsätze

Das DSG übernimmt im Wesentlichen die bestehenden Grundsätze. Jede Bearbeitung von Personendaten natürlicher Personen muss die allgemeinen datenschutzrechtlichen Prinzipien (Art. 6–8 DSG) respektieren, d. h. die Grundsätze der Rechtmässigkeit (Art. 6 Abs. 1 DSG), von Treu und Glauben (Art. 6 Abs. 2 und Abs. 4 DSG), der Verhältnismässigkeit (Art. 6 Abs. 2 DSG), der Erkennbarkeit (Art. 6 Abs. 3 DSG), der Zweckbindung (Art. 6 Abs. 3 DSG), der Richtigkeit (Art. 6 Abs. 5 DSG) und der Datensicherheit (Art. 8 DSG).[53]

Die Einhaltung des Grundsatzes der Rechtmässigkeit wird meist in Verbindung mit dem Erfordernis der gesetzlichen Grundlage, die den Bundesorganen die Bearbeitung von Personendaten erlaubt, geprüft werden.

Der Grundsatz der Verhältnismässigkeit umfasst den Grundsatz der Datenminimierung, gemäss dem der Verantwortliche nur die Daten beschafft und bearbeitet, die für die Bearbeitung erforderlich sind**.** Die beschafften Daten müssen in einem angemessenen Verhältnis zu den Bedürfnissen der Bearbeitung stehen. Anders ausgedrückt *«müssen die gespeicherten Informationen für den Zweck der Datensammlung relevant und unbedingt erforderlich sein» [Zitat aus dem Französischen übersetzt]*[54]. Dieser Grundsatz muss vom Verantwortlichen bereits bei der Planung der Bearbeitung berücksichtigt werden.

Der Grundsatz der Zweckbindung erfährt keine grösseren inhaltlichen Änderungen[55], doch wird der Wortlaut besser an Artikel 5 der modernisierten Datenschutzkonvention 108+ des Europarats (und der DSGVO) angepasst. Nach Artikel 6 Absatz 3 DSG dürfen Daten nur für bestimmte und für die betroffene Person erkennbare Zwecke erhoben werden und müssen in einer mit diesen Zwecken zu vereinbarenden Weise weiterverarbeitet werden. Artikel 4 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs, BÜPF[56], in

---

[52] Vgl. die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4 (insbesondere Ziff. 4.1).

[53] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1 (insbesondere *Anforderungen an die Normdichte*).

[54] Vgl. Art. 5 Bst. c DSGVO, vgl. auch die fünf grossen Datenschutzprinzipien gemäss der französischen Commission nationale de l'informatique et des libertés, Quels sont les grands principes des règles de protection des données personnelles? | Besoin d'aide | CNIL.

[55] Botschaft über die Totalrevision des DSG, S. 7025.

[56] SR **780.1** – Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) (admin.ch)

der durch das DSG geänderten Fassung[57], sieht beispielsweise vor, dass bestimmte, in der Gesetzesbestimmung bezeichnete Stellen und Behörden nur Daten bearbeiten dürfen, *«die sie benötigen, um Überwachungen anzuordnen, zu genehmigen und durchzuführen.»*

Bei der Datenaufbewahrung sind insbesondere die Grundsätze der Verhältnismässigkeit und der Zweckbindung einzuhalten. Der Gesetzgeber muss die Datenbearbeitung auf die für die Erfüllung einer bestimmten Aufgabe erforderliche Dauer beschränken (und nicht bis es allenfalls nützlich sein könnte), indem er Aufbewahrungsfristen festlegt.[58]

Die Botschaft des Bundesrates geht vom Grundsatz aus, dass ein bestimmter, in einem Gesetz vorgesehener Zweck für die betroffene Person grundsätzlich erkennbar ist.[59] Ein Gesetz kann somit den ursprünglichen Zweck der Datenbearbeitung in einem gewissen Masse ändern. Die Beachtung des Prinzips von Treu und Glauben bleibt vorbehalten.

Artikel 96*d* des Arbeitslosenversicherungsgesetzes[60] sieht z. B. vor:

> *«Die Durchführungsstellen nach Artikel 76 Absatz 1 Buchstaben a und c dürfen mittels Abrufverfahren auf das Einwohnerregister zugreifen, um den Wohnort der versicherten Person zu überprüfen, sofern das kantonale Recht sie dazu ermächtigt.»*

Das DSG führt darüber hinaus die Grundsätze des Datenschutzes durch Technik[61] und datenschutzfreundliche Voreinstellungen ein (Art. 7 DSG). Diese Grundsätze sind teilweise neu (sie leiten sich zum Teil aus den bestehenden Grundsätzen der Verhältnismässigkeit und der Datensicherheit ab).

III Fragen bei der Ausgestaltung einer gesetzlichen Grundlage für die Bearbeitung von Personendaten durch Bundesorgane

3.1 Vorbemerkungen und Anforderungen des Legalitätsprinzips

Nach der Anfangsphase des Projekts bleiben die Fragen, die sich bei der Ausgestaltung einer gesetzlichen Grundlage für die Bearbeitung von Personendaten durch Bundesorgane stellen, teilweise gleich wie unter dem Gesetz von 1992.

Dazu gehören insbesondere die Frage, ob eine Bearbeitung von Personendaten und/oder besonders schützenswerten Personendaten geplant ist, die Prüfung der Schwere eines

---

[57] BBl **2020** 7639 S. 7711

[58] Thomas HELD, Markus BRÖNIMANN, in Orell Füssli Kommentar (OFK) DSG Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, 2023, Hrsg. Adrian BIERI, Julian POWELL, zu Art. 34 N.°9–10 und die zitierte Rechtsprechung.

[59] Vgl. die Botschaft über die Totalrevision des DSG, S. 7025: *«Ist die Änderung des anfänglichen Zwecks gesetzlich vorgesehen, wird sie durch eine Gesetzesänderung verlangt oder ist sie durch einen anderen Rechtfertigungsgrund legitimiert (z. B. durch die Einwilligung der betroffenen Person), so gilt die Weiterbearbeitung ebenfalls als mit dem anfänglichen Zweck vereinbar.»*

[60] SR **837.0** – Bundesgesetz vom 25. Juni 1982 über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung (Arbeitslosenversicherungsgesetz, AVIG) (admin.ch)

[61] Vgl. dazu Sylvain MÉTILLE, 9. November 2020, La notion de protection des données dès la conception – swissprivacy.law.

Eingriffs in die Grundrechte der betroffenen Personen sowie die Bestimmung des Zwecks der Datenbearbeitungen, wobei die Anforderungen des Legalitätsprinzips im Auge zu behalten sind (siehe auch Ziff. 2.3 oben).

Wenn keine neuen staatlichen Aufgaben zur Diskussion stehen, d. h. wenn bereits eine Rechtsgrundlage für die zur Erfüllung dieser Aufgaben erforderlichen Datenbearbeitungen besteht, aber ein neues Konzept der Datenbearbeitung geplant ist, muss zunächst die aktuelle Situation (*«Ist»*) analysiert und mit der geplanten Situation (*«Soll»*) verglichen werden. So lässt sich feststellen, ob die betreffende Situation neue Datenbearbeitungen nach sich zieht und/oder neue Risiken für die betroffenen Personen birgt. Die Antwort auf diese Frage führt den Juristen bzw. die Juristin zur Frage nach der Normstufe und der Normdichte der zu erarbeitenden Rechtsgrundlagen.

3.1.1 Anforderungen des Legalitätsprinzips

Das Legalitätsprinzip verlangt eine hinreichende Bestimmtheit der gesetzlichen Normen. Diese müssen so präzise formuliert sein, dass die Rechtsunterworfenen ihr Verhalten danach ausrichten und die Folgen eines bestimmten Verhaltens mit einem den Umständen entsprechenden Grad an Gewissheit erkennen können.[62]

Die Rechtsgrundlage, die eine Bearbeitung von Personendaten durch Bundesorgane vorsieht, muss es der betroffenen Person somit ermöglichen zu erkennen, welches Bundesorgan welche Datenkategorien zu welchem Zweck (wer, was, warum) bearbeitet und in manchen Fällen auch, welches die Bearbeitungsform ist, insbesondere bei einem Online-Zugriff.

Die Rechtsgrundlage muss nämlich auch Hinweise auf die Bearbeitungsform geben, insbesondere wenn technologische Mittel verwendet werden, die für die rechtsunterworfene Person nicht erkennbar sind, und wenn der Einsatz dieser Mittel Auswirkungen auf die Grundrechte haben kann[63]. Zum Beispiel, wenn das Risiko einer Diskriminierung aufgrund der Bearbeitung von Daten durch einen Algorithmus[64] oder das Risiko einer Beeinträchtigung der persönlichen Freiheit aufgrund des Einsatzes von Überwachungsinstrumenten im öffentlichen Raum besteht. Je schwerwiegender der Eingriff in die Grundrechte sein kann, desto präziser muss die Rechtsgrundlage sein. Ist hingegen die Datenbearbeitung der von der Behörde ausgeführten Aufgabe inhärent und erweist sich das Risiko einer Grundrechtsverletzung als minimal, z. B. wenn der Behörde die Gewährung finanzieller Unterstützung obliegt, ist eine ausdrückliche Rechtsgrundlage für die Bearbeitung von Personendaten nicht zwingend erforderlich, und eine etwaige spezifische Rechtsgrundlage für die Bekanntgabe kann relativ allgemein gehalten sein.

---

[62] BGE **146** I 11, **136** I 87; DUBEY Jacques, Petit commentaire Constitution, N. 79 zu Art. 36.

[63] Monique COSSALI SAUVAIN, in Petit commentaire LPD, Loi sur la protection des données, Hrsg. Yaniv BENHAMOU, Bertil COTTIER, Helbing Lichtenhahn, 2023, zu Art. 34 N. 13.

[64] Frederik J. ZUIDERVEEN BORGESIUS, Discrimination, artificial intelligence and algorithmic decision-making, S. 13 ff. und 36.

3.1.2 Bekanntgabe von Daten und Legalitätsprinzip

Die Bekanntgabe von Daten muss ausdrücklich in einer gesetzlichen Grundlage vorgesehen sein (Art. 36 DSG). Sie erfordert daher eine spezifische Rechtsgrundlage (siehe nachfolgend Ziff. 3.2.4), die bestimmt, wer Zugang zu den Daten hat, an wen und zu welchem Zweck die Daten gegebenenfalls bekanntgegeben werden dürfen, sowie die Art und Weise der Bekanntgabe und den Umfang der Bearbeitung in groben Zügen (wer, was, an wen, warum, wie).

Beispielsweise sieht Artikel 20*b* Absatz 1 des Bundesgesetzes über die Eidgenössischen Technischen Hochschulen[65] Folgendes vor:

> *«Der ETH-Rat, die ETH und die Forschungsanstalten können Organen von in- und ausländischen Hochschulen, Forschungs- und Forschungsförderungsinstitutionen, die für die Aufdeckung und Sanktionierung wissenschaftlichen Fehlverhaltens zuständig sind, im Einzelfall und auf konkrete schriftliche Anfrage hin Auskünfte darüber erteilen:*
>
> > *a. ob ihre Angehörigen gegen die Regeln der wissenschaftlichen Integrität und der guten wissenschaftlichen Praxis verstossen haben oder ein begründeter Verdacht auf einen solchen Verstoss vorliegt;*
> >
> > *b. welche Sanktionen gegen die entsprechenden Personen verhängt wurden.»*

Artikel 20*c* dieses Gesetzes bestimmt, dass die betroffene Person schriftlich informiert werden muss.

3.1.3 IT-Architektur und Legalitätsprinzip

Die Frage, inwieweit die Architektur eines Informationssystems in den Rechtsgrundlagen zu beschreiben ist, stellte sich unter dem Gesetz von 1992 in besonderer Weise vor allem für Verwaltungseinheiten, die Microservices anstelle von Silosystemen einsetzen.

Ein Abrufverfahren liegt vor, wenn mehrere Verwaltungsstellen dasselbe Informatiksystem nutzen, oder wenn Dritte gegenüber dem Verantwortlichen nach dem Prinzip der Selbstbedienung Zugriff auf die Daten haben. In diesem Fall bleibt der Verantwortliche passiv, da er nicht unbedingt weiss, dass jemand Zugriff auf gewisse Daten hatte. Das DSG sieht den Begriff des Abrufverfahrens im Sinne von Artikel 19 Absatz 3 aDSG nicht mehr vor.[66] Diese Änderung führt indessen nicht zu einer Schwächung des Datenschutzes.[67] Es handelt sich um eine Form der Bekanntgabe, die als solche im Gesetz vorgesehen sein muss. Der Online-Zugriff nach dem Prinzip der Selbstbedienung kann zu einer besonders schwerwiegenden Beeinträchtigung der Grundrechte der betroffenen Person führen und muss in einem Gesetz im formellen Sinn vorgesehen sein, jedenfalls, wenn er besonders

---

[65] SR **414.110** - Bundesgesetz vom 4. Oktober 1991 über die Eidgenössischen Technischen Hochschulen

[66] Kritisch in Bezug auf diese Änderung Michael MONTAVON, L'abandon de la procédure d'appel en protection des données, *in:* LeGes 31 (2020) 2 S. 1–10.

[67] Botschaft über die Totalrevision des DSG, S. 7083.

schützenswerte oder auf Profiling beruhende Personendaten betrifft. Er kann in einem Gesetz im materiellen Sinn enthalten sein, wenn der Verantwortliche online Zugriff auf nicht besonders schützenswerte Personendaten gibt und die Wahrscheinlichkeit einer Beeinträchtigung der Grundrechte gering ist. Der Grundsatz der Zweckbindung verlangt einen engen Bezug zwischen dem Online-Zugriff und der jeweiligen Aufgabe der Behörde, für die er notwendig ist. Eine Behörde x greift zum Beispiel online auf die Datenkategorie y zu, um eine in Artikel z eines Gesetzes vorgesehene Aufgabe auszuführen. Eine andere Behörde a greift online auf die Datenkategorie b zu, um eine in Artikel d eines Gesetzes vorgesehene Aufgabe c zu erledigen. Je höher das Risiko eines Grundrechtsverletzung ist, desto genauer müssen die notwendigen Rechtsgrundlagen für einen Online-Zugriff sein. Die Schwere der Verletzung beurteilt sich nach der Art der bearbeiteten Daten und dem Zweck der Datenbearbeitung.

Bei der Ausarbeitung der Regelung über die Datenbearbeitung liegt der Schwerpunkt somit weniger auf der (technischen) Informatikarchitektur als auf der *«Datenbearbeitungsarchitektur»*, d. h. den Bearbeitungszwecken und der Bearbeitungslogik sowie den Datenflüssen und dem Online-Zugriff auf die Daten (wer hat Zugang zu welchen Daten).[68] Wenn Daten zur Erfüllung mehrerer gesetzlicher Aufgaben bearbeitet werden, muss bei der entsprechenden Regelung nach Massgabe dieser Aufgaben differenziert werden, damit ersichtlich ist, wer welche Bearbeitung zur Erfüllung welcher gesetzlichen Aufgabe durchführen darf und wie diese Bearbeitung erfolgt.

Bei mehreren gesetzlichen Aufgaben ist es wichtig, dass das Gesetz klar unterscheidet, für welche gesetzliche Aufgabe welche Personendaten bearbeitet werden dürfen und wem dieses Recht zusteht. Dies ist umso wichtiger, als in modernen Systemen «*Silo-Lösungen*» durch anders strukturierte Lösungen ersetzt werden (wie erwähnt z. B. «*Microservices*») und das Gesetz in Bezug auf die Technologie neutral bleiben muss. Deshalb ist es notwendig, die Bearbeitung von Personendaten nach Massgabe der zu erfüllenden Aufgaben zu regeln.

Artikel 9 Absatz 1 des Bundesgesetzes über das elektronische Patientendossier[69] sieht zum Beispiel Folgendes vor:

> *«Gesundheitsfachpersonen können auf die Daten von Patientinnen oder Patienten zugreifen, soweit diese ihnen Zugriffsrechte erteilt haben.»*

3.1.4 Informationspflicht und Legalitätsprinzip

Darüber hinaus sieht das DSG weiterhin eine Informationspflicht vor, die die Transparenz der Bearbeitung erhöht. Das für die Bearbeitung verantwortliche Bundesorgan ist jedoch von der Informationspflicht entbunden, wenn die Bearbeitung gesetzlich vorgeschrieben ist.[70] Das

---

[68] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1.

[69] SR **816.1** – Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier (EPDG) (admin.ch)

[70] Vgl. dazu Bertil COTTIER, Transparence des traitements de données personnelles opérés par les organes fédéraux: un pas en avant, deux en arrière, SZW 2021 S. 65 ff., 70, der die restriktiven Ausnahmen von der Informationspflicht nach Art. 18*a* aDSG mit der weiten Ausnahme nach Art. 20 Abs. 1 Bst. b nDSG vergleicht und dabei zu folgendem Schluss kommt (S. 72):

« Reste que cette regrettable exemption n'est en soi pas contraire au droit international supérieur: […], la convention 108 modernisée la prévoit déjà, au motif implicite que «Nul n'est censé ignorer la loi». Cela dit, comme le souligne la doctrine, cet adage permet certes de considérer que les citoyens sont déjà informés, mais cela n'est valable qu'à la condition que la loi en

Gesetz muss daher die für die Durchsetzung der Rechte der betroffenen Person notwendigen Informationen vorsehen und die Transparenz der Bearbeitung gewährleisten.[71]

Eine gesetzliche Bestimmung im Stile von Artikel 7*a* Absatz 3 des Bundesgesetzes über das Informationssystem für den Ausländer- und den Asylbereich[72], die in allgemeiner Weise vorsieht:

> *«Folgende Behörden oder Stellen können zur Erfüllung ihrer gesetzlichen Aufgaben biometrische Daten im Informationssystem bearbeiten:*
>
> *[…]*
>
> *g. das SIRENE-Büro von fedpol»;*

würde wahrscheinlich nicht mehr als ausreichende Information für die betroffene Person angesehen werden.

Die Zusammenarbeit mit den Informatikern und Informatikerinnen, die für die technische Umsetzung der Datenbearbeitung verantwortlich sind, bleibt somit entscheidend, um das informationstechnische Potenzial eines Datenbearbeitungsprojekts in einem bestimmten Masse zu erfassen. Der Verantwortliche muss im Übrigen bereits bei der Planung der Bearbeitung geeignete technische und organisatorische Massnahmen ergreifen, damit die Bearbeitung den Datenschutzgrundsätzen entspricht und die erforderlichen Garantien zum Schutz der Rechte der betroffenen Person bietet[73].

Ausgehend von diesem Ansatz müssen bei der Ausgestaltung einer Regelung, die Bundesorganen die Bearbeitung personenbezogener Daten erlaubt, insbesondere zwei Fragen beantwortet werden: die Frage nach der Normstufe und jene nach der Normdichte der geplanten Bestimmungen. Die Antworten auf diese Fragen hängen von den Eigenheiten der zu regelnden Materie ab. Sie sind weder schematisch noch sollten sie zu einer unverhältnismässigen Regelung führen.

3.1.5 Geschäftsverwaltungssysteme

Artikel 57*h* des Regierungs- und Verwaltungsorganisationsgesetzes, RVOG[74], in der durch das DSG geänderten Fassung[75], enthält die gesetzliche Grundlage, gestützt auf welche Einheiten der Bundesverwaltung elektronische Systeme betreiben können, um ihre Geschäftsprozesse reibungslos abzuwickeln und Dokumente zu verwalten. Sie können anderen Bundesbehörden sowie bundesexternen Stellen (z. B. kantonalen Dienststellen)

---

question soit suffisamment précise et apporte les renseignements nécessaires pour assurer une information loyale de personnes concernées ».

[71] Botschaft über die Totalrevision des DSG, S. 7051 und 7053; vgl. auch Claudius ETTLINGER, Die Informationspflicht gemäss neuem Datenschutzgesetz, in: Jusletter IT vom 16. Dezember 2021.

[72] SR **142.51** – Bundesgesetz vom 20. Juni 2023 über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA) (admin.ch)

[73] Art. 7 DSG, vgl. Sylvain MÉTILLE, La notion de protection des données dès la conception, 9. November 2020 in www.swissprivacy.law/26.

[74] SR **172.010** – Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG)

[75] BBl **2020** 7679

einen eingeschränkten Zugriff auf ihre eigenen Geschäftsverwaltungssysteme gewähren, soweit dieser für den reibungslosen Ablauf ihrer Geschäftsprozesse erforderlich ist (z. B. im Rahmen der Ämterkonsultation).

Die Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung, die GEVER-Verordnung[76], konkretisiert den Zweck und den Inhalt von elektronischen Geschäftsverwaltungssystemen. Sie sieht grundsätzlich die Verwendung des standardisierten GEVER vor, erlaubt aber unter bestimmten Bedingungen auch nicht standardisierte Geschäftsverwaltungssysteme (Art. 3).

Bei Bestehen eines Geschäftsverwaltungssystems kann auf den Erlass neuer Vorschriften verzichtet werden, wenn sich die Datenbearbeitung auf das RVOG und die GEVER-Verordnung stützen lässt. Dies setzt voraus, dass die betreffende allgemeine Regelung in ihrer Gesamtheit, einschliesslich allfälliger bereichsspezifischer Bestimmungen, ausreicht, um die Datenbearbeitung für die betroffene Person erkennbar zu machen.

3.1.6 Pilotprojekte

Das DSG sieht weiterhin die Möglichkeit vor, Pilotprojekte durchzuführen, für die die Anforderungen des Legalitätsprinzips gelockert werden.[77]

3.2 Normstufe (Gesetz im formellen Sinn oder Regelung in einer Verordnung) und Normdichte

Das Risiko eines Grundrechtseingriffs hat Auswirkungen auf die Frage nach der Normstufe der geplanten Regelung (Gesetz im formellen Sinn oder Regelung in einer Verordnung) sowie auf die Frage nach der Normdichte. Diese beiden Fragen sind somit bei der Bearbeitung und bei der Bekanntgabe von Personendaten, die eine besondere Form der Bearbeitung darstellt, gemeinsam zu behandeln.

3.2.1 Bearbeitung besonders schützenswerter Daten

Gemäss Artikel 34 Absatz 2 Buchstabe a DSG muss ein Gesetz im formellen Sinn die Bearbeitung von besonders schützenswerten Daten im Sinne von Artikel 5 Buchstabe c Ziffern 1–6 DSG vorsehen (vgl. oben Ziff. 2.3.2). Zur Wahrung des Legalitätsprinzips sowie der Transparenz der Datenbearbeitung gegenüber der betroffenen Person muss das Gesetz im formellen Sinn die Kategorien der bearbeiteten besonders schützenswerten Daten nach Artikel 5 Buchstabe c Ziffern 1–6 DSG aufzählen. Gemäss dem Grundsatz der Verhältnismässigkeit dürfen nur die Kategorien besonders schützenswerter Daten bearbeitet werden, die für die Erfüllung einer gesetzlichen Aufgabe unerlässlich sind. Es sollen also nach Möglichkeit Unterkategorien der in Artikel 5 Buchstabe c Ziffern 1–6 DSG aufgeführten Kategorien geschaffen werden; z. B. ist im Bereich der Gesundheitsdaten zu präzisieren,

[76] SR **172.010.441** – Verordnung vom 3. April 2019 über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung)

[77] Art. 35 DSG, vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1.

dass nur Daten über Krebs bearbeitet werden[78] (vgl. Art. 3 des Bundesgesetzes über die Registrierung von Krebserkrankungen).[79]

Zur Frage der Normdichte: Je höher das Risiko einer Verletzung der Persönlichkeit oder der Grundrechte ist, desto höher muss der Präzisionsgrad der gesetzlichen Bestimmung sein, und desto genauer und für die betroffene Person erkennbarer muss der Zweck der Bearbeitung definiert werden.

Die vorstehend beschriebenen Bestimmungen entsprechen dem bisherigen Recht. In Artikel 34 Absatz 3 DSG hat der Gesetzgeber jedoch den Bundesrat neu ermächtigt, eine gesetzliche Grundlage im materiellen Sinn zu erlassen, welche die Bearbeitung besonders schützenswerter Daten zulässt, wenn zwei kumulative Bedingungen erfüllt sind:

> – Die Bearbeitung muss für die Erfüllung einer gesetzlichen Aufgabe, die in einem Gesetz im formellen Sinn festgelegt ist, unentbehrlich sein. Die Aufgabe muss ausdrücklich in einem Gesetz im formellen Sinn definiert und ihr Umfang für die betroffene Person erkennbar sein.[80]
>
> – Der Zweck der Bearbeitung stellt keine besonderen Risiken für die Grundrechte der betroffenen Person dar, insbesondere nicht für die Achtung ihrer Privatsphäre (vgl. Art. 13 und 36 Abs. 1 BV; vgl. oben Ziff. 1.1). Darüber hinaus ist auch zu prüfen, ob die Art und Weise der Datenbearbeitung nicht zu einer schwerwiegenden Beeinträchtigung der Grundrechte führen kann (vgl. Art. 34 Abs. 2 Bst. c DSG).

Nur wenn alle diese Voraussetzungen erfüllt sind, kommt eine Regelung in einer Verordnung im Sinne von Artikel 34 Absatz 3 DSG in Betracht.

3.2.2 Profiling (Art. 34 Abs. 2 Bst. b DSG)

Die oben dargestellten Erwägungen sind auf das Profiling anwendbar. Der Bundesrat war der Ansicht, dass die Rechtsgrundlage für das Profiling auf derselben Stufe bestehen muss wie im Fall der Bearbeitung besonders schützenswerter Daten.[81] Bundesorgane sind demnach nur dann zum Profiling befugt, wenn ein Gesetz im formellen Sinn dies vorsieht. Bei der Prüfung, ob der Grundsatz der Verhältnismässigkeit eingehalten ist, geht es insbesondere um die Frage, ob nicht andere Möglichkeiten der Datenbearbeitung in Frage kommen könnten, die die Persönlichkeit der betroffenen Personen besser schützen.[82]

Das Erfordernis der formellen gesetzlichen Grundlage gilt nicht absolut; Artikel 34 Absatz 3 DSG, der oben (vgl. Ziff. 3.2.1) im Zusammenhang mit der Bearbeitung besonders schützenswerter Daten kommentiert wurde, ist auch auf das Profiling anwendbar.

---

[78] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.1 Bst. a).

[79] SR **818.33** – Bundesgesetz vom 18. März 2016 über die Registrierung von Krebserkrankungen (Krebsregistrierungsgesetz, KRG) (admin.ch)

[80] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.1 Bst. a).

[81] Botschaft über die Totalrevision des DSG, S. 7078 ff.

[82] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.1 Bst. b/dd).

Die Rechtsgrundlage muss hinreichend präzise sein. Dies setzt voraus, dass die Rechtsgrundlage das Profiling im Sinne von Artikel 5 Buchstabe f DSG ausdrücklich vorsieht oder es angemessen beschreibt. Sie muss zumindest den Zweck des Profilings und die Kategorien von Daten angeben, die im Profiling verwendet werden. Die betroffene Person sollte auch in der Lage sein, die Merkmale ihrer Person zu erkennen, die durch das Profiling bewertet werden. Es gilt das Recht auf informationelle Selbstbestimmung; die von einem individuellen Profiling betroffene Person muss ihr Auskunftsrecht ausüben und von den Bundesorganen Informationen erhalten können, die es ihr ermöglichen, die Logik des über sie durchgeführten Profilings zu verstehen. Die Bundesorgane sind darüber hinaus verpflichtet, technische und organisatorische Massnahmen zu ergreifen, um das Risiko von Fehlern[83], Verstössen gegen das Diskriminierungsverbot[84] oder das Willkürverbot zu minimieren.

Artikel 21*c* Absatz 1 Buchstabe b und Absatz 1bis des Bundesgesetzes über die Luftfahrt[85] in der durch das DSG geänderten Fassung[86] sieht z. B. Folgendes vor:

> «*Im Informationssystem werden folgende Daten über sicherheitsrelevante Ereignisse und damit in Verbindung stehende mögliche Gefährder bearbeitet:*
>
> *[…]*
>
> *b. Personendaten, die für die Beurteilung der Gefährdung des internationalen gewerbsmässigen Luftverkehrs notwendig sind, einschliesslich besonders schützenswerter Personendaten, wie Informationen über den Gesundheitszustand, über Verurteilungen oder hängige Straf- oder Verwaltungsverfahren und über die Zugehörigkeit zu kriminellen oder terroristischen Gruppierungen».*

Gemäss Absatz 1bis ist fedpol «*zur Beurteilung des Gefährlichkeitsgrades der in Absatz 1 genannten Personen […] zum Profiling […] nach dem Datenschutzgesetz vom 25. September 2020 befugt».*

3.2.3 Risiko eines schweren Grundrechtseingriffs aufgrund des Zwecks oder der Art und Weise der geplanten Bearbeitung (Art. 34 Abs. 2 Bst. c DSG)

Das DSG hält ausdrücklich fest, dass ein Gesetz im formellen Sinn erforderlich ist, wenn der Zweck der Bearbeitung von Personendaten oder die Art und Weise der Bearbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen können (Art. 36 Abs. 1 BV). Dies unabhängig davon, ob eine Bearbeitung besonders

---

[83] In Anwendung des Grundsatzes der Richtigkeit (vgl. Art. 6 Abs. 5 DSG von 2020) muss der Verantwortliche, der Profiling-Aktivitäten durchführt, sicherstellen, dass die von ihm verwendeten Daten im Hinblick auf die verfolgten Zwecke inhaltlich richtig und dass die aus dem Profiling gezogenen Schlussfolgerungen hinreichend zuverlässig sind. Da Profiling-Aktivitäten notwendigerweise eine gewisse Fehlerquote beinhalten, muss der Verantwortliche geeignete Massnahmen ergreifen, um Ungenauigkeitsfaktoren sowohl bei den verwendeten Daten als auch bei den erstellten Vorhersagen auszuschliessen, vgl. Michael MONTAVON, Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyen-ne-s et des autorités de contrôle, Genf – Zürich – Basel 2021, S. 647.

[84] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.1, Bst. b/dd).

[85] SR **748.0** – Bundesgesetz vom 21. Dezember 1948 über die Luftfahrt (Luftfahrtgesetz, LFG) (admin.ch)

[86] BBl **2020** 7710

schützenswerter Daten oder ein Profiling geplant ist. Das Risiko eines ernsthaften Eingriffs kann sich aus dem Zweck der geplanten Bearbeitung ergeben (z. B. zur Beurteilung der Gefährlichkeit einer Person[87]). Es kann sich auch aus der Art und Weise der geplanten Bearbeitung ergeben, insbesondere bei automatisierten Einzelentscheidungen und beim Einsatz von *«künstlicher Intelligenz»* ohne automatisierte Einzelentscheidung. Ein Beispiel für eine automatisierte Entscheidung wäre etwa eine vollautomatische Steuerveranlagung. Wird die Steuerveranlagung hingegen von einer natürlichen Person vorgenommen, von der zuständigen Person dabei aber ein Algorithmus verwendet, der sie auf mögliche Unstimmigkeiten in der Steuererklärung hinweist, würde es sich um den Einsatz künstlicher Intelligenz ohne automatisierte Entscheidung handeln.

Unter bestimmten Voraussetzungen können automatisierte Einzelentscheidungen einen schwerwiegenden Eingriff in die Grundrechte der betroffenen Person im Sinne von Artikel 34 Absatz 2 Buchstabe c DSG darstellen und müssen daher in einem Gesetz im formellen Sinn vorgesehen sein. Sie können auch als wichtige Fragen der Organisation und des Verfahrens der Bundesbehörden angesehen werden, für die nach Artikel 164 Absatz 1 Buchstabe g BV eine formell-gesetzliche Grundlage erforderlich ist.[88] Die Gesetzesgrundlage muss die automatisierte Einzelentscheidung ausdrücklich vorsehen oder sie angemessen beschreiben. Die Logik, die hinter der automatisierten Entscheidung steckt, muss für die betroffene Person in groben Zügen erkennbar sein.[89]

Der Einsatz von *«künstlicher Intelligenz»* durch die Verwaltung zur Vorbereitung von Entscheidungen ist derzeit nicht speziell geregelt.[90] Auf Bundesebene hat der Bundesrat am 25. November 2020 die Leitlinien *«Künstliche Intelligenz»* erlassen.[91] Diese stellen insbesondere den Menschen in den Mittelpunkt und erörtern den rechtlichen Rahmen für die Achtung der Grundrechte, ohne Kriterien zu liefern, die in der Gesetzgebung umgesetzt werden könnten.[92]

3.2.4 Bekanntgabe von Personendaten einschliesslich Zugriffe auf Personendaten

Die Bekanntgabe von Personendaten stellt eine Bearbeitung von Personendaten im Sinne von Artikel 5 Buchstabe d DSG dar. Die Bekanntgabe von Personendaten ist eine besonders

---

[87] Botschaft über die Totalrevision des DSG, S. 7079 f.

[88] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.1 Bst. c).

[89] *Ebd.*

[90] Vgl. dazu Nadja BRAUN BINDER, Thomas BURRI, Melinda Florina LOHMANN, Monika SIMMLER, Florent THOUVENIN, Kerstin Noëlle VOKINGER, *Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht*, in: Jusletter vom 28. Juni 2021. Diese Autoren weisen darauf hin, dass die Europäische Kommission am 21. April 2021 einen Vorschlag für eine Verordnung zur Regulierung von KI präsentiert hat.

[91] Bundesrat, *Leitlinien «Künstliche Intelligenz» für den Bund, Orientierungsrahmen für den Umgang mit künstlicher Intelligenz in der Bundesverwaltung* vom 25. November 2020.

[92] Der Einsatz von *«künstlicher Intelligenz»* durch die Verwaltung wurde hingegen in der vom Kanton Zürich in Auftrag gegebenen Studie «Einsatz Künstlicher Intelligenz in der Verwaltung» vom 28. Februar 2021 ausführlich im Hinblick auf die rechtlichen und ethischen Herausforderungen untersucht. Diese Studie befasst sich mit der Frage der Normstufe sowie der Normdichte; Staatskanzlei Kanton Zürich, *Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen – Schlussbericht vom 28. Februar 2021 zum Vorprojekt IP6.4*, 28. Februar 2021, abrufbar unter: https://www.zh.ch/de/news-uebersicht/medienmitteilungen/2021/04/kuenstliche-intelligenz-in-der-verwaltung-braucht-klare-leitlini.html (zuletzt abgerufen am 12.10.2021).

sensible Form der Datenbearbeitung. Sie besteht im Übermitteln oder Zugänglichmachen von Daten (Art. 5 Bst. e DSG) und ist in Artikel 36 DSG geregelt.

Gemäss dieser Bestimmung benötigen Bundesorgane weiterhin eine spezifische gesetzliche Grundlage, welche die Datenbekanntgabe vorsieht (vgl. Art. 19 aDSG und Art. 36 DSG). Mit anderen Worten wäre eine gesetzliche Bestimmung, die Bundesorgane in allgemeiner Weise zur Datenbearbeitung ermächtigt, nicht ausreichend.[93]

Vor der Schaffung einer gesetzlichen Grundlage für die Bekanntgabe von besonders schützenswerten Personendaten oder eines Profilings durch ein Bundesorgan bestimmt der Jurist bzw. die Juristin, inwiefern die Datenbekanntgabe die Persönlichkeit der betroffenen Person verletzt, unter Berücksichtigung insbesondere der Art der übermittelten Daten, des Zwecks der Bekanntgabe, des Empfängerkreises sowie der Form der Übermittlung. Dabei ist während des gesamten Prozesses auf die Einhaltung des Grundsatzes der Verhältnismässigkeit zu achten (vgl. oben Ziff. 2.4).

3.2.4.1 Risiko einer Persönlichkeits- und Grundrechtsverletzung

Die Anforderungen an die gesetzliche Grundlage nach Massgabe der Schwere des Risikos einer Persönlichkeits- oder Grundrechtsverletzung der betroffenen Person sind weitgehend dieselben wie bei anderen Formen der Datenbearbeitung. Artikel 36 Absatz 1 DSG verweist diesbezüglich auf Artikel 34 Absätze 1–3 DSG.

Die Bekanntgabe von besonders schützenswerten Daten ist grundsätzlich in einem Gesetz im formellen Sinn vorzusehen, ebenso wie die Bekanntgabe von Daten, die auf einem Profiling beruhen. Die Ausnahme nach Artikel 34 Absatz 3 DSG ist anwendbar (vgl. oben Ziff. 3.2.1 a. E. und Ziff. 3.2.2 a. E.).

3.2.4.2 Erkennbarkeit und Zweck der Bekanntgabe

Die Bekanntgabe muss für die betroffene Person erkennbar sein. Diese muss in der Lage sein zu erkennen, an wen und zu welchem Zweck ihre Daten bekanntgegeben werden dürfen. Der Zweck der Bekanntgabe muss zudem mit dem Zweck der Datenbeschaffung vereinbar sein (Art. 6 Abs. 3 DSG). Ein Gesetz kann für die Bekanntgabe einen anderen Zweck vorsehen als den ursprünglichen Zweck der Datenbeschaffung. Die Einhaltung des Grundsatzes von Treu und Glauben bleibt vorbehalten (vgl. Ziff. 2.4 oben).

Unterscheidet sich der Zweck der Bekanntgabe von jenem der Beschaffung, kann es wichtig sein, beide Gesetze – das Gesetz über die ursprüngliche Beschaffung und das Gesetz über die spätere Verwendung der Daten zu anderen Zwecken – anzupassen, damit die Bekanntgabe der Daten für die betroffene Person erkennbar bleibt. Beispielsweise sieht Artikel 50*a* des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG)[94] in Absatz 2 Folgendes vor:

---

[93] Vgl. dazu Bericht des BJ über die Totalrevision des DSG, Ziff. 2.1.

[94] SR **831.10** – Bundesgesetz vom 20 Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG) (admin.ch)

«Die zur Bekämpfung der Schwarzarbeit erforderlichen Daten dürfen von den betroffenen Behörden des Bundes, der Kantone und der Gemeinden nach den Artikeln 11 und 12 des Bundesgesetzes vom 17. Juni 2005 gegen die Schwarzarbeit bekannt gegeben werden.»

Die Zusammenarbeit der mit dem Vollzug der Sozialversicherungsgesetzgebung betrauten kantonalen oder eidgenössischen Behörden und privaten Organisationen mit den kantonalen Kontrollorganen nach dem Bundesgesetz über Massnahmen zur Bekämpfung der Schwarzarbeit (Bundesgesetz gegen die Schwarzarbeit, BGSA)[95] sowie die Datenbekanntgabe – insbesondere durch die AHV-Ausgleichskassen – ist im Bundesgesetz gegen die Schwarzarbeit näher geregelt.

3.2.4.3 Form der Bekanntgabe

Es werden vier verschiedene Formen der Bekanntgabe unterschieden: die Meldepflicht (von Amtes wegen oder auf Anfrage), die spontane Bekanntgabe, die Datenbekanntgabe auf Anfrage (nach eigenem Ermessen der angefragten Behörde) und der Online-Zugriff (nach dem Prinzip der Selbstbedienung).[96]

Die gewählte Form der Bekanntgabe muss dem Grundsatz der Verhältnismässigkeit entsprechen. Wenn also die Bekanntgabe auf Anfrage ausreicht, um dem Empfänger zu ermöglichen, seine gesetzlichen Aufgaben zu erfüllen, wird keine weitergehende Art der Bekanntgabe wie z. B. ein Online-Zugriff nach dem Prinzip der Selbstbedienung vorgesehen.

Aus den gesetzlichen Bestimmungen muss hervorgehen, um welche Form der Bekanntgabe es sich handelt. Mit anderen Worten muss der Jurist bzw. die Juristin die betreffenden Formen der Bekanntgabe in den gesetzlichen Bestimmungen weiterhin durch geeignete Formulierungen unterscheiden, wie z. B.:

– *«die Behörde ist verpflichtet, [...] von Amtes wegen zu übermitteln»;*

– *«die Behörde kann [...] spontan melden»;*

– *«die Behörde kann in besonderen Fällen und auf schriftlichen und begründeten Antrag hin [...]».*

– *«die Behörde kann einen Online-Zugriff gewähren [oder ... hat online Zugriff]»*

Das Erfordernis einer ausdrücklichen gesetzlichen Grundlage[97] wurde in Bezug auf das Abrufverfahren fallengelassen (wie oben unter Ziff. 3.1.3 betont). Beim Abrufverfahren handelt es sich um ein automatisiertes Verfahren, bei dem der Datenempfänger die Personendaten erhalten kann, ohne dass das für die Bearbeitung verantwortliche Bundesorgan die Daten bekanntgeben muss oder auch nur bemerkt, dass auf die Daten

---

[95] SR **822.41** – Bundesgesetz vom 17. Juni 2005 über Massnahmen zur Bekämpfung der Schwarzarbeit (Bundesgesetz gegen die Schwarzarbeit, BGSA) (admin.ch)

[96] Vgl. dazu den Gesetzgebungsleitfaden, Rz. 829 ff., sowie die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.2), siehe auch Camille DUBOIS, (2012): Recommandations pour la rédaction de dispositions légales réglant l'échange de données personnelles entre autorités, in: LeGes 23 (2012) 3, S. 389–396.

[97] Vgl. dazu die Aktennotiz des BJ zur Totalrevision des DSG, Ziff. 2.2 (insbesondere Ziff. 2.2.2).

zugegriffen wurde (Selbstbedienungsprinzip). Diese Gesetzesänderung bringt jedoch nur eine geringe materielle Änderung mit sich, da es der Wille des Gesetzgebers ist, dass der durch das früher geltende System gewährte Schutz aufrechterhalten bleibt. Beim Online-Zugriff handelt es sich im Übrigen um eine Form der Bekanntgabe, die weiterhin in einem Gesetz im formellen Sinn enthalten sein muss, soweit sie die Grundrechte der betroffenen Person in schwerwiegender Weise beeinträchtigen kann (Art. 34 Abs. 2 Bst. b DSG), d. h. namentlich und definitionsgemäss immer dann, wenn es um besonders schützenswerte Daten oder ein Profiling geht. In den übrigen Fällen wird diese Form der Bekanntgabe – gleich wie bei den restlichen Formen – zumindest in der Verordnung aufgeführt, damit das Legalitätsprinzip und die Transparenz gewahrt sind. Mit anderen Worten geht es darum, im Gesetz oder in der Verordnung anzugeben, dass es sich um einen Selbstbedienungszugang handelt, während der Verantwortliche durch Formulierungen wie *«erlaubt den Online-Zugriff»* passiv bleibt. Zu unterscheiden ist im Gesetz auch, ob es sich um einen *«Vollzugriff»* auf die Daten oder einen *«Indexzugriff»* handelt.[98]

Ausserdem muss der Grundsatz der Verhältnismässigkeit beachtet werden. Anders ausgedrückt bedeutet dies, dass den Empfängern nur diejenigen Daten mitgeteilt werden dürfen, die sie zur Erfüllung ihrer gesetzlichen Aufgaben benötigen.

3.2.4.4 Normdichte und Mindestinhalt des Gesetzes

Wie bei der Datenbearbeitung hängt die Normdichte der Bestimmungen vom Risiko der Verletzung der Persönlichkeit der betroffenen Person und deren Grundrechte ab. Aus den obigen Ausführungen ergibt sich, dass das Gesetz folgende Punkte regeln muss:

– die Behörde(n), die für die Bekanntgabe der Daten zuständig ist/sind;

– den Zweck der Datenbekanntgabe;

– die Kategorien der betroffenen Daten, einschliesslich Profiling;

– die Art und Weise der Datenbekanntgabe;

– den oder die Empfänger.[99]

3.2.5 Bekanntgabe ins Ausland

Die grenzüberschreitende Datenbekanntgabe hat einige Änderungen erfahren: Grundsätzlich muss der Bundesrat festgestellt haben, dass der Staat, in den die Daten übermittelt werden, in seiner Gesetzgebung und bei der Umsetzung dieser Gesetzgebung ein angemessenes Schutzniveau bietet (Art. 16 Abs. 1 DSG). In diesem Fall können die Daten ohne weitere Hindernisse bekanntgegeben werden. Liegt kein solcher Entscheid des Bundesrates vor, dürfen die Daten nur gegen zusätzliche Garantien ins Ausland bekanntgegeben werden (Art. 16 Abs. 2 und 3 DSG). Artikel 17 DSG listet jene Situationen auf, in denen es zulässig

---

[98] *Ebd.*

[99] Gesetzgebungsleitfaden, Rz. 833.

ist, von Artikel 16 Absätze 2 und 3 DSG abzuweichen und Daten ohne zusätzliche Garantien in einen Staat zu übermitteln, der kein angemessenes Schutzniveau bietet.

Gemäss Artikel 16 Absatz 1 DSG dürfen Personendaten grundsätzlich nur dann ins Ausland bekanntgegeben werden, wenn die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Datenschutz gewährleistet.

Dem Bundesrat obliegt es zu bestimmen, welche Staaten oder internationalen Organe ein solches Schutzniveau gewährleisten. Die Kriterien für die Beurteilung, ob ein ausländischer Staat oder ein internationales Organ ein angemessenes Schutzniveau für Personendaten gewährleistet, sind in Artikel 8 DSV festgelegt. Eine Liste der ausländischen Staaten, die ein angemessenes Schutzniveau gewährleisten, ist im Anhang zu dieser neuen Verordnung enthalten.[100]

Personendaten dürfen an einen Staat, der nicht auf der Liste des Bundesrates steht, bekanntgegeben werden, wenn ein geeignetes Datenschutzniveau durch andere Instrumente im Sinne von Artikel 16 Absatz 2 DSG gewährleistet ist. Dazu gehören insbesondere völkerrechtliche Verträge oder Datenschutzklauseln (Art. 16 Abs. 2 Bst. a, b und d DSG).

Beim Abschluss von Staatsverträgen ist es daher wichtig, darauf zu achten, dass im Ausland ein angemessenes Datenschutzniveau gewährleistet ist. Zentral sind dabei die Einhaltung der datenschutzrechtlichen Grundsätze, die Rechte der betroffenen Personen (wie z. B. das Recht auf Auskunft), Rechtsschutzmöglichkeiten, Anforderungen an eine allfällige weitere Datenbekanntgabe ins Ausland sowie das Bestehen einer unabhängigen Datenschutzaufsicht.

Artikel 9 des Rechtshilfevertrags, den die Schweiz mit Indonesien geschlossen hat[101], und der am 14. September 2021 in Kraft getreten ist, sieht unter anderem Folgendes vor (die Wiedergabe ist unvollständig):

«1. Personenbezogene Daten, die auf der Grundlage dieses Vertrags übermittelt werden, dürfen ausschliesslich für die Zwecke verwendet werden, für die sie übermittelt wurden; ihre Verwendung untersteht den Bedingungen, die vom übermittelnden Staat formuliert werden.

2. Für die Übermittlung und Verwendung personenbezogener Daten, die im Rahmen eines Ersuchens um Rechtshilfe nach diesem Vertrag übermittelt werden, gelten die folgenden Bestimmungen:

> *a. Der zuständigen Behörde des ersuchenden Staates werden nur Daten übermittelt, die einen Bezug zum Ersuchen haben.*
>
> *b. Auf Anfrage informiert die Vertragspartei, welche die Daten erhalten hat, den Staat, der die Daten übermittelt hat, über die Verwendung der Daten und die erzielten Ergebnisse.*
>
> *c. Stellt der übermittelnde Staat fest, dass unrichtige Daten übermittelt wurden oder Daten, die nicht hätten übermittelt werden sollen, so benachrichtigt*

---

[100] Vgl. dazu die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4.2.

[101] SR **0.351.942.7** – Vertrag zwischen der Schweizerischen Eidgenossenschaft und der Republik Indonesien über Rechtshilfe in Strafsachen (admin.ch), in Kraft getreten am 14. September 2021.

dieser Staat den Staat, der die Daten erhalten hat, unverzüglich. Der Staat, der die Daten erhalten hat, korrigiert allfällige Fehler umgehend oder vernichtet die erhaltenen Daten.

d. Die Vertragsparteien führen Aufzeichnungen in leicht abrufbarer Form betreffend die Übermittlung und den Erhalt der Daten.

e. Die Weiterübermittlung personenbezogener Daten ist ausschliesslich in Übereinstimmung mit dem innerstaatlichen Recht und mit vorgängiger Zustimmung des übermittelnden Staates gestattet.

f. Übermittelte Daten, die nicht länger für die nach diesem Vertrag zulässigen Zwecke benötigt werden, sind unverzüglich zu vernichten; gegebenenfalls sind andere nach innerstaatlichem Recht zulässige Massnahmen zu ergreifen, die den Rechten der betroffenen Person gleichermassen dienen.

3. Die Vertragsparteien schützen personenbezogene Daten vor zufälligem Verlust, zufälliger oder unbefugter Vernichtung oder Veränderung, unbefugtem Zugriff, unbefugter Nutzung oder Offenlegung oder anderem Missbrauch.

4. Die Vertragsparteien gewährleisten die legitimen Rechte der von der Datenübermittlung nach diesem Vertrag betroffenen Person auf Information und Auskunft über die sie betreffenden Daten, deren Berichtigung oder Löschung oder gegebenenfalls die Einschränkung ihrer Verarbeitung sowie auf einen wirksamen gerichtlichen Rechtsbehelf im Zusammenhang mit der Übermittlung oder Nutzung der Informationen auf Ersuchen der betroffenen Person.»

Bei Vertragsklauseln (Art. 16 Abs. 2 Bst. a, b und d DSG) ist zu berücksichtigen, dass diese unter Umständen nicht ausreichen, um einen angemessenen Schutz zu gewährleisten.[102]

3.3 Gesetzesdelegation

Artikel 182 BV ermächtigt den Bundesrat unter anderem, Vollzugs- oder Ausführungsbestimmungen zu erlassen, d. h. Sekundärnormen, die eine Gesetzesbestimmung verdeutlichen, deren praktische Rechtsfolgen umschreiben, unbestimmte Rechtsbegriffe konkretisieren oder Organisationsfragen regeln.[103] Im Bereich des Datenschutzes kann der Bundesrat z. B. die Modalitäten des Auskunftsrechts präzisieren.

Artikel 164 Absatz 2 BV gestattet dem Gesetzgeber, die Kompetenz zum Erlass primärer Normen zu delegieren, sofern die Verfassung dies nicht ausschliesst, z. B. bei schwerwiegenden Einschränkungen der Grundrechte. So muss die Dauer der Aufbewahrung besonders schützenswerter Daten dem Grundsatz der Verhältnismässigkeit und dem Grundsatz der Zweckbindung (vgl. oben Ziff. 2.4) Rechnung tragen und in einem Gesetz im

[102] Vgl. dazu die Erläuterungen des EDÖB, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html.

[103] Gesetzgebungsleitfaden, Rz. 721.

formellen Sinn vorgesehen sein. Sie kann jedoch Gegenstand einer Norm betreffend die Delegation von Gesetzgebungskompetenzen sein, und das Gesetz im formellen Sinn kann den Bundesrat beauftragen, die Aufbewahrungsdauer der bearbeiteten Daten zu regeln (vgl. z. B. Art. 38 Abs. 1 Bst. b a. E. des Bundesgesetzes über die im Ausland erbrachten privaten Sicherheitsdienstleistungen[104]).

Die Delegationsnorm hat den Gegenstand, das Ziel (soweit nicht offensichtlich), den Umfang und – soweit möglich – die Leitlinien der delegierten Regelung zu umschreiben.[105]

[104] SR **935.41** – Bundesgesetz vom 27. September 2013 über die im Ausland erbrachten privaten Sicherheitsdienstleistungen (BPS) (admin.ch)

[105] Gesetzgebungsleitfaden, Rz. 725.

IV Checkliste

In der nachfolgenden Checkliste sind die oben dargestellten Fragen zusammengefasst, die bei der Erarbeitung der Rechtsgrundlagen für die Bearbeitung von Personendaten durch Bundesorgane zu beantworten sind:

Fragen	Prüfablauf	Verweise
Werden Personendaten über eine/mehrere natürliche/n Person/en bearbeitet?	Wenn ja: Das DSG ist anwendbar.	vgl. oben Ziff. 2.2 und Ziff. 2.3.1 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4.5
Müssen gewisse Schritte vorgenommen werden, bevor mit der Erarbeitung der Rechtsgrundlagen begonnen werden kann?	Ja. Noch vor der Erarbeitung der Rechtsgrundlagen für die Datenbearbeitung ist zu prüfen, ob eine Datenschutz-Folgenabschätzung (DSFA, Art. 22 DSG) durchgeführt und ein ISDS-Konzept (Informationssicherheit und Datenschutz nach der Hermes-Methode) erstellt werden muss. Dabei ist die Zweckmässigkeit von technischen und organisatorischen Massnahmen zu prüfen (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, vgl. Art. 7 Abs. 2 DSG) und diese sind gegebenenfalls festzulegen. Zu konsultieren sind die spezifischen Hilfsmittel zur Projektführung im Bereich Digitalisierung und die allgemeinen Hilfsmittel für die Gesetzgebung.	vgl. oben Einleitung vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4.3 und 4.5
Ist die Datenbearbeitung für die betroffene Person gestützt auf die geplante Rechtsgrundlage erkennbar?	Die Rechtsgrundlage, die eine Bearbeitung von Personendaten durch Bundesorgane vorsieht, muss angeben, wer welche Daten zu welchem Zweck bearbeitet (wer, was,	vgl. oben Ziff. 2.4 und Ziff. 3.1

	warum), und in einigen Fällen auch, wie die Bearbeitung erfolgt.	
Besteht bei der Datenbearbeitung ein hohes Risiko für die Grundrechte der betroffenen Person?	Ja. Auswirkungen auf die Normstufe (formell-gesetzliche Grundlage im Sinne von Art. 34 Abs. 2 Bst. c DSG) und auf die Normdichte.	vgl. oben Ziff. 1.1, Ziff. 3.1 und 3.2 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4.3
Werden besonders schützenswerte Daten im Sinne des erweiterten Katalogs von Art. 5 Bst. c DSG bearbeitet?	Ja. Auswirkungen auf die gesetzliche Grundlage, die grundsätzlich formell sein muss (Art. 34 Abs. 2 Bst. a DSG). Zur Gewährleistung der Transparenz der Bearbeitung gegenüber der betroffenen Person sind die in Art. 5 Bst. c Ziff. 1–6 DSG genannten Kategorien oder Unterkategorien für besonders schützenswerte Daten in den gesetzlichen Bestimmungen aufzuführen.	vgl. oben Ziff. 2.3.2 und Ziff. 3.2.1 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2.1, Bst. a
Wird ein Profiling im Sinne von Art. 5 Bst. f DSG durchgeführt?	Ja. Auswirkungen auf die gesetzliche Grundlage, die grundsätzlich formell sein muss (Art. 34 Abs. 2 Bst. b DSG). Es müssen mindestens der Zweck des Profilings und die Kategorien besonders schützenswerter Daten, die für das Profiling verwendet werden, sowie die persönlichen Aspekte, die durch das Profiling bewertet werden, in der gesetzlichen Bestimmung aufgeführt sein.	vgl. oben Ziff. 2.3.3 und Ziff. 3.2.2 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2.1, Bst. b
Besteht aufgrund des Zwecks oder der Art und Weise der Bearbeitung die Gefahr eines schwerwiegenden Eingriffs in die Grundrechte?	Ja. Mögliche Auswirkungen auf die Normstufe (formell-gesetzliche Grundlage im Sinne von Art. 34 Abs. 2 Bst. c DSG) und auf die Normdichte.	vgl. oben. Ziff. 3.2.3 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2.1, Bst cc
Liegt eine automatisierte	Ja.	vgl. oben Ziff. 2.3.4 und Ziff. 3.2.3

Einzelentscheidung im Sinne von Art. 21 DSG vor?	Mögliche Auswirkungen auf die Normstufe ([meist formell-]gesetzliche Grundlage im Sinne von Art. 34 Abs. 2 Bst. c DSG). Die Logik, auf der die automatisierte Entscheidung beruht, muss für die betroffene Person in den groben Zügen erkennbar sein.	vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2.1, Bst. cc
Gibt es eine automatisierte Unterstützung bei der Entscheidfindung (Vorbereitung der Entscheidung durch einen automatisierten Prozess oder sogar durch den Einsatz von künstlicher Intelligenz)?	Ja. Mögliche Auswirkungen auf die Normstufe ([meist formell-]gesetzliche Grundlage im Sinne von Art. 34 Abs. 2 Bst. c DSG).	vgl. oben Ziff. 2.3.5 und Ziff. 3.2.3 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2.1, Bst. cc
Ist der Verantwortliche im Sinne von Art. 5 Bst. j DSG identifiziert?	Ja. Er muss als solcher in den gesetzlichen Bestimmungen erscheinen, gleich wie der derzeitige Inhaber der Datensammlung. Bei ihm wird das Auskunftsrecht ausgeübt. Der Verantwortliche muss zudem sicherstellen, dass die Datenschutzbestimmungen eingehalten werden.	vgl. oben Ziff. 2.3.7 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4.1, Ziff. 4.4.2 und Ziff. 4.5
Bearbeitet ein Bundesorgan Daten gemeinsam mit anderen Bundes- oder kantonalen Organen oder mit Privatpersonen im Sinne von Art. 33 DSG?	Ja. Dem Bundesrat obliegt es diesfalls, die Verantwortlichkeiten und Kontrollverfahren zu festzulegen.	vgl. oben Ziff. 2.3.7 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4.1
Wird ein Auftragsbearbeiter mit der Datenbearbeitung beauftragt?	Ja. Mögliche Auswirkungen auf die Gesetzgebung, ansonsten Übertragung auf einen Auftragsbearbeiter vertraglich vorsehen.	vgl. oben Ziff. 2.3.8 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4.1
Ist der Zweck der Bearbeitung explizit angegeben?	Ja. Er muss in der gesetzlichen Grundlage erkennbar aufgeführt sein.	vgl. oben Ziff. 2.4

		vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1
Werden die weiteren Datenschutzgrundsätze, insbesondere die Verhältnismässigkeit der Bearbeitung und die Richtigkeit der Daten, eingehalten?	Ja. Sicherstellen, dass die durch das internationale Recht garantierten Datenschutzgrundsätze und die verfassungsrechtlichen Grenzen für die Einschränkung von Grundrechten eingehalten werden (Art. 36 BV).	vgl. oben Ziff. 1.1 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1
Sind für die Daten Aufbewahrungsfristen vorgesehen?	Ja. Sicherstellen, dass die Grundsätze der Verhältnismässigkeit und der Zweckbindung eingehalten werden.	vgl. oben Ziff. 2.4, i.V.m. Ziff. 3.3
Ist eine Bekanntgabe (einschliesslich ein Zugriff auf die Personendaten) vorgesehen?	Ja. Diese müssen in einer speziellen gesetzlichen Grundlage vorgesehen sein, welche regeln muss: die für die Bekanntgabe der Daten zuständige Behörde; den Zweck der Bekanntgabe oder des Zugriffs auf die Daten; die betroffenen Datenkategorien; die Formen der Bekanntgabe der Daten; die Empfänger.	vgl. oben Ziff. 3.2.4 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1
Kann der Zweck der Bekanntgabe (einschliesslich des Zugriffs auf die Daten) oder die Art und Weise der Bekanntgabe die Grundrechte in schwerwiegender Weise beeinträchtigen?	Ja. Auswirkungen auf die Normstufe (formell-gesetzliche Grundlage im Sinn von Art. 34 Abs. 2 Bst. c DSG, auf den Art. 36 Abs. 1 DSG verweist) und die Normdichte.	vgl. oben Ziff. 3.2.3 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.1 und Ziff. 2.2.2
Werden besonders schützenswerte Daten bekanntgegeben (oder wird ein Zugriff auf solche erteilt)?	Ja. Auswirkungen auf die gesetzliche Grundlage, die grundsätzlich formell sein muss (Art. 34 Abs. 2 Bst. a DSG, auf den Art. 36 Abs. 1 DSG verweist).	vgl. oben Ziff. 2.3.2 und Ziff. 3.2.4.1 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2.1, Bst. a
Wird ein Profiling bekanntgegeben (oder	Ja.	vgl. oben Ziff. 2.3.3 und Ziff. 3.2.4.1

wird ein Zugriff auf ein solches erteilt)?	Auswirkungen auf die gesetzliche Grundlage, die grundsätzlich formell sein muss (Art. 34 Abs. 2 Bst. b DSG, auf den Art. 36 Abs. 1 DSG verweist).	vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 2.2.1, Bst. b
Werden Daten ins Ausland bekanntgegeben (oder wird ein Zugriff dorthin erteilt)?	Ja. Sicherstellen, dass die Gesetzgebung des Empfängerstaates ein angemessenes Schutzniveau im Sinne von Art. 16 Abs. 1 DSG gewährleistet, oder dass die Bedingungen nach Art. 16 Abs. 2 DSG erfüllt sind.	vgl. oben Ziff. 3.2.5 vgl. auch die Aktennotiz des BJ über die Totalrevision des DSG, Ziff. 4 und Ziff. 4.2
Ist eine Gesetzesdelegation vorgesehen?	Ja. Sicherstellen, dass die Grundsätze der Gesetzesdelegation eingehalten werden.	vgl. oben Ziff. 3.3