Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte I

September 2022

Totalrevision des Datenschutzgesetzes (DSG)

Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane

Das totalrevidierte Datenschutzgesetz (nachfolgend: «nDSG») soll den Datenschutz an die technologischen Entwicklungen anpassen und das schweizerische Datenschutzniveau dem europäischen Standard annähern. Das nDSG bleibt wie bisher ein Rahmen- und Querschnittsgesetz. Es legt in den Datenschutzgrundsätzen die Anforderungen an die Datenbearbeitungen fest und sieht institutionelle, organisatorische sowie verfahrensrechtliche Massnahmen vor, welche die Einhaltung dieser Grundsätze sicherstellen sollen. Wie die Datenbearbeitungen im öffentlich-rechtlichen Bereich auf Bundesebene konkret ausgestaltet werden, ist jedoch weiterhin hauptsächlich in den jeweiligen Sacherlassen zu regeln. Das nDSG macht dazu allgemeine Vorgaben. Dabei bleiben viele der zentralen Grundsätze unverändert. Die Totalrevision des DSG bringt aber auch verschiedene Neuerungen mit sich, die inskünftig bei Rechtssetzungsprojekten zu berücksichtigen sind (wie z.B. das «Profiling» oder die «automatisierten Einzelentscheidungen»).

Das vorliegende Dokument vertieft die wichtigsten Änderungen für die Erarbeitung von Rechtsgrundlagen zu den Datenbearbeitungen von Bundesorganen. Es ergänzt die grundlegenden Ausführungen im Gesetzgebungsleitfaden (Kapitel 14; Rz. 813 ff.) und im Gesetzgebungsleitfaden Datenschutz. Es richtet sich vor allem an Personen, die für die Ausarbeitung von Rechtsgrundlagen zuständig sind und sich für ihr Rechtsetzungsprojekt detailliert mit dem totalrevidierten Datenschutzgesetz auseinandersetzen möchten.

Das Dokument enthält nachfolgend eine kurze Übersicht zu den Eckdaten und Materialien der Totalrevision des DSG (► Ziff. 1). Anschliessend zeigt es auf, welche datenschutzrechtlichen und legistischen Grundsätze sich trotz der Totalrevision des DSG nicht ändern (► Ziff. 2.1). Im Hauptteil werden die wichtigsten neuen Vorgaben des totalrevidierten Datenschutzgesetzes an die Normstufe und Normdichte der spezialgesetzlichen Grundlagen zur Bearbeitung von Personendaten durch Bundesorgane vorgestellt (► Ziff. 2.2). In einem separaten Kapitel wird sodann auf den Umgang mit Daten juristischer Personen, die neu vom Geltungsbereich des Datenschutzgesetzes ausgenommen sind, eingegangen (Ziff. 3). Das letzte Kapitel enthält eine Übersicht über verschiedene weitere Neuerungen der Totalrevision des DSG, die auch im Rahmen von Rechtssetzungsprojekten relevant werden können (► Ziff. 4).

Inhaltsverzeichnis

1 Wichtigste Eckdaten zur Totalrevision des DSG

Das Parlament hat die Vorlage des Bundesrates vom 15. September 2017 zur Totalrevision des DSG (E-DSG) in zwei Etappen aufgeteilt:

- In einer **ersten Etappe** wurde ausschliesslich die Schengen-relevante EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen umgesetzt. Dazu wurde – übergangsweise – ein neues Schengen-Datenschutzgesetz (SDSG; SR 235.3) geschaffen, welches am 1. März 2019 in Kraft getreten ist.[1] Dieser Erlass enthält die Rahmenbestimmungen zum Datenschutz bei der Schengener Zusammenarbeit im Strafrechtsbereich, soweit das bisherige DSG die Anforderungen der EU-Richtlinie 2016/680 nicht erfüllt. Neben dem SDSG wurden auch die für die polizeiliche und justizielle Zusammenarbeit relevanten Datenschutzbestimmungen in anderen Bundesgesetzen (insbesondere im Strafgesetzbuch [StGB; SR 311.0] und im Rechtshilfegesetz [SR 351.1]) angepasst bzw. ergänzt. Mit Inkrafttreten der Totalrevision des DSG wird das SDSG wieder aufgehoben, da der Schutzstandard der EU-Richtlinie 2016/680 grundsätzlich durch das nDSG erfüllt wird.

- In der **zweiten Etappe** wurde die «eigentliche» Totalrevision des DSG beraten. Diese Revision setzt unter anderem die Anforderungen der Datenschutz-Konvention 108+ des Europarates[2] um. Ausserdem nähert sie das schweizerische Datenschutzrecht der EU-Datenschutz-Grundverordnung 2016/679 an, damit der Schweiz von der EU weiterhin ein angemessenes Datenschutzniveau attestiert wird (sog. «Angemessenheitsbeschluss»). Das Parlament hat die Totalrevision des DSG am 25. September 2020 verabschiedet. Die Referendumsfrist ist am 14. Januar 2021 unbenutzt abgelaufen.

1.1 Dokumentation zur Totalrevision des DSG

- **Schlussabstimmungstext** zum nDSG vom 25. September 2020: BBl **2020** 7639 / FF **2020** 7397

- **Amtliches Bulletin**

- **Curia Vista:** Die Ratsunterlagen und Fahnen sowie die Chronologie sind einsehbar unter der Geschäftsnummer 17.059.

- **Botschaft und Entwurf des Bundesrates** vom 15. September 2017: BBl **2017** 6941 und **2017** 7193 / FF **2017** 6565 und **2017** 6803

- **Weitere Unterlagen**: Dokumente aus den früheren Projektstadien wie z.B. der Vorentwurf, die Vernehmlassungsergebnisse oder Expertenberichte sind auf der Webseite des BJ «Stärkung des Datenschutzes» aufgeschaltet.

[1] Vgl. dazu auch den Erläuternden Bericht des BJ von Oktober 2018 zum Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (einsehbar unter <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html>).

[2] Die Schweiz hat die Datenschutz-Konvention 108+ des Europarates zwar noch nicht ratifiziert. Allerdings hat der Bundesrat das entsprechende Änderungsprotokoll am 21. November 2019 unterzeichnet. Am 19. Juni 2020 hat das Parlament den Bundesbeschluss zur Genehmigung der Konvention 108+ mit grosser Mehrheit gutgeheissen (Geschäftsnummer 19.068). Die Totalrevision des DSG setzt die Vorgaben der Konvention 108+ auf Bundesebene um. Die Ratifizierung bzw. der Beitritt der Schweiz zur Konvention 108+ ist erst bei Inkrafttreten des neuen Datenschutzrechts möglich.

1.2 Ausblick: Anpassung des Verordnungsrechts und voraussichtliches Inkrafttreten des neuen Datenschutzrechts

- Aufgrund der Totalrevision des DSG sind die Verordnung zum Bundesgesetz über den Datenschutz (**VDSG**; neu: Verordnung über den Datenschutz, DSV) und die Verordnung über die Datenschutzzertifizierungen (**VDSZ**) anzupassen. Ausserdem muss im Anhang zur DSV eine Vielzahl spezialrechtlicher Datenschutzbestimmungen geändert werden. Diese **Änderungen anderer Verordnungen** beschränken sich auf Anpassungen, die sich direkt aus dem nDSG oder den Revisionen der VDSG bzw. der VDSZ ergeben (z.B. die Streichung oder Ablösung des «Persönlichkeitsprofils» ► Ziff. 2.2.1 Bst. b) oder die Anpassung des Begriffs der «Datensammlung»
  ► Ziff. 4.4.2).

- **Wichtigste Inhalte der Revision der VDSG**: Mindestanforderungen an die Datensicherheit; Auftragsbearbeitung; Bekanntgabe von Personendaten ins Ausland (inkl. Liste der Staaten mit einem angemessenen Datenschutz); Modalitäten verschiedener Pflichten der für die Datenbearbeitung Verantwortlichen (namentlich der Informationspflicht, der Datenschutz-Folgenabschätzung und der Meldung von Verletzungen der Datensicherheit); Modalitäten des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung [Datenportabilität]; Ernennung, Aufgaben und Stellung der Datenschutzberaterinnen und -berater; Meldung der Projekte von Bundesorganen zur automatisierten Bearbeitung von Personendaten an den EDÖB; Informationspflichten; Pilotversuche; Organisation und Aufgaben des EDÖB.

- **Inkrafttreten des neuen Datenschutzrechts**: Gemäss Art. 74 Abs. 2 nDSG bestimmt der Bundesrat das Inkrafttreten der Totalrevision des DSG (und des revidierten Verordnungsrechts). Das neue Datenschutzrecht wird am 1. September 2023 in Kraft treten.

2 Anforderungen der Totalrevision des DSG an die Rechtsgrundlagen für die Bearbeitung von Personendaten durch Bundesorgane

2.1 Was sich mit der Totalrevision des DSG *nicht ändert*

- **Datenschutzrechtliche Grundsätze**: Bei der Bearbeitung von Daten natürlicher Personen (= Personendaten; zu den Daten juristischer Personen vgl. ► Ziff. 3) durch Bundesorgane müssen die allgemeinen datenschutzrechtlichen Prinzipen gemäss den Art. 6 – 8 nDSG berücksichtigt werden. Die zentralen Grundsätze der Rechtmässigkeit (Art. 6 Abs. 1 nDSG), der Verhältnismässigkeit (einschliesslich der Datensparsamkeit) und von Treu und Glauben (Art. 6 Abs. 2 und 4 nDSG), der Zweckbindung[3] und der Erkennbarkeit[4] (Art. 6 Abs. 3 nDSG), der Datenrichtigkeit (Art. 6 Abs. 5 nDSG)[5] sowie der Datensicherheit (Art. 8 nDSG) entsprechen im Wesentlichen dem geltenden Recht. Neu werden in Art. 7 nDSG die Grundsätze des Datenschutzes durch Technik und der datenschutzfreundlichen Voreinstellungen («Privacy by Design and by Default») genannt. Der Grundsatz des Datenschutzes durch Technik verlangt, dass die Datenbearbeitung bereits ab Planung in organisatorischer und technischer Hinsicht so ausgestaltet wird, dass die Datenschutzvorschriften eingehalten werden (Art. 7 Abs. 1 nDSG). Der Grundsatz der datenschutzrechtlichen Voreinstellungen erfordert hingegen, dass mittels geeigneter Voreinstellungen sichergestellt wird, dass die Datenbearbeitung – soweit die betroffene Person nichts Anderes bestimmt – auf das für den Verwendungszweck notwendige Mass beschränkt wird (Art. 7 Abs. 3 nDSG). Die beiden Grundsätze ergeben sich zum Teil bereits aus den bestehenden Grundsätzen der Verhältnismässigkeit und der Datensicherheit. Für die Datenbekanntgabe ins Ausland sind ausserdem die Art. 16 und 17 nDSG zu beachten (► Ziff. 4.2).

- **Prinzip der Spezialermächtigung**: Das nDSG enthält – von einzelnen Ausnahmen abgesehen – keine allgemeine Ermächtigung für Datenbearbeitungen durch Bundesorgane, sondern verlangt dafür bereichsspezifische Rechtsgrundlagen. Wenn Bundesorgane Personendaten bearbeiten, müssen die gesetzlichen Grundlagen also in den entsprechenden Sacherlassen geschaffen werden. Das nDSG gibt verschiedene Anforderungen an diese Rechtsgrundlagen vor.

- **Erfordernis der gesetzlichen Grundlage**: Bundesorgane dürfen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Art. 34 Abs. 1 nDSG). Dies gilt für alle Formen und Phasen der *Datenbearbeitung* (Art. 5 Bst. d nDSG), wie etwa das Beschaffen, Verwenden, Aufbewahren oder Löschen der Daten ("Lifecycle" von Personendaten). Die *Datenbekanntgabe* (Art. 5 Bst. e nDSG), bei welcher es sich um eine besonders sen-

---

[3] Der Grundsatz der Zweckbindung wird in Art. 6 Abs. 3 nDSG leicht anders formuliert als bisher (Art. 4 Abs. 3 DSG). Insbesondere wird neu ausdrücklich festgehalten, dass Daten nur so bearbeitet werden dürfen, dass es mit dem anfänglichen Zweck, zu welchem sie beschafft worden sind, **vereinbar** ist. Diese neue Formulierung bringt gemäss der Botschaft des Bundesrates vom 15. September 2017 (► BBl **2017** 6941, 7025) keine wesentlichen Änderungen mit sich: Wie bereits heute ist eine Weiterbearbeitung von Personendaten nicht zulässig, wenn die betroffene Person dies berechtigterweise als unerwartet, unangebracht oder beanstandbar erachten kann. Eine Änderung des anfänglichen Zwecks einer Datenbearbeitung durch Bundesorgane muss also grundsätzlich gesetzlich vorgesehen werden. Der Grundsatz der Zweckbindung ist auch bei Projekten der Bundesverwaltung zur Mehrfachnutzung von Daten («Once-Only-Prinzip») zu beachten.

[4] Auch wenn der Grundsatz der Erkennbarkeit in Art. 6 Abs. 3 nDSG von der Formulierung im geltenden Recht (Art. 4 Abs. 4 DSG) etwas abweicht, soll dies gemäss der Botschaft des Bundesrates vom 15. September 2017 (► BBl **2017** 6941, 7025) – und entgegen anders lautender Lehrmeinungen (namentlich DAVID ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter vom 16. November 2020, Rz. 35) – keine materiellen Änderungen zur Folge haben.

[5] Nach Art. 6 Abs. 5 erster und zweiter Satz nDSG muss sich jeder, der Personendaten bearbeitet, über deren Richtigkeit vergewissern und alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Dies entspricht dem geltenden Art. 5 Abs. 1 DSG. In Art. 6 Abs. 5 *dritter Satz* nDSG hat das Parlament 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. Es ist aber keine inhaltliche Änderung beabsichtigt.

sible Form der Datenbearbeitung handelt, ist in Art. 36 nDSG geregelt. Bundesorgane benötigen für die Datenbekanntgabe eine eigenständige Rechtsgrundlage (d.h.: eine allgemeine Kompetenz zur Datenbearbeitung genügt nicht). Die Anforderungen an die Rechtsgrundlage sind aber weitgehend gleich wie bei anderen Formen der Datenbearbeitung (Verweis in Art. 36 Abs. 1 nDSG auf Art. 34 Abs. 1 – 3 nDSG).

- **Anforderungen an die Normstufe**: Grundsätzlich gilt: Je schwerer der Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 der Bundesverfassung [BV; SR 101])[6] wiegt, desto eher ist für die Datenbearbeitung eine gesetzliche Grundlage in Form eines formellen Gesetzes zu verlangen. Wie bisher gibt der Datenschutzgesetzgeber selber Fällen vor, in denen eine formell-gesetzliche Ermächtigung erforderlich ist (Art. 34 Abs. 2 und Art. 36 Abs. 1 nDSG). Dabei gibt es im Vergleich zum heutigen Recht einige Änderungen zu beachten (► Ziff. 2.2.1).

- **Anforderungen an die Normdichte**: Die rechtliche Grundlage für die Datenbearbeitung muss eine ausreichende Bestimmtheit aufweisen. Weder das geltende DSG noch das nDSG sehen dazu besondere Regelungen vor. Die Anforderungen an die Normdichte richten sich deshalb nach den allgemeinen Grundsätzen des Legalitätsprinzips bzw. nach dem Risikopotenzial einer Datenbearbeitung. Die Rechtsgrundlage ist umso detaillierter auszugestalten, je intensiver in das Recht auf informationelle Selbstbestimmung eingegriffen wird. Massgebend sind insbesondere die folgenden Kriterien: die Art der Daten, die Art und Weise der Datenbearbeitung, der Zweck der Datenbearbeitung, die Anzahl und der Kreis der betroffenen Personen, der allfällige Einbezug weiterer Stellen in die Datenbearbeitung (Bundesorgane, kantonale Organe oder private Stellen) oder der Einsatz neuer Technologien.

  Als Faustregel gilt: Die gesetzliche Grundlage soll Transparenz über die Datenbearbeitung der Bundesorgane schaffen. In den Fällen von Art. 34 Abs. 2 nDSG (i.V.m. Art. 36 Abs. 1 nDSG) muss im formellen Gesetz für die betroffenen Personen im Wesentlichen erkennbar sein, *wer* (► Ziff. 4.1) zu *welchem Zweck welche Daten* bearbeitet, einschliesslich *wem* er sie zu *welchem Zweck* bekannt gibt, und auf *welche Art und Weise* die Bearbeitung geschieht. Zur Art und Weise der Datenbearbeitung gehören beispielsweise Bearbeitungsmethoden wie die Verknüpfung oder das Abgleichen von Daten (einschliesslich Profiling; siehe ► Ziff. 2.2.1 Bst. b)) oder der Einsatz neuer Technologien (z.B. biometrische Verfahren oder künstliche Intelligenz; siehe ► Ziff. 2.2.1 Bst. c)/cc) sowie – bei einem schweren Grundrechtseingriff – die Aufbewahrungsdauer der Daten. Zur Art und Weise der Datenbekanntgabe vgl. auch ► Ziff. 2.2.2.

  In den letzten Jahren stellte sich vermehrt die Frage, ob und – falls ja – wie detailliert die *Architektur eines Systems*, mit welchem Personendaten bearbeitet werden, in den Rechtsgrundlagen abzubilden ist. Dies betrifft insbesondere Verwaltungseinheiten, welche keine «monolithischen» Informationssysteme, sondern neuere Architekturkonzepte wie Microservices einsetzen, bei welchen sich die bearbeiteten Daten nicht mehr separaten «Silos» zuweisen lassen. Für die rechtliche Regelung steht dabei weniger die (technische) Informatikarchitektur, sondern vielmehr die «Datenbearbeitungsarchitektur» (namentlich die Bearbeitungszwecke und -logik sowie die Datenflüsse und -zugriffe) im Vordergrund. Wichtig ist, dass auch bei der Auflösung von klassischen Systemstrukturen im-

[6] Das Grundrecht der informationellen Selbstbestimmung nach Art. 13 Abs. 2 BV garantiert, «dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fragliche Information tatsächlich ist, jede Person gegenüber fremder staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden» (BGE **146** I 11 E. 3.1.1).

mer erkennbar sein muss, welche Daten von wem für welche Aufgaben bzw. Zwecke bearbeitet werden. Die «Aufgabenbezogenheit» der Datenbearbeitung muss also auch bei einem horizontalen Architekturkonzept gewährleistet sein.

Zusammengefasst wird den Anforderungen an die Normdichte in der Regel nicht Genüge getan, wenn eine Bestimmung lediglich pauschal vorsieht, dass die Datenbearbeitung dem verantwortlichen Bundesorgan die Erfüllung seiner gesetzlichen Aufgaben ermöglichen soll.[7] Weniger strenge Anforderungen gelten aber in jenen Fällen, in welchen ein Bundesorgan bereits einen präzis umschriebenen Aufgabenbereich hat und keine heiklen oder komplexen Datenbearbeitungen vornimmt.

- **Ausnahmen vom Erfordernis der gesetzlichen Grundlage**: Da es kaum möglich ist, für sämtliche Konstellationen die nötigen Bestimmungen zu schaffen, sind im nDSG – wie bisher – Ausnahmen vom Erfordernis der gesetzlichen Grundlage für Datenbearbeitungen (Art. 34 Abs. 4 nDSG[8] und Art. 36 Abs. 2 nDSG[9]) vorgesehen. In diesen (abschliessend aufgezählten) Fällen ist eine Datenbearbeitung im Einzelfall *ohne Rechtsgrundlage* zulässig, ungeachtet dessen, ob es sich um eine «gewöhnliche» Datenbearbeitung nach Art. 34 Abs. 1 nDSG oder einen besonders heiklen Vorgang nach Art. 34 Abs. 2 nDSG handelt. Die Ausnahmetatbestände des nDSG entsprechen grossteils dem geltenden Recht. Für die Neuerungen wird auf die bundesrätliche Botschaft vom 15. September 2017 verwiesen (► BBl **2017** 6941, 7081 f.). Auch wenn im Gesetzestext – anders als heute (vgl. Art. 17 Abs. 2 DSG) – der Ausdruck «ausnahmsweise» nicht mehr verwendet wird, so geht damit keine inhaltliche Änderung einher. Es gilt nach wie vor, dass sich eine Datenbearbeitung, die mit einer gewissen Regelmässigkeit oder Dauerhaftigkeit erfolgt, auf eine gesetzliche Grundlage stützen können muss.

- **«Spezialfälle»**: Wie bisher sieht das nDSG verschiedene Spezialbestimmungen vor, welche die Anforderungen an die gesetzliche Grundlage lockern (bei Pilotversuchen nach Art. 35 nDSG sowie bei der Datenbearbeitung für nicht personenbezogene Zwecke wie Forschung, Planung oder Statistik nach Art. 39 nDSG) oder Bundesorgane direkt zur Datenbekanntgabe ermächtigen (erleichterte Datenbekanntgabe bei Stammdaten nach Art. 36 Abs. 4 nDSG). Eine weitere Sonderregelung betrifft die Bekanntgabe von Personendaten im Rahmen der behördlichen Information der Öffentlichkeit (Art. 36 Abs. 3 und 5 nDSG). Diese Spezialbestimmungen des nDSG entsprechen grossteils dem geltenden Recht. Für die Neuerungen wird auf die bundesrätliche Botschaft vom 15. September 2017 verwiesen (► BBl **2017** 6941, 7081 ff.).

---

[7] Zu den Anforderungen des Bundesgerichts an die Normdichte vgl. zwei Beispiele, welche polizeiliche Datenbearbeitungen in den Kantonen Thurgau (BGE **146** I 11) und Zürich (BGE **136** I 87) betreffen.

[8] Gemäss Art. 34 Abs. 4 nDSG dürfen Bundesorgane Personendaten ohne Rechtsgrundlage bearbeiten, wenn: (a) der Bundesrat die Bearbeitung bewilligt, weil er die Rechte der betroffenen Person für nicht gefährdet hält; (b) die betroffene Person im Einzelfall nach Art. 6 Abs. 6 und 7 nDSG in die Bearbeitung eingewilligt hat oder ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat; oder *neu* (c) die Bearbeitung notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen. *Anders* als im geltenden Art. 17 Abs. 2 Bst. a DSG ist keine Ausnahme vom Erfordernis der gesetzlichen Grundlage mehr vorgesehen, wenn eine Datenbearbeitung für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist. In diesem Fall gelten immerhin weniger strenge Anforderungen an die Normstufe (siehe Art. 34 Abs. 3 nDSG; ▸ Ziff. 2.2.1 Bst. a)/cc und b)/ee).

[9] Gemäss Art. 36 Abs. 2 nDSG dürfen Bundesorgane Personendaten im Einzelfall ohne Rechtsgrundlage bekanntgeben, wenn (a) die Bekanntgabe der Daten für die Empfängerin oder den Empfänger oder *neu* für den Verantwortlichen zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich ist; (b) die betroffene Person nach Art. 6 Abs. 6 und 7 nDSG in die Bekanntgabe eingewilligt hat; (c) die Bekanntgabe der Daten notwendig ist, um das Leben oder die Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen (*neu*); (d) die betroffene Person ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt hat; oder (e) die Empfängerin oder der Empfänger glaubhaft macht, dass die betroffene Person die Einwilligung verweigert oder Widerspruch gegen die Bekanntgabe einlegt um ihr oder ihm die Durchsetzung von Rechtsansprüche oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren.

- **Verhältnis DSG – leges speciales**: Angesichts der grundsätzlichen Gleichrangigkeit von Normen derselben Erlassstufe, ist es nicht ausgeschlossen, dass eine andere formell-gesetzliche Bestimmung dem nDSG als lex specialis vorgeht.[10] Der Gesetzgeber kann somit in den bereichsspezifischen Rechtsgrundlagen von gewissen Prinzipien des nDSG abweichen, wenn dies die in einem anderen Gesetz enthaltenen Wertungen erfordern. Allerdings sind die verfassungs- und völkerrechtlichen Schranken zu beachten:

  – Das nDSG setzt verschiedene Schutzgehalte des *Grundrechts auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV bzw. Art. 8 EMRK* um (z.B. den Auskunfts-, Berichtigungs- und Löschungsanspruch). Für die Einschränkung solcher durch die Datenschutzgesetzgebung konkretisierter Garantien gelten die Vorgaben von Art. 36 BV.

    Das **Grundrecht auf informationelle Selbstbestimmung** garantiert gemäss der Rechtsprechung des Bundesgerichts, «dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, jede Person gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden».[11] Lehre und Rechtsprechung leiten daraus verschiedene spezifische Ansprüche ab. Dazu gehören mindestens das Recht auf Einsicht in die eigenen Daten, das Recht auf Berichtigung falscher Personendaten sowie das Recht auf Löschung von widerrechtlich bearbeiteten Personendaten.[12]

  – Zu berücksichtigen ist des Weiteren, dass im nDSG für die Schweiz verbindliche völker- bzw. europarechtliche Bestimmungen übernommen werden: So setzen die Vorgaben der *Datenschutz-Konvention 108+ des Europarates* und der Schengen-relevanten *EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen* den spezialgesetzlichen Abweichungen vom nDSG Grenzen.

  – Ausserhalb des Anwendungsbereichs der EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen gilt die Schweiz der EU gegenüber als Drittstaat. Im Jahr 2000 hat die Europäische Kommission der Schweiz ein angemessenes Datenschutzniveau attestiert. Dieser *Angemessenheitsbeschluss* ermöglicht, dass Personendaten aus den EU-Mitgliedstaaten ohne weitere Hindernisse in die Schweiz bekanntgegeben werden können. Der Angemessenheitsbeschluss der Schweiz wird derzeit durch die Europäische Kommission überprüft. Auch inskünftig sind periodische Überprüfungen des schweizerischen Datenschutzrechts vorgesehen. Nur wenn die Schweiz ein der EU-Datenschutz-Grundverordnung 2016/679 *angemessenes* Datenschutzniveau gewährleistet, kann sie den Angemessenheitsbeschluss beibehalten. Dabei ist nicht nur der allgemeine, sondern auch der sektorielle Datenschutz Gegenstand der Evaluation durch die Europäische Kommission. Ein besonderes Augenmerk legt die EU auf Datenzugriffe der Behörden in den Bereichen der nationalen Sicherheit und des Strafrechts.[13] Vor diesem Hintergrund ist auch in den bereichsspezifischen Erlassen auf ein angemessenes Datenschutzniveau zu achten. Eine (teilweise oder gar umfassende) Aufhebung des Angemessenheitsbeschlusses würde den grenzüberschreitenden Datenverkehr

[10] Vgl. z.B. BGE **142** II 268 E. 6.3 sowie das Urteil des Bundesverwaltungsgerichts B-6547/2014 vom 25. April 2017, E. 5.2.

[11] Statt vieler BGE **146** I 11 E. 3.1.1. Vgl. dazu auch 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, 2021, S. 44-63 (insbesondere S. 47 f.).

[12] Vgl. dazu ALEXANDRE FLÜCKIGER, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, in: AJP 2013 S. 837 ff. (insbesondere S. 852) m.w.H. FLÜCKIGER leitet aus dem Grundrecht auf informationelle Selbstbestimmung noch weitere verfassungsrechtliche Ansprüche ab, namentlich «le droit de spécifier le but de l'utilisation des données récoltées, le droit de s'opposer à leur traitement, le droit à la transparence de la collecte (caractère reconnaissable de celle-ci et devoir d'information), le droit de ne pas exporter ses données vers des pays moins protecteurs, le droit à la sécurité des données (protection en cas d'atteinte à l'intégrité des données suite à un traitement illicite ou contraire à sa volonté ainsi qu'en cas de brèche de sécurité [vol ou perte des données], comprenant en plus le droit d'être avisé en pareil cas), le droit à l'anonymat, en particulier celui d'aller et venir anonymement, le droit à l'oubli, le droit d'exiger un cadre et des moyens techniques permettant à chacun d'exercer effectivement des choix éclairés: architecture informatique conçue pour améliorer le pouvoir de contrôle (privacy enhancing technologies), protection intégrée de la vie privée (privacy by design), dépôts de données personnelles (personal data store), de même que le droit de disposer librement de ses données à sa mort (droit successoral numérique)».

[13] Siehe dazu die Referenzgrundlage für Angemessenheit der ehemaligen Artikel-29-Datenschutzgruppe vom 28. November 2017 bzw. 6. Februar 2018

beträchtlich erschweren. Vgl. zum Ganzen Art. 45 ff. der EU-Datenschutz-Grundverordnung 2016/679.

Fazit: Spezialgesetzliche Abweichungen vom nDSG (als datenschutzrechtlicher «Mindeststandard») dürfen nur aus triftigen Gründen erfolgen und müssen gut begründet werden können.

2.2 Was sich mit der Totalrevision des DSG *ändert*

2.2.1 Vorgaben zur Normstufe (Erfordernis eines formellen Gesetzes)

In Art. 34 Abs. 2 und 3 nDSG werden verschiedene Vorgaben zur Normstufe für besonders risikobehaftete Datenbearbeitungen durch Bundesorgane festgelegt. Diese Vorgaben finden auch auf die Datenbekanntgabe Anwendung (Art. 36 Abs. 1 nDSG).

a) Bearbeitung von besonders schützenswerten Personendaten (Art. 34 Abs. 2 Bst. a nDSG)

aa) Wie bisher: Grundsatz der Grundlage in Gesetz im formellen Sinn

Gemäss Art. 34 Abs. 2 Bst. a nDSG ist für die Bearbeitung von besonders schützenswerten Personendaten grundsätzlich eine Ermächtigung in einem Gesetz im formellen Sinn erforderlich. Um die Transparenz gegenüber den betroffenen Personen zu wahren, sind in der gesetzlichen Bestimmung die *Kategorien* der bearbeiteten besonders schützenswerten Daten *nach Art. 5 Bst. c Ziff. 1–6 nDSG* zu nennen. Aufgrund des Verhältnismässigkeitsprinzips darf sich die Ermächtigung nur auf diejenigen Kategorien erstrecken, die für das Bundesorgan notwendig sind, damit es seine Aufgaben erfüllen kann. Falls möglich und nötig sind Unterkategorien zu bilden (Beispiel: es dürfen nicht alle, sondern nur bestimmte Gesundheitsdaten – wie Daten zu Krebserkrankungen – bearbeitet werden). Diese Vorgaben entsprechen dem geltenden Recht. Es sind jedoch zwei Neuerungen zu beachten:

- Der Katalog der besonders schützenswerten Personendaten in Art. 5 Bst. c nDSG wird mit der Totalrevision des DSG erweitert (► nachfolgend Bst. bb).

- Neu ist es unter bestimmten Voraussetzungen zulässig, die Bearbeitung von besonders schützenswerten Personendaten primär auf Verordnungsstufe zu regeln (► nachfolgend Bst. cc).

bb) Neu: Erweiterung des Katalogs der besonders schützenswerten Personendaten

Der Begriff der besonders schützenswerten Personendaten wird in Art. 5 Bst. c nDSG 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 folgende Kategorien zu den besonders schützenswerten Personendaten:

- **Daten über die Zugehörigkeit zu einer Ethnie** (Art. 5 Bst. c Ziff. 2 nDSG): 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»[14].

  Beispiele: Kosovo-Albaner, Araber, Palästinenser oder Fahrende.[15]

[14] BGE **143** IV 193 E. 2.3.

[15] FABIENNE ZANNOL, Die Anwendung der Strafnorm gegen Rassendiskriminierung (Studie im Auftrag der EKR), Bern 2007.

- **genetische Daten** (Art. 5 Bst. c Ziff. 3 nDSG): Gemäss der Botschaft des Bundesrates vom 15. September 2017 sind genetische Daten «Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden» (► BBl **2017** 6941, 7020).[16] Diese Definition entspricht Art. 3 Bst. l des Bundesgesetzes über genetische Untersuchungen beim Menschen.

  Beispiel: DNA-Profil.

- **biometrische Daten, die eine natürliche Person eindeutig identifizieren** (Art. 5 Bst. c Ziff. 4 nDSG): Unter biometrischen Daten im Sinne von Art. 5 Bst. c Ziff. 4 nDSG 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 (► BBl **2017** 6941, 7020). Anders als bei genetischen Daten ist bei biometrischen Daten der technische Prozess, welcher 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: Gesichtsbildern, die mit einer Gesichtserkennungssoftware bearbeitet werden, Fingerabdruck-, Iris- und Retinascans.

Die Begriffe der «genetischen Daten» und der «biometrischen Daten, die eine natürliche Person eindeutig identifizieren» sind sehr weit. Es ist deshalb auf formell-gesetzlicher Stufe zu präzisieren, *welche* genetischen oder biometrischen Daten bearbeitet werden. Delegationsnormen sollten nur zurückhaltend eingesetzt werden.

Vgl. als Beispiel für eine Delegationsnorm Art. 2*b* Abs. 4 des Entwurfs vom 4. Dezember 2020 zum DNA-Profil-Gesetz[17] betreffend Phänotypisierung: «Der Bundesrat kann in Abhängigkeit vom technischem Fortschritt und wenn die praktische Zuverlässigkeit gegeben ist weitere äusserlich sichtbare Merkmale festlegen».

Mit der Erweiterung des Katalogs der besonders schützenswerten Personendaten werden die Anforderungen von Art. 6 Abs. 1 der Datenschutz-Konvention 108+ des Europarates und Art. 3 Ziff. 12 und 13 sowie Art. 10 der Schengen-relevanten EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen umgesetzt. Ausserdem wird das schweizerische Datenschutzrecht damit der EU-Datenschutz-Grundverordnung 2016/679 (Art. 4 Ziff. 13 und 14 sowie Art. 9) angenähert. Diese europäischen Vorschriften sind deshalb im Rahmen der Auslegung von Art. 5 Bst. c nDSG mitzuberücksichtigen.

cc) Neu: Senkung der Anforderungen an die Normstufe unter bestimmten Voraussetzungen

Art. 34 Abs. 3 nDSG sieht neu[18] vor, dass für die Bearbeitung von besonders schützenswerten Personendaten eine Grundlage in einem Gesetz im materiellen Sinn ausreichend ist, wenn zwei Voraussetzungen (kumulativ) erfüllt sind:

---

[16] Die vom Nationalrat beantragte Einschränkung der Begriffsdefinition in Art. 5 Bst. c Ziff. 3 nDSG, wonach genetische Daten nur dann besonders schützenswert sein sollen, wenn sie «eine natürliche Person eindeutig identifizieren», wurde vom Ständerat (= bundesrätliche Fassung) abgelehnt. Der Ständerat hat sich in der Differenzbereinigung durchgesetzt. Um allfällige Missverständnisse zu beheben, hat die Departementsvorsteherin des EJPD im Nationalrat klargestellt, dass nicht alle genetische Daten von Art. 5 Bst. c Ziff. 3 nDSG erfasst werden, sondern nur genetische *Personen*daten (= Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen; Art. 5 Bst. a nDSG). 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 (z.B. bei anonymisierten Daten), fallen die genetischen Daten nicht in den Anwendungsbereich des nDSG (vgl. Amtl. Bull. **2019** N 1787).

[17] BBl **2021** 45

[18] Nach dem geltenden Art. 17 Abs. 2 Bst. a DSG dürfen besonders schützenswerte Personendaten *ohne Rechtsgrundlage* bearbeitet werden, wenn es ausnahmsweise für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist. Allerdings darf sich eine Datenbearbeitung nur im Einzelfall auf diese Ausnahmebestimmung stützen (siehe CLAUDIA MUND, Stämpflis Handkommentar zum Datenschutzgesetz, Bern 2015 [«SHK DSG»], Art. 17 DSG N 16).

- **Die Bearbeitung ist für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe unentbehrlich**: Vorausgesetzt ist, dass die Aufgabe, für welche die Personendaten bearbeitet werden, ausdrücklich in einem Gesetz im formellen Sinn vorgesehen ist und in ihrem Umfang klar erkennbar ist. Nur so kann die notwendige Transparenz für die betroffene Person geschaffen werden. Eine implizit abzulesende Aufgabe ist nicht ausreichend. Ausserdem muss die Datenbearbeitung zur Aufgabenerfüllung unentbehrlich sein. Dies ist nur dann der Fall, wenn die Aufgabenerfüllung ohne die Bearbeitung der betroffenen Daten geradezu verunmöglicht würde. Eine bloss verbesserte oder effizientere Aufgabenerfüllung genügt dagegen nicht.[19]

- **Der Bearbeitungszweck birgt für die Grundrechte der betroffenen Person keine besonderen Risiken**: Zu denken ist hier insbesondere an den Schutz der Privatsphäre nach Art. 13 BV. Entgegen des (zu) engen Wortlauts schützt Art. 13 Abs. 2 BV nach der herrschenden Lehre und der Rechtsprechung des Bundesgerichts nicht nur vor dem Missbrauch der persönlichen Daten, sondern gibt einen umfassenden Anspruch auf informationelle Selbstbestimmung. Dies bedeutet, dass jede Person grundsätzlich selber darüber entscheiden können soll, ob und zu welchem Zweck Informationen über sie bearbeitet werden (► vgl. Ziff. 2.1).[20] Eine verfassungsrechtliche Grundgarantie zum Schutz der Persönlichkeit bietet sodann das Recht auf persönliche Freiheit in Art. 10 Abs. 2 BV (insbesondere der Schutz der elementaren Erscheinungen der elementaren Persönlichkeitsentfaltung). Aber auch weitere Grundrechte wie z.B. die Wirtschaftsfreiheit (Art. 27 BV) sind zu berücksichtigen. Zu den Fallkonstellationen, in welchen der Bearbeitungszweck zu einem schwerwiegenden Eingriff in die Grundrecht der betroffenen Person führt, ► vgl. Ziff. 2.2.1 Bst. c)/Bst. bb. Zu beachten ist ausserdem, dass nicht nur der Bearbeitungszweck, sondern auch die Art und Weise der Datenbearbeitung Risiken für die Grundrechte der betroffenen Person mit sich bringen kann; vgl. dazu Art. 34 Abs. 2 Bst. c nDSG sowie ► Ziff. 2.2.1 Bst. c)/cc.

b) Profiling (Art. 34 Abs. 2 Bst. b nDSG)

aa) Ausgangslage: Vom Persönlichkeitsprofil zum Profiling

Der technische Fortschritt hat zu neuen Methoden der Datenbearbeitung geführt. Dazu gehört die Möglichkeit, grosse Datenmengen zu speichern, zu verknüpfen und zu analysieren (Stichwort «Big Data»). So können aus einer Unmenge an Daten, die für sich alleine genommen möglicherweise wenig aufschlussreich sind, anhand statistisch-mathematischer Verfahren neue Informationen über Personen generiert werden. Dieser Entwicklung wird in der Totalrevision des DSG unter anderem dadurch Rechnung getragen, dass der bisherige Begriff des «Persönlichkeitsprofils» (Art. 3 Bst. d DSG) durch das «Profiling» (Art. 5 Bst. f und g nDSG) abgelöst wird. Obwohl die beiden Begriffe auf den ersten Blick sehr ähnlich erscheinen, sind sie nicht deckungsgleich. Während ein **Persönlichkeitsprofil** als *Ergebnis eines Bearbeitungsprozesses* entsteht (= Zusammenstellung von Daten, aus welcher sich ein Bild über wesentliche [Teil-]Aspekte einer natürlichen Person ergibt), umschreibt das **Profiling** eine *Art bzw. Methode der Datenbearbeitung* (= automatisierte Bewertung bestimmter Aspekte einer natürlichen Person).

[19] Vgl. dazu auch das Urteil des Bundesgerichts 2C_1040/2018 und 2C_1051/2018 vom 18. März 2021 (zur Publikation vorgesehen), wonach Unentbehrlichkeit bedeutet, dass sich eine gesetzliche Aufgabe nur mit den betreffenden Daten erfüllen lässt und diese insofern die einzige Möglichkeit darstellen, die Aufgabe zu erfüllen (E. 5.4).

[20] BGE **140** I 2 E. 9.1.

Wie heute an die Bearbeitung von Persönlichkeitsprofilen werden im nDSG inskünftig auch an das Profiling (bzw. im privatrechtlichen Bereich: an das Profiling mit hohem Risiko) qualifizierte Rechtsfolgen geknüpft. Dazu gehört, dass für das Profiling durch Bundesorgane grundsätzliche eine formell-gesetzliche Ermächtigung verlangt wird (► siehe nachfolgend Bst. dd). Durch ein Profiling können besondere Risiken für die Grundrechte der betroffenen Personen entstehen: Profiling-Verfahren sind oft wenig transparent, dies insbesondere, wenn das Profiling auf der Anwendung von Algrorithmen basiert. Die betroffenen Personen wissen nicht, nach welcher Logik ihre Daten bearbeitet werden und welche Folgen eine solche Bearbeitung für sie haben kann. Durch ein Profiling ist es möglich, Menschen zu analysieren, in Kategorien einzuordnen und zu bewerten. Dadurch können sich nicht nur bestehende Klischeevorstellungen verfestigen. Mitunter kann es durch Profiling auch zu falschen Vorhersagen und zu Diskriminierung kommen.

bb) Begriff des «Profilings» (Art. 5 Bst. f nDSG)

Das Parlament ist bei der Legaldefinition des Profilings vom bundesrätlichen Entwurfs abgewichen und hat sich am **Wortlaut der Datenschutzvorschriften der EU** orientiert (Art. 3 Ziff. 4 der EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen; Art. 4 Ziff. 4 der EU-Datenschutz-Grundverordnung 2016/679).[21] Der Bundesrat hatte ursprünglich eine eigene Umschreibung für das Profiling gewählt, auch wenn er inhaltlich keine Differenz zum europäischen Datenschutzrecht schaffen wollte (► BBl **2017** 6941, 7021 f.). Diese Entstehungsgeschichte zeigt, dass die europäischen Vorschriften bei der Auslegung des Profiling-Begriffs eine wichtige Rolle spielen.

Als **Profiling** gilt gemäss Art. 5 Bst. f nDSG «jede Art 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, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen». Im Einzelnen:

- Die **Datenbearbeitung**, insbesondere der Bewertungsprozess[22], erfolgt **automatisiert**. Anders als beim Begriff der automatisierten Einzelentscheidung (► vgl. dazu Ziff. 2.2.1 Bst. c)/cc) muss beim Profiling die Datenbearbeitung *nicht vollständig automatisiert* sein. Das Eingreifen eines Menschen schliesst eine Aktivität nicht von der Profiling-Definition aus, solange die Datenbearbeitung *im Wesentlichen automatisiert* abläuft.[23]

- Das **Ziel der Datenbearbeitung** besteht darin, bestimmte persönliche Aspekte einer natürlichen Person **zu bewerten**. Dabei kann die Bewertung sowohl in der *Analyse* von Persönlichkeitsmerkmalen liegen, aber auch dazu verwendet werden, um eine *Prognose* über zukünftige Verhaltensweisen bzw. Eigenschaften einer Person zu erstellen. Zur Veranschauli-

[21] Vgl. dazu das Votum des Berichterstatters der SPK-N MATTHIAS JAUSLIN im Nationalrat am 24. September 2019: AB **2019** N 1790.

[22] Vgl. dazu das Beispiel vom SIMON ROTH, Das Profiling im neuen Datenschutzrecht, in: SWZ 2021 34–39, S. 35: Oberserviert ein Privatdetektiv eine Person, um sozialversicherungsrelevante Behauptungen zu ihrem Gesundheitszustand zu verifizieren, und setzt dabei eine Foto- oder Videokamera ein, liegt noch kein Profiling vor. Denn die Bewertung, ob die observierte Person die behaupteten gesundheitlichen Einschränkungen aufweist oder nicht, erfolgt durch manuelle Analyse des aufgenommenen Bild- und Filmmaterials und nicht automatisiert. Die Foto- oder Videokamera trifft keine automatisierte Aussage über den Gesundheitszustand der betroffenen Person.

[23] Siehe dazu die «Leitlinien zu automatisierten Entscheidungen im Einzelfall einschliesslich Profiling für die Zwecke der Verordnung 2016/679» der ehemaligen Artikel-29-Datenschutzgruppe vom 6. Februar 2018, S. 7. Diese Leitlinien sind inzwischen vom Europäischen Datenschutzausschuss (EDSA) übernommen worden. Vgl. ausserdem DAVID VASELLA, Profiling nach der DSGVO und dem E-DSG bei Banken, in: SUSAN EMMENEGGER (Hrsg.), Banken und Datenschutz, Basel 2019, S. 197. In der Botschaft des Bundesrates vom 15. September 2017 heisst es, dass ein Profiling nur vorliege, wenn der Bewertungsprozess vollständig automatisiert sei. Diese Aussage ist angesichts der Anpassung der Legaldefinition durch das Parlament (Angleichung an das EU-Datenschutzrecht) und der Auslegung des Profiling-Begriffs in den europäischen Rechtsakten zu absolut.

chung nennt die Legaldefinition in Art. 5 Bst. f nDSG einige Beispiele (Analyse oder Vorhersage bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Aufenthaltsort und Ortswechsel).

Der Begriff der «Bewertung» zeigt, dass es beim Profiling um eine Art Einschätzung oder Beurteilung einer Person geht. So können beim Profiling etwa bestimmte Merkmale einer Person analysiert werden, um zu ermitteln, ob diese für gewisse Tätigkeiten geeignet ist oder nicht. Das Profiling basiert dabei auf der Grundannahme, dass sich eine Person in der Zukunft gleich oder ähnlich verhält wie in der Vergangenheit oder dass sich eine Person mit einem bestimmten Profil gleich verhält wie andere Personen mit einem gleichen oder ähnlichen Profil. Mit dem Profiling werden also Wahrscheinlichkeitsaussagen getroffen, nicht aber unbedingt die Realität abgebildet.[24] Kein Profiling ist daher die objektive Feststellung eines Sachverhalts. Auch eine einfache Einteilung von Personen anhand bekannter Merkmale wie Alter, Geschlecht und Grösse führt nicht notwendigerweise zu einem Profiling. Hierbei kommt es auf den Grund der Einteilung an. So kann ein Datenbearbeiter zum Beispiel seine Kunden zu statistischen Zwecken nach Alter oder Geschlecht einteilen, um einen zusammenfassenden Überblick zu erhalten, ohne Vorhersagen zu treffen oder Schlussfolgerungen über einzelne Personen zu ziehen. In diesem Fall besteht der Grund der Einteilung nicht in der Bewertung individueller Merkmale, weshalb es sich nicht um ein Profiling handelt.[25] Ebenso stellt die blosse Zusammenstellung von Eckdaten – wie z.B. Name, Geburtsdatum und Geschlecht als Identifikationsdaten – noch kein Profiling dar, da keine Bewertung von persönlichen Merkmalen vorgenommen wird.[26]

Beispiele[27] (ohne Beurteilung, ob es sich um ein «gewöhnliches» Profiling oder ein «Profiling mit hohem Risiko» handelt; ► vgl. dazu nachfolgend Bst. cc):

- *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.
- *Bewertung der persönlichen Vorlieben*: Von einem Profiling ist sodann auszugehen, wenn die betroffenen Personen aufgrund von unterschiedlichen Methoden zur Nutzerverfolgung im Internet, wie z.B. Cookies, die anzeigen, welche Webseiten besucht wurden, Likes auf Social-Media-Plattformen oder der auf einem Smartphone verwendeten Apps in verschiedene Kategorien eingeteilt werden, die ihrem Verhaltensmuster entsprechen (wie etwa «treibt viel Sport», «kocht vegetarisch», «legt den Fokus auf das Arbeiten» oder «ist introvertiert/extrovertiert»). Solche Profile werden dann unter anderem für personalisierte Werbung genutzt.

---

[24] OLIVIER HEUBERGER, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, Diss. Luzern, 2020, Rz. 59.

[25] Siehe die «Leitlinien zu automatisierten Entscheidungen im Einzelfall einschliesslich Profiling für die Zwecke der Verordnung 2016/679» der ehemaligen Artikel-29-Datenschutzgruppe vom 6. Februar 2018, S. 7; David ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter vom 16. November 2020, Rz. 24; David VASELLA, a.a.O., S. 193 f.

[26] OLIVIER HEUBERGER, a.a.O., Rz. 147.

[27] Die ersten drei Beispiele stammen aus OLIVIER HEUBERGER, a.a.O., Rz. 157 ff.

– *Bewertung des Verhaltens*: Im öffentlichen Sektor könnte ein Profiling vorliegen, wenn Personendaten durch eine Polizeibehörde automatisiert ausgewertet werden, um den Gefährlichkeitsgrad einer Person zu beurteilen.

– *Bewertung des Verhaltens*: Die FINMA erhält im Rahmen ihrer Finanzmarktaufsicht eine sehr grosse Menge von Daten, aus welchen sie durch Profiling ein allfälliges aufsichtsrechtliches Fehlverhalten eruiert. Insbesondere im Rahmen der sog. Marktaufsicht (z.B. zur Abklärung eines möglichen Insiderhandels oder einer Marktmanipulation) wertet die FINMA Handels- und Transaktionsdaten personenbezogen automatisiert aus (► vgl. dazu die Botschaft des Bundesrates vom 15. September 2017, BBl **2017** 6941, 7151 zum neu geschaffenen Art. 23 Abs. 3 FINMAG).

cc) Begriff des «Profilings mit hohem Risiko» (Art. 5 Bst. g nDSG)

Der Begriff des Profilings mit hohem Risiko wurde in der **parlamentarischen Beratung** eingeführt. Nach der Ansicht des Parlaments war der Entwurf des Bundesrates zum Profiling insbesondere für die privaten Datenbearbeiter zu strikt. Denn der Bundesrat hatte das Profiling *per se* als risikobehaftet eingestuft und nicht berücksichtigt, dass das Profiling auch harmlose Vorgänge erfassen kann. Das Parlament hat sich deshalb 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 (► siehe dazu nachfolgend Bst. dd).

Auf die **Legaldefinition des Profilings mit hohem Risiko** konnten sich National- und Ständerat erst auf Antrag der Einigungskonferenz hin verständigen.[28] Gemäss Art. 5 Bst. g nDSG ist darunter ein Profiling zu verstehen, «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». Zur Erläuterung:

- Die Umschreibung des hohen Risikos in Art. 5 Bst. g nDSG entspricht dem **heutigen Begriff des «Persönlichkeitsprofils»** nach Art. 3 Bst. d DSG. Einzig der bisher verwendete Ausdruck «Zusammenstellung von Daten» wird durch «Verknüpfung von Daten» ersetzt, um den neuen technischen Möglichkeiten sprachlich besser Rechnung zu tragen. Damit bleibt auch die Rechtsprechung zum Persönlichkeitsprofil (insbesondere das Leiturteil des Bundesverwaltungsgerichts in Sachen Moneyhouse[29]) massgebend.

- Vereinfacht gesagt, liegt ein Profiling mit hohem Risiko i.S.v. Art. 5 Bst. g nDSG dann vor, wenn das Profiling ein Persönlichkeitsprofil nach geltendem DSG 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 kann, 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. Dadurch wird sie in ihrer Freiheit eingeschränkt, sich so darzustellen, wie sie es für richtig hält. Werden Personendaten über einen längeren Zeitraum zusammengetragen («Längsprofil»), führen sie eher zu einem Persönlichkeitsprofil bzw. einem Profiling mit hohem Risiko, also solche, die eine blosse Momentaufnahme enthalten.[30]

---

[28] Sitzungen des Nationalrates (AB **2020** N 1816 ff.) und des Ständerates am 24. September 2020 (AB **2020** S 1024 ff.).

[29] Urteil des Bundesverwaltungsgerichts A-4232/2015 i.S. EDÖB gegen Moneyhouse AG vom 18. April 2017.

[30] Siehe SIMON ROTH, a.a.O., S. 36 m.w.H.

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 (Persönlichkeitsprofil), 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.[31]

In der Praxis kann ein Profiling durch Bundesorgane auch aus anderen Gründen (d.h. ohne ein Persönlichkeitsprofil als Ergebnis) zu schwerwiegenden Eingriffen in die Grundrechte der betroffenen Personen führen. Zu denken ist etwa an das Profiling von minderjährigen und anderen schutzbedürftigen Personen oder an ein Profiling, das zur Verweigerung einer wichtigen Leistung führen kann. Diese Risiken sind bei der Erarbeitung der Rechtsgrundlagen nach Art. 34 ff. nDSG oder bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 22 nDSG (► Ziff. 4.3) mitzuberücksichtigen, zumal die entsprechenden Bestimmungen nicht an das Vorliegen eines Profilings mit hohem Risiko gemäss Art. 5 Bst. g nDSG knüpfen.

dd) Grundsatz: Grundlage in einem Gesetz im formellen Sinn

Gemäss Art. 34 Abs. 2 Bst. b nDSG gilt, dass Bundesorgane zu einem Profiling in der Regel durch eine **formell-gesetzliche Grundlage** ermächtigt werden müssen. Diese Bestimmung ersetzt den heutigen Art. 17 Abs. 2 DSG, nach welchem Bundesorgane Persönlichkeitsprofile nur bearbeiten dürfen, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht. Das Erfordernis des formellen Gesetzes gilt nicht nur beim Profiling mit hohem Risiko, sondern auch beim «gewöhnlichen» Profiling. Eine Verordnungsbestimmung kommt nur unter den Voraussetzungen von Art. 34 Abs. 3 nDSG in Frage (► nachfolgend Bst. ee).

Die formell-gesetzliche Grundlage für das Profiling muss eine **ausreichende Bestimmtheit** aufweisen. Dazu gehört, dass die Rechtsgrundlage das Profiling i.S.v. Art. 5 Bst. f nDSG ausdrücklich vorsieht oder adäquat umschreibt. Dasselbe gilt für das Profiling mit hohem Risiko nach Art. 5 Bst. g nDSG. Aufgrund des Verhältnismässigkeitsprinzips dürfen Bundesorgane nur dann zum Profiling oder Profiling mit hohem Risiko ermächtigt werden, wenn dies zur Aufgabenerfüllung notwendig ist. Es sind immer auch andere Datenbearbeitungsmethoden in Betracht zu ziehen. Bei der Verhältnismässigkeitsprüfung ist unter anderem zu fragen, ob alternative Bearbeitungsoptionen bei gleicher Wirksamkeit die Persönlichkeit der betroffenen Personen besser schonen würden. Des Weiteren müssen in der Rechtsgrundlage mindestens der Zweck des Profilings sowie die Kategorien der besonders schützenswerten Daten nach Art. 5 Bst. c Ziff. 1–6 nDSG, welche in das Profiling einfliessen, genannt werden. Auch sollte für die betroffene Person erkennbar sein, welche ihrer persönlichen Merkmale durch das Profiling bewertet werden. Es ist im Einzelfall zu klären, welche weiteren Punkte gegebenenfalls in der Rechtsgrundlage umschrieben werden müssen (z.B. welche «gewöhnlichen» Personendaten in das Profiling einfliessen). Abzubilden sind diejenigen Parameter des Profilings, welche für den Eingriff in die informationelle Selbstbestimmung besonders entscheidend sind.

[31] Zur Beurteilung dieses Sachverhalts unter geltendem Recht bzw. zum Begriff des Persönlichkeitsprofils vgl. das Urteil des Bundesverwaltungsgerichts A-4232/2015 i.S. EDÖB gegen Moneyhouse AG vom 18. April 2017.

Wichtig ist schliesslich, dass die Bundesorgane geeignete mathematische oder statistische Verfahren für das Profiling verwenden sowie technische und organisatorische Massnahmen treffen, mit denen das Fehler- und Diskriminierungsrisiko minimiert werden.

Schliesslich stellt sich die Frage, ob auch besondere Rechtsgrundlagen für den Umgang mit **Daten, die aus einem Profiling resultieren**, geschaffen werden müssen. Solche Daten sind nicht immer besonders schützenswerte Personendaten. Es kann sich dabei auch um «gewöhnliche» Personendaten handeln (wie z.B. die Information, dass jemand als nicht kreditwürdig eingeschätzt wird). Die Frage sollte in den einzelnen Rechtssetzungsprojekten aufgeworfen werden und unter Berücksichtigung des jeweiligen Kontextes beurteilt werden.

ee) Senkung der Anforderungen an die Normstufe unter bestimmten Voraussetzungen

Wie für die Bearbeitung von besonders schützenswerten Personendaten ist gemäss Art. 34 Abs. 3 nDSG auch für das Profiling eine Grundlage in einem Gesetz im materiellen Sinn ausreichend, wenn zwei Voraussetzungen (kumulativ) erfüllt sind:

- Das Profiling ist **für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe unentbehrlich**.
- Der **Zweck des Profilings** birgt für die Grundrechte der betroffenen Person **keine besonderen Risiken**.

Vgl. dazu die Ausführungen unter ► Ziff. 2.2.1 Bst. a)/cc.

c) Schwerwiegender Eingriff in die Grundrechte der betroffenen Person (Art. 34 Abs. 2 Bst. c nDSG)

aa) Erfordernis der Grundlage in einem Gesetz im formellen Sinn

Art. 34 Abs. 2 Bst. c nDSG hält neu ausdrücklich fest, was bereits aufgrund von Art. 36 Abs. 1 BV gilt: Unabhängig davon, ob besonders schützenswerte Personendaten bearbeitet werden oder ein Profiling durchgeführt wird, bedarf es einer Grundlage in einem Gesetz im formellen Sinn, wenn der **Zweck einer Datenbearbeitung** (► nachfolgend Bst. bb) oder die **Art und Weise der Datenbearbeitung** (► nachfolgend Bst. cc) zu einem **schwerwiegenden Eingriff in die Grundrechte** der betroffenen Person führen können (► zu den relevanten Grundrechten vgl. Ziff. 2.2.1 Bst. a)/cc). Eine Senkung der Anforderungen an die Normstufe nach Art. 34 Abs. 3 nDSG ist in diesen Fällen nicht möglich. Neben der Eingriffsintensität in die Grundrechte der betroffenen Person sind auch weitere allgemeine Kriterien wie die Grösse des Adressatenkreises, die politische Bedeutung, die Akzeptanz in der Bevölkerung, die Abweichung von geltenden Regelungen oder die zeitliche Dimension der Auswirkungen der Datenbearbeitung zu berücksichtigen.

bb) Schwerwiegender Eingriff in die Grundrechte aufgrund des Zwecks der Datenbearbeitung (erster Anwendungsfall von Art. 34 Abs. 2 Bst. c nDSG)

Ein schwerwiegender Eingriff in die Grundrechte der betroffenen Person kann sich aus dem **Zweck der Datenbearbeitung** ergeben. Als Beispiel wird in der Botschaft des Bundesrates vom 15. September 2017 angeführt, dass Bundesorgane in gewissen Bereichen Personendaten bearbeiten, um etwa die Gefährlichkeit, das Potenzial für eine Funktion, die Eignung für die Erfüllung einer gesetzlichen Pflicht oder die Lebensführung einer Person zu beurteilen. Je nach Zweck, den das Bundesorgan damit verfolgt, kann eine solchen Datenbearbeitung die Grundrechte der betroffenen Person – unabhängig von der Art der bearbeiteten Daten – in

schwerwiegender Weise einschränken, sodass sie in einem Gesetz im formellen Sinn vorgesehen werden muss (► BBl **2017** 6941, 7079 f.). Für dieses Beispiel, in welchem es um die Bewertung bestimmter Eigenschaften einer Person geht, ist allerdings zu beachten, dass bei einem hohen Automatisierungsgrad der Datenbearbeitung auch ein Profiling nach Art. 5 Bst. f nDSG vorliegen könnte (► Ziff. 2.2.1 Bst. b)).

cc) Schwerwiegender Eingriff in die Grundrechte aufgrund der Art und Weise der Datenbearbeitung (zweiter Anwendungsfall von Art. 34 Abs. 2 Bst. c nDSG)

Ein schwerwiegender Eingriff in die Grundrechte der betroffenen Person kann sich ausserdem aus der **Art und Weise einer Datenbearbeitung** ergeben. Dies kann beispielsweise der Fall sein, wenn die Form der Datenbeschaffung (insbesondere die geheime Beschaffung oder die Überwachung mittels Kamera) eine Eingriffsintensität erreicht, welche eine formell-gesetzliche Rechtsgrundlage erforderlich macht. Auch für neue Technologien (z.B. biometrische Verfahren wie die Gesichtserkennung) sind in der Regel klare formell-gesetzliche Grundlagen erforderlich.[32]

Nachfolgend wird besonders auf den **Einsatz von künstlicher Intelligenz[33] in der Verwaltung** eingegangen. Die Verwaltung kann künstliche Intelligenz in unterschiedlichen Aufgabenbereichen und mit unterschiedlicher Intensität nutzen. Die Einsatzmöglichkeiten reichen von einer lediglich *internen Unterstützung mit keiner oder nur geringer Aussenwirkung* (z.B. Anwendungen, die automatisiert Aufgaben an die Mitarbeitenden verteilen, Dokumente übersetzen oder Gesprächsprotokolle erstellen) über *Systeme, welche die Verwaltung in der Entscheidungsfindung unterstützen* (Teilautomatisation), bis hin zu *Systemen, welche die Entscheidung selber treffen* (Vollautomation). Nachfolgend soll auf die zwei letzteren Fallgruppen eingegangen werden: Das nDSG enthält verschiedene Vorschriften zu den automatisierten Einzelentscheidungen (Vollautomatisation; Fallgruppe 1). In der Praxis ist derzeit aber der Einsatz von künstlicher Intelligenz zur Entscheidungsunterstützung von grösserer Bedeutung (Teilautomation; Fallgruppe 2). Besonderes Potenzial für künstliche Intelligenz besteht in erster Linie in der Massenverwaltung, wo die Verwaltung in einer grossen Anzahl von ähnlich gelagerten Fällen verfügt (z.B. Steuer- oder Sozialversicherungsverfahren).[34]

Hinweis: Eine interdepartementale Arbeitsgruppe des Bundes hat sich unter der Leitung des SBFI mit dem Umgang mit künstlicher Intelligenz auseinandergesetzt. Dabei sind unter anderem die Leitlinien «Künstliche Intelligenz» für die Bundesverwaltung entstanden, welche der Bundesrat am 25. November 2020 verabschiedet hat.[35] Eine ausführliche Diskussion der rechtlichen und ethischen Herausforderungen der künstlichen Intelligenz findet sich ausserdem in der vom Kanton Zürich in Auftrag gegebenen Studie «Einsatz Künstlicher Intelligenz in der Verwaltung» vom 28. Februar 2021. Aus dieser Studie stammen auch die nachfolgenden Beispiele zur Anwendung von künstlicher Intelligenz in der (hauptsächlich kantonalen) Verwaltung.

---

[32] Vgl. DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Zürich 2008 («Handkommentar DSG»), Art. 17 DSG N 26 ff.; CLAUDIA MUND, SHK DSG, Art. 17 DSG N 9.

[33] Es gibt noch keine allgemeingültige Definition des Begriffs der künstlichen Intelligenz. Eingehend zur Terminologie und Funktionsweise NADJA BRAUN BINDER/MATTHIAS SPIELKAMP/CATHERINE EGLI, in Staatskanzlei Kanton Zürich (Hrsg.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28. Februar 2021, S. 10. Im Bericht «Herausforderungen der künstlichen Intelligenz» der interdepartementalen Arbeitsgruppe des Bundes «Künstliche Intelligenz» vom 13. Dezember 2019 wird der Begriff der künstlichen Intelligenz (KI) nicht abstrakt definiert, sondern durch verschiedene strukturelle Elemente charakterisiert. Danach sind KI-Systeme in der Lage, (1) Daten in Komplexität und Menge in einer Form auszuwerten, die mit anderen Technologien nach heutigem Stand nicht möglich wäre, insbesondere, wenn Algorithmen selbstständig lernen und dabei in Daten relevante statistische Merkmale finden; (2) Vorhersagen als wesentliche Grundlage für (automatisierte) Entscheidungen zu erstellen; (3) dadurch Fähigkeiten nachzubilden, die mit menschlicher Kognition und Intelligenz in Verbindung gebracht werden; (4) auf dieser Basis weitgehend autonom zu agieren.

[34] Zum Ganzen JESSICA WULF/CATHERINE EGLI, in Staatskanzlei Kanton Zürich (Hrsg.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28. Februar 2021, S. 23 f.

[35] Vgl. dazu die Webseite des SBFI; abrufbar unter <https://www.sbfi.admin.ch/sbfi/de/home/bfi-politik/bfi-2021-2024/transversale-themen/digitalisierung-bfi/kuenstliche-intelligenz.html>.

Beispiele[36]:

- *Steuerverfahren*: Aktuell prüfen verschiedene Kantone den Einsatz von künstlicher Intelligenz in Steuerverfahren. Heute werden in den meisten Kantonen die digital eingereichten Steuererklärungen durch automatische Veranlagungsprogramme zumindest teilweise automatisiert bearbeitet. In Zukunft soll die künstliche Intelligenz die Steuerverwaltungen noch stärker unterstützen. Dazu wird insbesondere die vollautomatische Veranlagung gefördert. Künstliche Intelligenz könnte daneben aber auch zur Entscheidungsunterstützung eingesetzt werden, z.B. zur Unterstützung der für die Steuerveranlagung zuständigen Fachpersonen mit konkreten Hinweisen auf Fehlerbereiche oder für einen automatischen Abgleich zwischen Steuererklärung und eingereichten Dokumenten.
- *Sozialversicherungsverfahren*: Im Sozialrecht finden sich in der Schweiz noch wenig Technologien der künstlichen Intelligenz. Insbesondere der Kanton Genf möchte künstliche Intelligenz zur Sozialversicherungsbetrugsbekämpfung einsetzen. Damit sollen unter anderem ungerechtfertigte Sozialleistungsbezüge aufgedeckt werden können (z.B. Entwicklung von Algorithmen für Warn- und Erinnerungssysteme, zur Durchführung von Konsistenzkontrollen und Kreuzanalysen der Einkommens- und Vermögensschwankungen).
- *Ortsbezogenes «Predictive Policing»*: Die Kantonspolizeien Aargau und Basel-Landschaft sowie die Stadtpolizei Zürich setzen die in Deutschland entwickelte Software PRECOBS zur Bekämpfung von Wohnungseinbruchsdiebstählen ein. Die Anwendung auf weitere Deliktstypen wird geprüft. PRECOBS basiert auf der Theorie, dass (professionelle) Einbrüche häufig serienmässig sowie örtlich und zeitlich konzentriert erfolgen. Die Software trifft Vorhersagen über erhöhte Wahrscheinlichkeiten für Wohnungseinbrüche in bestimmten Gebieten zu bestimmten Zeiten.
- *Personenbezogenes Predictive Policing*: Einige Kantone (darunter Luzern und St. Gallen) setzen das Analysetool DyRiAS-Intimpartner ein, welches das Risikopotenzial einer männlichen Person, Gewaltdelikte gegen die aktuelle oder ehemalige Partnerin zu begehen, analysiert. Allerdings hat sich gezeigt, dass DyRiAS mit einer Risikoüberschätzung arbeitet.
- Bei der *automatischen Fahrzeugerkennung und Verkehrsüberwachung*[37] werden die Kontrollschilder von Fahrzeugen mittels einer Kamera erfasst und die Identität der Fahrzeughalterin oder des Fahrzeughalters sowie Zeitpunkt, Standort, Fahrtrichtung und andere Fahrzeuginsassen ermittelt. Diese Daten werden anschliessend automatisiert mit anderen Datenbanken abgeglichen, z.B. um gestohlene Fahrzeuge zu finden oder Kriminelle zu verfolgen. Der grösste Anteil der aktiven AFV-Kameras wird derzeit vom Grenzwachtkorps des Bundes zur Bekämpfung von grenzüberschreitender Kriminalität eingesetzt.
- *Justizvollzug*: In der Urteilsfindung werden in der Schweiz (noch) keine Anwendungen der künstlichen Intelligenz eingesetzt. Zu erwähnen ist dagegen der Strafvollzug, wo (in der ganzen Deutschschweiz) anhand des Programms ROS (Risikoorientierter Sanktionenvollzug) die Möglichkeit von Vollzugslockerungen geprüft wird. Dabei werden Daten zu einer Person aus dem Strafregisterauszug (z.B. Alter, begangene Gewaltdelikte vor dem 18. Lebensjahr, Anzahl der Vorstrafen oder Strafmass) in das vollautomatisierte Fall-Screening-Tool (FaST) überführt, welches eine Triage in drei Risikokategorien betreffend die Flucht- und Rückfallgefahr der inhaftierten Person vornimmt. Dies dient als Basis für die Entscheidung, ob eine vertiefte risikoorientierte Einzelfallanalyse notwendig ist.

[36] Die Beispiele stammen von NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Staatskanzlei Kanton Zürich (Hrsg.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28. Februar 2021, S. 23 f.

[37] Zur automatischen Fahrzeugfahndung und Verkehrsüberwachung (AFV) vgl. BGE **146** I 11.

- **Fallgruppe 1: Automatisierte Einzelentscheidungen**

  Als automatisierte Einzelentscheidung gilt gemäss Art. 21 Abs. 1 nDSG «eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für [die betroffene Person] mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt».

  Zur Begriffsdefinition:

  – **Die Entscheidung beruht ausschliesslich auf einer automatisierten Datenbearbeitung**: Das bedeutet, dass sowohl die inhaltliche Beurteilung eines Sachverhalts als auch die darauf basierende Entscheidung durch eine Maschine bzw. einen Algorithmus erfolgt, ohne dass eine natürliche Person mitwirkt. Ob die Programmierung des Algorithmus durch einen Menschen erfolgt, ist hingegen nicht massgeblich. Die automatisierte Einzelentscheidung kann auf einem einfachen regelbasierten Algorithmus beruhen. Sie kann aber auch von einer Anwendung getroffen werden, welche fähig ist, aus grossen Mengen von Daten und darin enthaltenen Korrelationen eigenständig Regeln zu entwickeln sowie anzuwenden (maschinelles Lernen)[38]. Eine automatisierte Einzelentscheidung liegt im Übrigen auch dann vor, wenn die Entscheidung zwar von einer natürlichen Person mitgeteilt wird, von dieser aber nicht vorgenommen worden ist.[39]

    Dabei ist zu beachten, dass eine wortlautgetreue Auslegung von Art. 21 Abs. 1 nDSG den Anwendungsbereich der Vorschriften zu den automatisierten Einzelentscheidungen sehr weit ziehen würde. In der Botschaft vom 15. September 2017 hat der Bundesrat deshalb festgehalten, dass nur eine Entscheidung, welche eine «**gewisse Komplexität**» aufweist, die Begriffsdefinition erfüllt (► BBl **2017** 6941, 7057). Zwar wird das erforderliche Mass an Komplexität, welches einer automatisierte Einzelentscheidung innewohnen muss, in der Botschaft nicht näher definiert. Aus dem Schutzzweck der einschlägigen Bestimmungen des nDSG (namentlich Art. 21, Art. 25 Abs. 2 Bst. f und Art. 34 Abs. 2 Bst. c nDSG) lässt sich aber schliessen, dass sich diese insbesondere gegen Entscheidungsprozesse richten, die für die betroffenen Personen nicht nachvollziehbar sind.[40] Im Sinne einer teleologischen Reduktion von Art. 21 Abs. 1 nDSG 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. Dazu gehören beispielsweise der Bezug von Geld aus einem bestehenden Guthaben am Bancomaten oder die chipkartenbasierte Zutrittskontrolle anhand vorgegebener Listen zutrittsberechtigter Personen.[41] Aber auch simple mathematische Operationen (wie z.B. das reine Zusammenzählen von Werten) dürften in der Regel die für eine automatisierte Einzelentscheidung i.S.v. Art. 21 Abs. 1 nDSG erforderliche Komplexität nicht erreichen.

  – **Wirkung der Entscheidung:** Des Weiteren werden vom Begriff der automatisierten Einzelentscheidung nach Art. 21 Abs. 1 nDSG 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

---

38 Vgl. NADJA BRAUN BINDER/MATTHIAS SPIELKAMP/CATHERINE EGLI, in Staatskanzlei Kanton Zürich (Hrsg.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28. Februar 2021, S. 19.

39 Vgl. DAVID RECHSTEINER, Der Algorithmus verfugt. Verfassungs- und verwaltungsrechtliche Aspekte automatisierter Einzelentscheidungen, in: Jusletter vom 26. November 2018, Rz. 1 und 5 f.

40 So zum Schutzzweck von Art. 22 der EU-Datenschutz-Grundverordnung 2016/679 unter anderem MARTIN EBERS/CHRISTIAN A. HEINZE/TINA KRÜGEL/BJÖRN STEINRÖTTER (Hrsg.), Künstliche Intelligenz und Robotik, München 2020, § 11 Rz. 41 f.

41 Vgl. betreffend Art. 22 der EU-Datenschutz-Grundverordnung 2016/679 SEBASTIAN SCHULZ, in: PETER GOLA (Hrsg.), Kommentar zur DS-GVO, 2. A., München 2018, Art. 22 DS-GVO Rz. 20; GISELHER RÜPKE/KAI VON LEWINSKI/JENS ECKHARDT, Datenschutzrecht, München 2018 § 16 Rz. 11; MARTIN EBERS/CHRISTIAN A. HEINZE/TINA KRÜGEL/BJÖRN STEINRÖTTER (Hrsg.), a.a.O., § 11 Rz. 41 f.

im privatrechtlichen Bereich namentlich bei Abschluss eines Vertrags oder dessen Kündigung der Fall. Der Nichtabschluss eines Vertrags entfaltet hingegen in der Regel keine rechtliche Wirkung, denn die Rechtsposition der betroffenen Person wird gerade nicht verändert (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 Verfügungen vollautomatisiert erlassen wird (► BBl **2017** 6941, 7057). Noch offen ist, ob auch eine positive Rechtsfolge die Begriffsdefinition erfüllt. In der europäischen und schweizerischen Lehre wird dies aufgrund des Schutzzweckes der Norm zum Teil abgelehnt, da die betroffene Person vor einer vollständig begünstigenden Entscheidung nicht geschützt werden müsse. Aufgrund des Verweises in Art. 21 Abs. 4 nDSG auf Art. 30 Abs. 2 des Verwaltungsverfahrensgesetzes (VwVG) könnte für Bundesorgane aber auch geschlossen werden, dass bei einer automatisierten Einzelentscheidung, die den Begehren der betroffenen Person voll entspricht, lediglich der Anspruch auf Anhörung und Überprüfung durch eine natürliche Person nach Art. 21 Abs. 2 nDSG, nicht aber die Informationspflicht nach Art. 21 Abs. 1 und 4 nDSG entfällt.

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. Eine erhebliche Beeinträchtigung kann beispielsweise vorliegen, wenn medizinische Leistungen auf der Basis automatisierter Entscheidungen zugeteilt werden (► BBl **2017** 6941, 7057).

– **Verhältnis zum Profiling (► Ziff. 2.2.1 Bst. b))**: 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.[42] 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).[43]

– Mit den Bestimmungen im nDSG zu den automatisierten Einzelentscheidungen werden unter anderem die Anforderungen von Art. 9 Abs. 1 Bst. a der Datenschutz-Konvention 108+ des Europarates sowie von Art. 11 der EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen umgesetzt. Ausserdem wird das schweizerische Datenschutzrecht damit der EU-Datenschutz-Grundverordnung 2016/679 (Art. 14 Abs. 2 Bst. g und Art. 22) angenähert. Diese **europäischen Vorschriften** sind deshalb im Rahmen der Auslegung des Begriffs der automatisierten Einzelentscheidung mitzuberücksichtigen.

---

[42] Art. 19 Abs. 1 E-DSG (nach der Schlussabstimmung: Art. 21 Abs. 1 nDSG) lautete im Entwurf des Bundesrates wie folgt: «Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung, *einschliesslich Profiling*, beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt». Im Parlament wurde der Einschub «einschliesslich Profiling» gestrichen. Wie die Departementsvorsteherin des EJPD im Ständerat am 18. Dezember 2019 ausführte, hat diese Streichung materiell keine Änderung zur Folge (vgl. AB **2019** S 1241). Das Profiling hat in dieser Bestimmung keine selbstständige Bedeutung und fällt mit oder ohne ausdrückliche Erwähnung in den Anwendungsbereich von Art. 19 Abs. 1 E-DSG bzw. Art. 21 Abs. 1 nDSG, sofern es zu einer automatisierten Einzelentscheidung führt. Dies gilt sowohl für das «gewöhnliche» Profiling» als auch für das Profiling mit hohem Risiko nach Art. 5 Bst. g nDSG.

[43] Siehe dazu die «Leitlinien zu automatisierten Entscheidungen im Einzelfall einschliesslich Profiling für die Zwecke der Verordnung 2016/679» der ehemaligen Artikel-29-Datenschutzgruppe vom 6. Februar 2018, S. 8 f. mit Beispielen.

Zu den Anforderungen an die Rechtsgrundlage:

- **Normstufe**: Automatisierte Einzelentscheidungen können unter Umständen zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person nach Art. 34 Abs. 2 Bst. c nDSG führen, sodass eine Ermächtigung in einem Gesetz im formellen Sinn erforderlich ist (vgl. dazu die Botschaft des Bundesrates vom 15. September 2017: ► BBl **2017** 6941, 7080). Dies ist insbesondere dann der Fall, wenn die automatisierte Einzelentscheidung auf einem Profiling oder der Bearbeitung von besonders schützenswerten Personendaten beruht. Des Weiteren ist zu berücksichtigen, wie stark und dauerhaft die automatisierte Einzelentscheidung in die Rechte der betroffenen Person eingreift oder die betroffene Person anderweitig beeinträchtigt. Ausserdem gilt: Je komplexer eine automatisierte Einzelentscheidung ist, d.h. je schwieriger sie für die betroffene Person nachzuvollziehen ist, desto eher ist eine formell-gesetzliche Grundlage zu verlangen. Automatisierte Einzelentscheidungen können ferner z.B. auch aus verfahrens- oder organisationsrechtlichen Gründen als wichtige Frage betrachtet werden, für welche nach Art. 164 Abs. 1 Bst. g BV eine Grundlage im formellen Gesetz erforderlich ist. So braucht es unter anderem dann eine formell-gesetzliche Grundlage, wenn ein Verwaltungsverfahren ausschliesslich elektronisch geführt wird.

- **Normdichte**: In der Rechtsgrundlage muss die die automatisierte Einzelentscheidung ausdrücklich vorgesehen oder adäquat umschrieben werden. Auch muss daraus hervorgehen, welche Arten von Verfügungen vollautomatisiert erlassen werden dürfen (z.B. Verfügungen zur Festsetzung einer Abgabe) und welche Daten darin einfliessen. Schliesslich sollte für die betroffene Person zumindest in groben Zügen erkennbar sein, auf welcher Logik die automatisierte Einzelentscheidung beruht (z.B. Art und Gewichtung der Daten). Ob noch weitere Aspekte in der Rechtsgrundlage genannt werden müssen, ist im Einzelfall zu klären.

Weitere Rechtsfolgen bei automatisierten Einzelentscheidungen:

Gemäss Art. 21 Abs. 1 und 4 nDSG besteht bei automatisierten Einzelentscheidungen eine **Pflicht zur Information** der betroffenen Person. Bundesorgane müssen ihre vollautomatisiert erlassenen Entscheidungen entsprechend kennzeichnen. Art. 21 Abs. 2 nDSG räumt der betroffenen Person sodann das **Recht** ein, auf Antrag **ihren Standpunkt darzulegen** und zu verlangen, dass der Entscheid **von einer natürlichen Person überprüft** wird. Für Bundesorgane ist Art. 21 Abs. 2 nDSG nicht anwendbar, wenn die betroffene Person nach Art. 30 Abs. 2 VwVG 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). Schliesslich müssen der betroffenen Person im Rahmen ihres **Auskunftsrechts** gemäss Art. 25 Abs. 2 Bst. f nDSG Angaben über das Vorliegen einer automatisierten Einzelentscheidung sowie zur Logik, auf der die Entscheidung beruht, gemacht werden. Wird ein Bundesorgan zur Durchführung von automatisierten Einzelentscheidungen ermächtigt, ist zu **prüfen, ob all diese Vorgaben eingehalten werden können**.

Vereinbarkeit mit dem Verfassungs- und Verfahrensrecht:

Beim Einsatz von automatisierten Einzelentscheidungen in der Bundesverwaltung stellt sich – unabhängig von den datenschutzrechtlichen Vorgaben – die Frage, ob und unter welchen Voraussetzungen der vollautomatisierte Erlass von Verfügungen mit den verfassungs- und verwaltungsrechtlichen Grundsätzen überhaupt vereinbar ist. Insbesondere aus den Verfahrensgarantien (Art. 29 ff. BV; VwVG) könnten sich weitere Einschränkungen für automatisierte Einzelentscheidungen ergeben.

Nachfolgend werden einige in der Lehre aufgeworfene Grundsatzfragen aufgelistet, die weiter zu vertiefen sind:

- **Untersuchungsgrundsatz und Mitwirkungspflichten** (Art. 12 ff. VwVG): Können bei automatisierten Einzelentscheidungen die verfahrensrechtlichen Vorgaben an die Sachverhaltsfeststellung eingehalten werden?[44] Von zentraler Bedeutung ist, dass die im Rahmen der automatisierten Einzelentscheidung genutzten Daten vollständig, korrekt und im notwendigen Umfang verfügbar sind. Dies gilt insbesondere auch für die beim maschinellen Lernen eingesetzten Trainingsdaten.[45]
- **Diskriminierungsverbot**: Grosse Herausforderungen stellen sich sodann mit Blick auf das Diskriminierungsverbot. Bei automatisierten Einzelentscheidungen besteht – wie beim Einsatz von künstlicher Intelligenz allgemein – das Risiko, dass sich in den Datensätzen, welche zur Entwicklung oder zum Training von künstlicher Intelligenz verwendet werden werden, historisch gewachsene Vorurteile niederschlagen, sodass (unbewusste) Diskriminierungen verstärkt werden. Vor diesem Hintergrund ist die Sicherstellung der Datenqualität entscheidend. Weitere Massnahmen könnten auch der Einsatz von Kontrollalgorithmen, welche die Gewichtung der in die Entscheidung einfliessenden Faktoren analysieren, oder regelmässige Kontrollen durch andere staatliche Institutionen oder Drittorganisationen sein.[46]
- **Recht auf Begründung**: Des Weiteren stellt sich die Frage, wie bei automatisierten Einzelentscheidungen das Recht auf Begründung gewährleistet werden kann. Bei einem regelbasierten Algorithmus, der – ähnlich der juristischen Denkweise eines Menschen – das Vorhandensein gewisser Voraussetzungen prüft, dürfte dies vermutlich keine grösseren Schwierigkeiten bereiten. Zweifelhaft ist dagegen, ob eine rechtlich genügende Begründung bei einer auf künstlicher Intelligenz basierenden automatisierten Einzelentscheidung möglich ist, da die Funktionsweise von maschinellen Lernverfahren oft nur sehr schwer nachvollziehbar ist.[47] Gemäss der vom Kanton Zürich in Auftrag gegebenen Studie zum Einsatz künstlicher Intelligenz in der Verwaltung muss eine Verfügung, die mithilfe von künstlicher Intelligenz erlassen wird, unter anderem Angaben zur Entscheidungslogik des Algorithmus mit Art, Menge, Erhebungszeitraum und Gewichtung der Daten sowie zur Anwendung der Entscheidungslogik auf den konkreten Einzelfall machen. Darüber hinaus können Angaben über die Vergleichsgruppe, in welche der Algorithmus eine Person einordnet, und die im Einzelfall entscheidenden individuellen Besonderheiten erforderlich sein. Ausnahmsweise und unter besonderen Umständen wird auch die Offenlegung des Quellcodes des Algorithmus in Betracht gezogen.[48]
- **Ermessens- und Beurteilungsspielraum**: Schliesslich ist unklar, ob automatisierte Einzelentscheidungen bei Bestehen eines behördlichen Ermessens- oder Beurteilungsspielraums möglich sein sollen. Diese Frage wird in der Lehre zum Teil verneint. So wird argumentiert, dass es rechtsfehlerhaft sei, wenn ein Bundesorgan durch den Erlass einer automatisierten Verfügung auf die Ausübung seines Ermessens- bzw. Beurteilungsspielraums verzichtet. Einzelfallgerechtigkeit bedinge die Möglichkeit zur Abweichung von Regeln. Regelbasierte Algorithmen seien aber nicht in der Lage, solche

---

[44] NADJA BRAUN BINDER, Automatisierte Entscheidungen: Perspektive Datenschutzrecht und öffentliche Verwaltung, in SZW 2020 S. 27 ff.

[45] NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Staatskanzlei Kanton Zürich (Hrsg.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28. Februar 2021, S. 38 f.

[46] Vgl. NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Staatskanzlei Kanton Zürich (Hrsg.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28. Februar 2021, S. 39 ff.

[47] DAVID RECHSTEINER, a.a.O., Rz. 24 ff.

[48] NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Staatskanzlei Kanton Zürich (Hrsg.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28. Februar 2021, S. 38.

Spielräume auszufüllen. Bei Algorithmen, welche auf maschinellem Lernen basieren, bestehe zwar keine starre Regelbindung. Dafür beruhe ihre Entscheidungsfindung ausschliesslich auf bereits gefällten, vergangenen Entscheidungen, was der korrekten Beurteilung eines bisher noch unbekannten Einzelfalls entgegenstehe.[49]

- **Fallgruppe 2: Unterstützender Einsatz von künstlicher Intelligenz**

  Keine automatisierte Einzelentscheidung nach Art. 21 Abs. 1 nDSG liegt vor, wenn ein Entscheid lediglich *automatisiert vorbereitet*, aber von einer natürlichen Person getroffen wird. Auch zur **automatisierten Entscheidungs*unterstützung*** werden in naher Zukunft wohl vermehrt auf künstlicher Intelligenz basierende Systeme herangezogen. Die bei den automatisierten Einzelentscheidungen aufgezeigten rechtlichen Herausforderungen stellen sich in ähnlicher Weise beim lediglich unterstützenden Einsatz von künstlicher Intelligenz, wenn auch zum Teil andere Lösungsmöglichkeiten bestehen. So kann beispielweise zur Verhinderung diskriminierender Entscheidungen darauf hingewirkt werden, dass die Sachbearbeitenden über die notwendigen Kenntnisse und Kompetenzen verfügen, um diskriminierende Vorschläge der künstlichen Intelligenz zu erkennen und davon abweichende Entscheidungen zu treffen.[50]

  Werden beim unterstützenden Einsatz von künstlicher Intelligenz Personendaten bearbeitet, ist sicherzustellen, dass sowohl hinsichtlich der Normstufe als auch bezüglich der Normdichte eine ausreichende **Rechtsgrundlage** existiert, welche die Anforderungen des Art. 34 nDSG erfüllt. Kann die Art und Weise der Datenbearbeitung bzw. des Einsatzes der künstlichen Intelligenz zu schwerwiegenden Eingriffen in die Grundrechte der betroffenen Personen führen, ist nach Art. 34 Abs. 2 Bst. c nDSG eine formell-gesetzliche Grundlage erforderlich. Betreffend die Normdichte sind dieselben Anforderungen wie bei den automatisierten Einzelentscheidungen (► Fallgruppe 1) und beim Profiling (► Ziff. 2.2.1 Bst. b)/dd) zu stellen: In die Rechtsgrundlage sind insbesondere der Zweck des Einsatzes der künstlichen Intelligenz, die Daten, die in KI-Anwendung einfliessen und die der Anwendung zugrundliegende Logik (z.B. Art und Gewichtung der Daten) sowie (wenn anwendbar) die beurteilten Merkmale der Persönlichkeit zu nennen. Ob noch weitere Aspekte in der Rechtsgrundlage genannt werden müssen, ist im Einzelfall zu klären.

2.2.2 Art und Weise der Datenbekanntgabe: Aufhebung der erhöhten Anforderungen an die Rechtsgrundlage für das Abrufverfahren

Das Abrufverfahren («Online-Zugriff») ist eine besondere Form der Datenbekanntgabe. Es handelt sich um ein automatisiertes Verfahren, bei welchem sich der Datenempfänger die Personendaten beschaffen kann, ohne dass das datenbesitzende Bundesorgan mitwirken muss bzw. den Datenbezug überhaupt bemerkt («Prinzip der Selbstbedienung»). Nach dem geltenden Art. 19 Abs. 3 DSG dürfen Bundesorgane Personendaten nur dann durch ein Abrufverfahren zugänglich machen, wenn dies in der Rechtsgrundlage ausdrücklich vorgesehen ist. Bei besonders schützenswerten Personendaten (und Persönlichkeitsprofilen) ist das Abrufverfahren sogar nur dann zulässig, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht.

Diese erhöhten Anforderungen an die Rechtsgrundlagen für Abrufverfahren werden mit der Totalrevision des DSG aufgehoben. Gemäss der Botschaft des Bundesrates vom 15. Septem-

---

[49] DAVID RECHSTEINER, a.a.O., Rz. 28 ff. Vgl. auch NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Staatskanzlei Kanton Zürich (Hrsg.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28. Februar 2021, S. 46 ff., welche ebenfalls zum Schluss kommen, das künstliche Intelligenz in der Verwaltung nicht eingesetzt werden sollte, wo Ermessens- oder Beurteilungsspielräume bestehen.

[50] Vgl. NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Staatskanzlei Kanton Zürich (Hrsg.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28. Februar 2021, S. 42.

ber 2017 erscheinen sie im digitalen Zeitalter als überholt (► BBl **2017** 6941, 7083). Mit anderen Worten: Die Form des Abrufverfahrens muss inskünftig in der gesetzlichen Grundlage nicht mehr ausdrücklich genannt werden. Selbstverständlich wird für die Datenbekanntgabe an sich aber weiterhin eine Rechtsgrundlage benötigt. Ausserdem dürfte es sich in vielen Fällen – insbesondere bei schwerwiegenden Grundrechtseingriffen – aus Gründen der Transparenz gleichwohl aufdrängen, den Umstand, dass es sich um einen «Zugriff» («accès») auf Daten handelt, bei welchem der Datenherr passiv bleibt, im Gesetzes- bzw. Verordnungstext auszuweisen (wobei statt von «Abrufverfahren» auch von «Zugriff auf Daten/Informationssysteme/etc.» gesprochen werden könnte). Zu unterscheiden ist auch, ob es sich um einen «Vollzugriff» oder lediglich einen «Indexzugriff» handelt. Im Übrigen gilt auch inskünftig, dass bei der Gewährung eines Datenzugriffs Zurückhaltung angebracht ist, vor allem wenn der Zweck des Informationssystems, auf welches zugegriffen wird, sich stark vom Zweck unterscheidet, den der Datenempfänger verfolgt. Somit sind immer auch andere Arten der Datenbekanntgabe als der Zugang mittels Abrufverfahren in Betracht zu ziehen.

Neben dem Abrufverfahren werden noch drei weitere Formen der Datenbekanntgabe unterschieden: die Meldepflicht (von Amtes wegen oder auf Anfrage), die spontanen Bekanntgabe sowie die Datenbekanntgabe auf Anfrage und nach eigenem Ermessen der angefragten Behörde; ► vgl. dazu insbesondere den Gesetzgebungsleitfaden (Kapitel 14; Rz. 834 ff.). Diese Formen der Datenbekanntgabe sind in den Rechtsgrundlagen – nicht nur aus datenschutzrechtlichen Gründen – auch weiterhin abzubilden.

3 Daten juristischer Personen

3.1 Ausgangslage: Aufhebung des Schutzes für Daten juristischer Personen im nDSG

Mit der Totalrevision des DSG wird die Bearbeitung von Daten juristischer Personen vom sachlichen Anwendungsbereich des Datenschutzgesetzes ausgenommen. Gemäss Art. 2 Abs. 1 nDSG gilt das Gesetz nur noch für die Personendaten natürlicher Personen. Entsprechend werden Personendaten definiert als «Angaben, die sich auf eine bestimmte oder bestimmbare *natürliche* Person beziehen» (Art. 5 Bst. a nDSG). Geschützt bleiben juristische Personen weiterhin über andere Bestimmungen der schweizerischen Rechtsordnung. So gelten für sie namentlich der Persönlichkeitsschutz gemäss Zivilgesetzbuch (Art. 28 ff. ZGB), das Bundesgesetz gegen den unlauteren Wettbewerb, das Urheberrechtsgesetz oder die Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen.

Die Aufhebung des Schutzes der Daten juristischer Personen im nDSG sowie die Beschränkung des Begriffs der Personendaten auf Angaben zu natürlichen Personen hat verschiedene Auswirkungen auf die Datenbearbeitung durch Bundesorgane. Insbesondere führt diese Neuerung dazu, dass die bundesrechtlichen Grundlagen, mit denen Bundesorgane zur Bearbeitung und Bekanntgabe von *Personendaten* ermächtigt werden, inskünftig nicht mehr anwendbar sind, wenn *Daten juristischer Personen* bearbeitet bzw. bekanntgegeben werden. Aufgrund des Legalitätsprinzips nach Art. 5 Abs. 1 BV und des Erfordernisses der gesetzlichen Grundlage für die Einschränkung von Grundrechten nach Art. 36 Abs. 1 BV bedarf die staatliche Bearbeitung und Bekanntgabe von Daten juristischer Personen aber einer Rechtsgrundlage. Denn auch für juristische Personen gilt der Schutz der Privatsphäre nach Art. 13 BV, selbst wenn sie nicht Trägerinnen sämtlicher Schutzgehalte dieses Grundrechts sind.[51]

Mit der Totalrevision des DSG werden deshalb im Regierungs- und Verwaltungsorganisationsgesetz (nRVOG; Ziff. 13 des Anhangs 1/II zum nDSG) eine Reihe von neuen Bestimmungen eingeführt, welche den Umgang mit Daten juristischer Personen durch Bundesorgane regeln (Art. 57*r* ff. nRVOG; ► Ziff. 3.2). Ausserdem soll die Übergangsbestimmung in Art. 71 nDSG während fünf Jahren mögliche Rechtslücken verhindern (► Ziff. 3.3).

3.2 Neue Bestimmungen zum Umgang mit Daten juristischer Personen im nRVOG

3.2.1 Begriffe

Nachfolgend werden die wichtigsten Begriffe im Zusammenhang mit der Bearbeitung von Daten juristischer Personen durch Bundesorgane[52] erläutert. Dazu werden hauptsächlich die Bestimmungen des DSG bzw. des nDSG hinzugezogen und analog angewendet. In den Art. 57*r* ff. nRVOG wird lediglich der Begriff der «besonders schützenswerten Daten juristischer Personen» definiert.

- **Daten (juristischer Personen)**: Entsprechend dem Begriff der Personendaten (Art. 5 Bst. a nDSG) gelten als Daten juristischer Personen alle Angaben, die sich auf eine bestimmte oder bestimmbare juristische Person beziehen. Ist die juristische Person nicht mindestens bestimmbar (z.B. weil ihre Daten anonymisiert worden sind), so sind die Vorschriften in Art. 57*r* ff. RVOG nicht anwendbar.

[51] BGE **137** II 371 E. 6.

[52] Gemäss der Botschaft des Bundesrates vom 15. September 2017 (► BBl **2017** 6941, 7119.) ist für den Begriff der «Bundesorgane» in den Art. 57*r* ff. nRVOG auf die Legaldefinition in Art. 5 Bst. i nDSG abzustellen («Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist»).

- **juristische Personen**: sind primär alle körperschaftlich organisierten Personenverbindungen sowie die einem besonderen Zweck gewidmeten, selbstständigen Anstalten mit Rechtspersönlichkeit. Dazu gehören der Verein, die Stiftung, die Aktiengesellschaft, die Kommanditaktiengesellschaft, die Gesellschaft mit beschränkter Haftung, die Genossenschaft sowie die privatrechtlichen Körperschaften des kantonalen Rechts und die öffentlich-rechtlichen Anstalten und Körperschaften der Kantone und des Bundes. In der Lehre zum heutigen DSG wird der Begriff der juristischen Personen allerdings in einem erweiterten Sinn verstanden. Über den Wortlaut des Gesetzes hinaus werden auch Personengesellschaften, die zwar keine eigene Persönlichkeit im rechtlichen Sinne haben, aber partei- und prozessfähig sind (wie Kollektivgesellschaften, Kommanditgesellschaften und Stockwerkeigentümergesellschaften), dazu gezählt. Dieses weite Verständnis des Begriffs der juristischen Personen liegt auch den neuen Art. 57*r* ff. nRVOG zugrunde. Nicht erfasst sind dagegen Personenverbindungen, die nach schweizerischem Recht keinerlei Elemente einer Rechtspersönlichkeit aufweisen, wie z.B. einfache Gesellschaften oder Erbengemeinschaften.[53]

- **besonders schützenswerte Daten juristischer Personen**: sind gemäss der abschliessenden Aufzählung in Art. 57*r* Abs. 2 nRVOG:

  – Daten über verwaltungs- und strafrechtliche Verfolgungen und Sanktionen (Bst. a; siehe dazu auch Art. 5 Bst. c Ziff. 5 nDSG)

  – Daten über Berufs-, Geschäfts- und Fabrikationsgeheimnisse (Bst. b)[54].

  Der Katalog der besonders schützenswerten Daten ist bei juristischen Personen damit weniger umfassend als bei natürlichen Personen, auch wenn er mit den «Daten über Berufs-, Geschäfts- und Fabrikationsgeheimnissen» eine neue Datenkategorie aufzählt. Juristische Personen haben hier einen weniger weitgehenden Schutzbedarf als natürliche Personen.

3.2.2 Bearbeitung von Daten juristischer Personen (Art. 57*r* nRVOG)

Art. 57*r* Abs. 1 nRVOG schafft für die *Bearbeitung* von Daten juristischer Personen eine allgemeine, direkt anwendbare gesetzliche Grundlage. Demnach dürfen Bundesorgane Daten juristischer Personen, einschliesslich besonders schützenswerter Daten, bearbeiten:

- soweit dies **für die Erfüllung ihrer Aufgaben erforderlich** ist und
- die **Aufgabe in einem Gesetz im formellen Sinn umschrieben** ist. Eine Verordnungsbestimmung oder eine lediglich implizit abzulesende Aufgabe genügen nicht. Die Aufgabe muss klar erkennbar und hinreichend bestimmt sein.

Sind die Vorgaben von Art. 57*r* Abs. 1 nRVOG erfüllt, so ist keine spezialgesetzliche Ermächtigung mehr erforderlich. Dies gilt sowohl für die Bearbeitung von «gewöhnlichen» Daten juristischer Personen als auch von besonders schützenswerten Daten. Art. 57*r* nDSG bezieht sodann grundsätzlich alle möglichen Bearbeitungsarten, einschliesslich des Profilings, mit ein. Etwas anders gilt jedoch, wenn der Zweck oder die Art und Weise der Datenbearbeitung zu einem derart schwerwiegenden Eingriff in die Grundrechte der betroffenen juristischen Person führen, dass Art. 57*r* nRVOG die Anforderungen des Legalitätsprinzips gemäss Art. 5 Abs. 1 und Art. 36 Abs. 1 BV an die Normdichte nicht mehr erfüllt. In einem solchen Fall ist eine ausdrückliche Regelung im jeweiligen Sacherlass nötig.

---

[53] Zum Ganzen: DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar DSG, Art. 2 DSG N 6 ff., BEAT RUDIN, SHK DSG, Art. 2 DSG N 12. Bereits in der Botschaft des Bundesrates vom 23. März 1988 zum Bundesgesetz über den Datenschutz wurde der Begriff der juristischen Personen im oben dargelegten erweiterten Sinn verstanden (BBl **1988** II 413, 438).

[54] Art. 57*r* nRVOG ändert nichts an den bestehenden straf-, verwaltungs- und verfahrensrechtlichen Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen, sondern kann nur insoweit Anwendung finden, als solche Daten von den Bundesorganen überhaupt beschafft werden dürfen.

Ob die Bearbeitung von Daten juristischer Personen auf Art. 57*r* nRVOG gestützt werden kann oder ob eine spezialgesetzliche Regelung erforderlich ist, muss in jedem Rechtsetzungsprojekt einzeln geprüft werden. Ein besonderes Augenmerk ist darauf zu halten, dass die gesetzliche Aufgabe, welche die Datenbearbeitung erforderlich macht, genügend klar umschrieben ist. Auch ist zu prüfen, ob allenfalls weitere Modalitäten der Datenbearbeitung (wie Aufbewahrungsfristen oder technische und organisatorische Massnahmen zur Gewährleistung der Datensicherheit) geregelt werden müssen.

3.2.3 Bekanntgabe von Daten juristischer Personen (Art. 57*s* nRVOG)

Für die *Bekanntgabe* von Daten juristischer Personen hält Art. 57*s* Abs. 1 nRVOG fest, dass diese in einer spezialgesetzlichen Grundlage vorgesehen werden muss. Anders als Art. 57*r* nRVOG betreffend die Bearbeitung von Daten juristischer Personen stellt Art. 57*s* nRVOG damit keine Rechtsgrundlage für spezifische Datenbekanntgaben durch Bundesorgane dar. Stattdessen gilt hier das **Prinzip der Spezialermächtigung**.

Analog zu Art. 36 nDSG (Bekanntgabe von Personendaten) regelt Art. 57*s* nRVOG die Frage, gestützt auf welche gesetzlichen Grundlagen ein Bundesorgan Daten juristischer Personen bekanntgeben darf, und legt die Voraussetzungen fest, in welchen Fällen dies ausnahmsweise ohne gesetzliche Grundlage erfolgen kann:

- **Erfordernis der gesetzlichen Grundlage**: Bundesorgane dürfen Daten juristischer Personen grundsätzlich nur bekanntgeben, wenn eine gesetzliche Grundlage dies vorsieht (Art. 57*s* Abs. 1 nRVOG). Die Rechtsgrundlage kann in einem völkerrechtlichen Vertrag, einem Gesetz im formellen Sinn oder in einer Verordnung enthalten sein. Während für die Bekanntgabe von «gewöhnlichen» Daten juristischer Personen in der Regel eine **Verordnungsbestimmung** genügt, ist bei besonders schützenswerten Daten eine **Grundlage in einem Gesetz im formellen Sinn** erforderlich (Art. 57*s* Abs. 2 nDSG). Anders als Art. 36 Abs. 1 i.V.m. Art. 34 Abs. 3 nDSG sieht Art. 57*s* nRVOG nicht ausdrücklich vor, dass die Bekanntgabe von besonders schützenswerten Daten juristischer Personen auf eine Verordnungsbestimmung gestützt werden kann, wenn die Datenbekanntgabe für eine formell-gesetzliche Aufgabe unentbehrlich ist und der Bearbeitungszweck für die Grundrechte der betroffenen Person keine besonderen Risiken birgt. Diese Lücke kann allerdings per Analogieschluss gefüllt werden. Denn das nRVOG will beim Umgang mit Daten juristischer Personen grosszügiger (und nicht strenger) sein als das nDSG.

- **Ausnahmen vom Erfordernis der gesetzlichen Grundlage**: Art. 57*s* Abs. 3 nRVOG zählt abschliessend auf, in welchen Fällen eine Bekanntgabe von «gewöhnlichen» oder von besonders schützenswerten Daten juristischer Personen im Einzelfall *ohne Rechtsgrundlage* zulässig ist. Dabei handelt es sich um dieselben Ausnahmen wie in Art. 36 Abs. 2 Bst. a, b und e nDSG betreffend die Bekanntgabe von Personendaten (► Ziff. 2.1).

- **«Spezialfälle»**: Art. 57*s* Abs. 4 und 5 nRVOG enthält dieselbe Sonderregelung betreffend die Bekanntgabe von Daten juristischer Personen im Rahmen der behördlichen Information der Öffentlichkeit wie Art. 36 Abs. 3 und 5 nDSG (► Ziff. 2.1).

3.2.4 Rechte juristischer Personen (Art. 57*t* nRVOG)

Die Aufhebung des Schutzes von Daten juristischer Personen im nDSG führt dazu, dass sich die juristischen Personen nicht mehr auf die besonderen datenschutzrechtlichen Ansprüche berufen können. Dies betrifft insbesondere das Auskunftsrecht nach Art. 25 f. nDSG. Art. *57t* nRVOG verweist deshalb auf das anwendbare Verfahrensrecht. So können juristische Personen in einem erstinstanzlichen Verwaltungsverfahren nach Art. 26 ff. VwVG die Akten einse-

hen, ihren Anspruch auf rechtliches Gehör nach Art. 29 ff. VwVG geltend machen und gegebenenfalls gegen die Verfügung des zuständigen Bundesorgans Beschwerde erheben. Die juristischen Personen können auch Art. 25*a* VwVG geltend machen. Nach dieser Bestimmung kann jede Person, die ein schutzwürdiges Interesse hat, vom Bundesorgan, das für Handlungen zuständig ist, welche sich auf das öffentliche Recht des Bundes stützen und Rechte oder Pflichten berühren, verlangen, dass es eine beschwerdefähige Verfügung erlässt. Auf diese Weise können juristische Personen z.B. ein Recht auf Berichtigung bzw. Vernichtung ihrer Daten erlangen. Schliesslich steht den juristischen Personen die Möglichkeit offen, gestützt auf das Öffentlichkeitsgesetz (BGÖ) Einsicht in amtliche Dokumente zu beantragen. Dabei ist allerdings zu berücksichtigen, dass im BGÖ der Grundsatz des gleichen Zugangs für jede Person gilt («acces to one, access to all»). Den juristischen Personen müssen deshalb sämtliche Ausnahmebestimmungen des BGÖ (Art. 7 – 9 BGÖ) entgegengehalten werden, auch wenn es sich um amtliche Dokumente handelt, die ihre eigenen Daten beinhalten.

3.3 Übergangsbestimmung betreffend Daten juristischer Personen (Art. 71 nDSG)

Die vorangehend dargestellte Neureglung des Schutzes der Daten juristischer Personen führt dazu, dass zahlreiche spezialgesetzliche Rechtsgrundlagen geändert werden müssen. Diese Änderungen konnten im Rahmen der Totalrevision des DSG noch nicht bzw. nur sehr punktuell[55] durchgeführt werden. Stattdessen sollen nach dem Inkrafttreten des neuen Datenschutzrechts sämtliche spezialgesetzlichen Bestimmungen in einem vom BJ koordinierten Projekt überprüft und möglichst einheitlich an die neuen Vorgaben der Art. 57*r* ff. nRVOG angepasst werden.

Damit in der Zwischenzeit keine Rechtslücken entstehen, wird für Bundesorgane in Art. 71 nDSG eine Übergangsbestimmung eingeführt. Diese Bestimmung sieht vor, dass die bisherigen spezialrechtlichen Datenschutzbestimmungen[56] – die sowohl in Gesetzen im formellen als auch im materiellen Sinn enthalten sein können – während fünf Jahren nach Inkrafttreten des nDSG für die Daten juristischer Personen weiter gelten. Insbesondere sollen sich die Bundesorgane während dieser Zeit für die Bekanntgabe von Daten juristischer Personen auf die bisherigen Rechtsgrundlagen zur Bekanntgabe von Personendaten stützen können. Art. 71 nDSG gilt auch für spezialrechtliche Datenschutzbestimmungen, die erst nach der Verabschiedung oder dem Inkrafttreten des nDSG in Kraft treten.

Die Anwendung der Übergangsbestimmung von Art. 71 nDSG ist nicht zwingend: Will eine Verwaltungseinheit den Umgang mit den Daten juristischer Personen schon während der fünfjährigen Übergangsfrist ausdrücklich regeln, so ist dies natürlich möglich.

---

[55] Im Anhang 1/II zum nDSG wurden einzelne Bundesgesetze aus Gründen der Rechtssicherheit und Praktikabilität betreffend den Umgang mit Daten juristischer Personen bereits überprüft und angepasst. Dies gilt u.a. für das RVOG, das BGÖ, das Bundesstatistikgesetz sowie das Revisionsaufsichtsgesetz. Eine ausführliche Übersicht findet sich in der Botschaft des Bundesrates vom 15. September 2017 ► BBl **2017** 6941, 7107 f. Diese Anpassungen sind auch bei der Revision des Verordnungsrechts zu berücksichtigen.

[56] E contrario ist das Übergangsregime des Art. 71 nDSG nicht für die Bestimmungen des nDSG anwendbar.

4 Weitere Neuerungen der Totalrevision des DSG

4.1 Akteure der Datenbearbeitung: Verantwortlicher und Auftragsbearbeiter

Die Datenschutzgesetzgebung kennt verschiedene Akteure, deren datenschutzrechtlichen Rollen mit unterschiedlichen Rechten und Pflichten verbunden sind. In Angleichung an das europäische Datenschutzrecht (siehe Art. 2 Bst. d und f der Datenschutz-Konvention 108+ des Europarates; Art. 3 Ziff. 8 und 9 der EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen sowie Art. 4 Ziff. 8 und 9 der EU-Datenschutz-Grundverordnung 2016/679) baut das nDSG inskünftig hauptsächlich auf den Begriffen des «Verantwortlichen» und des «Auftragsbearbeiters» auf. Der bisherige «Inhaber der Datensammlung» (Art. 3 Bst. i DSG) wird abgeschafft. Seine Rolle wird jedoch weitgehend im Begriff des «Verantwortlichen» übernommen. Soweit bisher ersichtlich, führen die neuen Rollenumschreibungen kaum zu materiellen Änderungen.

In den spezialrechtlichen Datenschutzbestimmungen sind die verschiedenen an der Datenbearbeitung beteiligten Akteure zu klären. Die Bestimmungen müssen angeben, welche Stelle für eine Datenbearbeitung verantwortlich ist. Ausserdem müssen allfällige weitere an der Datenbearbeitung Beteiligte und ihre Rollen für die betroffenen Personen erkennbar sein. Dabei ist immer nur auf das *datenschutzrechtliche Verhältnis* abzustellen. Dieses kann sich vom «Aussenverhältnis» unterscheiden. So ist zum Beispiel bei einem obligationenrechtlichen Auftrag der Auftraggeber nicht zwingend auch der verantwortliche Datenbearbeiter und der Auftragnehmer nicht unbedingt der Auftragsbearbeiter.

- **Verantwortlicher** (Art. 5 Bst. j nDSG): Als Verantwortlicher gilt, wer allein oder zusammen mit anderen über den Zweck und die Mittel der Datenbearbeitung entscheidet. Beim Entscheid über die Mittel der Datenbearbeitung geht es um die Festlegung der wesentlichen Parameter der Datenbearbeitung. Damit sind weniger die technischen und organisatorischen Mittel, sondern vielmehr diejenigen Faktoren gemeint, die für die datenschutzrechtliche Zulässigkeit oder die datenschutzrechtlichen Risiken relevant sind (z.B. welche Daten werden aus welchen Quellen wie lange und auf welche Weise bearbeitet).[57] Der Verantwortliche muss sicherstellen, dass die datenschutzrechtlichen Vorgaben eingehalten werden. Ausserdem liegt es am Verantwortlichen, die Rechte der betroffenen Personen, insbesondere deren Auskunftsrecht (Art. 25 f. nDSG), zu wahren.

- **Auftragsbearbeiter** (Art. 5 Bst. h nDSG): Bearbeitet jemand im Auftrag des Verantwortlichen Personendaten, so gilt er – wie bisher – als Auftragsbearbeiter. Die Auftragsbearbeitung kann beispielswiese im Rahmen der Nutzung eines Cloud-Dienstes erfolgen. Werden die Daten dabei gleichzeitig ins Ausland bekanntgegeben, so müssen kumulativ auch die Vorgaben von Art. 16 ff. nDSG eingehalten werden. Der Auftragsbearbeiter führt die Datenbearbeitung im Wesentlichen nach den Weisungen des Verantwortlichen aus. Auch Bundesorgane können die Bearbeitung von Personendaten vertraglich oder durch die Gesetzgebung auf einen Auftragsbearbeiter übertragen (Art. 9 Abs. 1 nDSG). Dies entbindet sie aber nicht von der Pflicht, die datenschutzrechtliche Verantwortung wahrzunehmen. Sie müssen – mittels sorgfältiger Auswahl, Instruktion und Kontrolle – aktiv sicherstellen, dass der Auftragsbearbeiter die datenschutzrechtlichen Vorgaben (insbesondere die Datensicherheit) so einhält, wie sie selbst es tun müssten. Durch die Auslagerung der Datenbearbeitung darf sich die Rechtsposition der betroffenen Personen nicht verschlechtern.

  Sind die Voraussetzungen einer Auftragsbearbeitung erfüllt, so wird der Auftragsbearbeiter dem Verantwortlichen datenschutzrechtlich zugerechnet. Der Auftragsbearbeiter ist in die-

[57] DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter vom 17. Juni 2019, Rz. 33.

sem Fall kein Dritter mehr (siehe unten). Die Voraussetzungen für eine Auftragsbearbeitung haben sich im totalrevidierten DSG grundsätzlich nicht geändert (vgl. dazu Art. 9 nDSG). Neu ist die Regelung von Art. 9 Abs. 3 nDSG, wonach die «Unterauftragsbearbeitung» (d.h. der Beizug weiterer Auftragsbearbeiter durch den Auftragsbearbeiter) nur mit vorgängiger Genehmigung des Verantwortlichen zulässig ist. Diese vorgängige Genehmigung kann spezifischer oder allgemeiner Art sein (Art. 7 Abs. 1 und 2 DSV).

- **Gemeinsame Datenbearbeitung** (Art. 33 nDSG): Werden Personendaten von mehreren Bundesorganen oder mit kantonalen Organen oder Privaten bearbeitet, können sich schwierige Abgrenzungsfragen zur Verantwortlichkeit stellen.[58] Um dies zu vermeiden, schreibt Art. 33 nDSG vor, dass der Bundesrat die Verantwortung und Kontrollverfahren regelt. Diese Bestimmung entspricht grösstenteils dem heutigen Art. 16 Abs. 2 DSG. Anders als heute wird der Bundesrat aber verpflichtet und nicht bloss ermächtigt, besondere Regeln über die Kontrolle und Verantwortung für den Datenschutz vorzusehen. Dabei sind auch Fragen wie die Zugriffsrechte auf die Daten, die Datensicherheit und die Umsetzung der Rechte der von der Datenbearbeitung betroffenen Personen zu klären.

- **Dritter**: Der Begriff des Dritten wird im nDSG nicht ausdrücklich definiert. In Anlehnung an die EU-Datenschutz-Grundverordnung 2016/679 (Art. 4 Ziff. 10) handelt es sich beim Dritten um eine private Person, ein Bundesorgan oder ein kantonales Organ, welche bzw. welches weder Verantwortlicher noch Auftragsbearbeiter ist. Anders als im geltenden Art. 10*a* DSG wird der Auftragsbearbeiter im nDSG deshalb nicht mehr als Dritter bezeichnet. Denn ab dem Zeitpunkt, an welchem ein Auftragsbearbeiter seine Tätigkeit für den Verantwortlichen beginnt, ist er kein Dritter mehr (► BBl **2017** 6941, 7023).

- **Empfänger**: Als Empfänger gilt eine private Person, ein Bundesorgan oder ein kantonales Organ, welcher bzw. welchem Personendaten bekanntgegeben werden, unabhängig davon, ob es sich dabei um einen Dritten handelt oder nicht (vgl. Art. 2 Bst. d der Datenschutz-Konvention 108+ des Europarates sowie Art. 3 Ziff. 10 der EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen und Art. 4 Ziff. 9 der EU-Datenschutz-Grundverordnung 2016/679 [beide mit Ausnahmen für Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags Personendaten erhalten]). Auch Auftragsbearbeiter (oder Mitverantwortliche) gelten deshalb als Empfänger.

4.2 Datenbekanntgabe ins Ausland

Wie im geltenden Recht (Art. 6 DSG) sind auch im nDSG besondere Anforderungen für die Bekanntgabe von Personendaten ins Ausland vorgesehen (Art. 16 f. nDSG). Allerdings erfährt die grenzüberschreitende Datenbekanntgabe mit der Totalrevision des DSG einige systematische und inhaltliche Änderungen:

- **Angemessenes Datenschutzniveau**: Gemäss Art. 16 Abs. 1 nDSG dürfen Personendaten grundsätzlich nur dann ins Ausland bekanntgegeben werden, wenn die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Datenschutz gewährleistet. *Neu* obliegt es dem Bundesrat, verbindlich festzustellen, welche Länder oder internationalen Organe über ein solches Schutzniveau verfügen. Die Kriterien, nach wel-

[58] Vgl. zu diesen Abgrenzungsfragen im EU-Datenschutzrecht die «Guidelines 07/2020 on the concepts of controller and processor in the GDPR» des Europäischen Datenschutzausschusses.

chen der Bundesrat die ausländische Gesetzgebung zu prüfen hat, werden im Verordnungsrecht (Art. 8 DSV) präzisiert. Die Staaten mit einem angemessenen Datenschutzniveau werden im Anhang 1 zur DSV aufgelistet.

- **Geeignete Garantien zur Gewährleistung des Datenschutzes**: In einen Staat, welcher nicht in der Liste des Bundesrates enthalten ist, können Personendaten nach Art. 16 Abs. 2 nDSG dann bekanntgegeben werden, wenn ein geeigneter Datenschutz[59] mit anderen Instrumenten sichergestellt wird. Dazu gehören: völkerrechtliche Verträge (Bst. a), vertragliche Datenschutzklauseln (Bst. b), spezifische Garantien bei Bundesorganen (Bst. c), Standarddatenschutzklauseln (Bst. d) und verbindliche unternehmensinterne Datenschutzvorschriften («Binding Corporate Rules»; Bst. e). Die Mindestinhalte dieser Garantien werden im Verordnungsrecht konkretisiert (Art. 9 – 11 DSV). Ausserdem werden in der DSV noch zwei weitere Garantien vorgesehen: Verhaltenskodizes und Zertifizierungen (Art. 12 DSV und Art. 16 Abs. 3 nDSG). Bei verschiedenen dieser Garantien besteht eine Pflicht zur vorgängigen Mitteilung an den EDÖB (Art. 16 Abs. 2 Bst. b und c nDSG) oder zur Genehmigung durch den EDÖB (Art. 16 Abs. 2 Bst. d und e nDSG sowie Art. 12 Abs. 2 DSV). Die geeigneten Garantien des Art. 16 Abs. 2 nDSG entsprechen zu einem grossen Teil dem geltenden Recht (Art. 6 Abs. 2 Bst. a und g sowie Abs. 3 DSG). Sie erfahren aber einige inhaltliche Änderungen. Zu den Neuerungen wird insbesondere auf die bundesrätliche Botschaft vom 15. September 2017 verwiesen (► BBl **2017** 6941, 7039 ff.).

  Vor diesem Hintergrund ist namentlich beim **Abschluss von Staatsverträgen** ein besonderes Augenmerk darauf zu legen, dass im Ausland ein ausreichendes Schutzniveau gewährleistet wird. Zentral sind dabei die Einhaltung der datenschutzrechtlichen Grundsätze, die Rechte der betroffenen Personen (wie das Auskunfts-, Widerspruchs-, Löschungs- und Berichtigungsrecht mit entsprechenden Rechtsschutzmöglichkeiten), die Anforderungen an eine allfällige weitere Datenbekanntgabe ins Ausland sowie die unabhängige Datenschutzaufsicht.

- **Ausnahmen** (Art. 17 nDSG): Wie im geltenden Recht (Art. 6 Abs. 2 Bst. b – f DSG) sind auch in Art. 17 nDSG verschiedene Ausnahmefälle angeführt, in welchen Daten ins Ausland bekanntgegeben werden können, obwohl ein angemessener Datenschutz gemäss Art. 16 Abs. 1 nDSG fehlt und keine geeigneten Schutzgarantien nach Art. 16 Abs. 2 und 3 nDSG getroffen werden. Die Ausnahmen in Art. 17 Abs. 1 Bst. a-e nDSG wurden aus dem geltenden Recht übernommen und erfahren nur geringe Anpassungen, die in der Botschaft des Bundesrates vom 15. September 2017 erläutert werden (► BBl **2017** 6941, 7042 f.). Art. 17 Abs. 1 Bst. f nDSG hingegen ist neu. Die Bestimmung ermöglicht die Bekanntgabe von Personendaten bei Fehlen eines angemessenen Datenschutzes für den Fall, dass die Daten aus einem gesetzlich geregelten öffentlichen Register stammen und die dort aufgeführten Voraussetzungen erfüllt sind.

[59] Im Urteil vom 16. Juli 2020 betreffend die Rechtssache C-311/18 («Schrems II») hat der EuGH festgehalten, dass die geeigneten Garantien so beschaffen sein müssen, dass sie ein Schutzniveau gewährleisten, das dem in der EU garantierten Datenschutzniveau der Sache nach gleichwertig (m.a.W.: angemessen) ist (Rz. 96).

4.3 Datenschutz-Folgenabschätzung

Mit der **Datenschutz-Folgenabschätzung** sollen die verantwortlichen Datenbearbeiter (Bundesorgane und Private) Risiken frühzeitig erkennen und, falls nötig, angemessene Schutzmassnahmen treffen. 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 nDSG). Als hohes Risiko nennt das nDSG zum Beispiel die umfangreiche Bearbeitung von besonders schützenswerten Personendaten (Art. 22 Abs. 2 nDSG). In der Datenschutz-Folgenabschätzung müssen die geplante Datenbearbeitung, deren Risiken für die Persönlichkeit oder die Grundrechte sowie die bereits getroffenen oder noch zu treffenden Schutzmassnahmen beschrieben werden (Art. 22 Abs. 3 nDSG). Bleibt trotz der getroffenen oder geplanten Massnahmen ein hohes «Restrisiko» für die Persönlichkeit oder die Grundrechte der betroffenen Person bestehen, muss der **EDÖB konsultiert** werden (Art. 23 Abs. 1 nDSG). Der EDÖB teilt seine allfälligen Einwände gegen die geplante Datenbearbeitung mit und kann selber geeignete Schutzmassnahmen vorschlagen. Für die Bundesorgane dürfte die Datenschutz-Folgenabschätzung nur teilweise eine Neuerung sein. Bereits heute müssen sie gestützt auf Art. 20 Abs. 2 VDSG der Datenschutzberaterin bzw. dem Datenschutzberater oder dem EDÖB alle Projekte zur automatisierten Bearbeitung von Personendaten melden, damit die Erfordernisse des Datenschutzes berücksichtigt werden können. Für Bundesorgane sind die Vorgaben im Zusammenhang mit der Erstellung einer Datenschutz-Folgenabschätzung mit den bestehenden Prozessen, namentlich der der Projektmanagementmethode Hermes zu koordinieren.

Es ist geplant, die Datenschutz-Folgenabschätzung inskünftig **mit dem Rechtsetzungsverfahren zu koordinieren**: Erfordert die Datenbearbeitung eines Bundesorgans den Erlass oder die Änderung einer gesetzlichen Grundlage und sind die Voraussetzungen für eine Datenschutz-Folgenabschätzung erfüllt, soll letztere zusammen mit dem Erlassentwurf (und ggf. der Stellungnahme des EDÖB) dem Antrag an den Bundesrat beigefügt werden. Die Resultate der Datenschutz-Folgenabschätzung (und eine allfällige Stellungnahme des EDÖB) sollen ausserdem in der Botschaft des Bundesrates veröffentlicht werden.

4.4 Terminologische Anpassungen

4.4.1 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Für die Bezeichnung «Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter» werden mit der Totalrevision des DSG neue Abkürzungen eingeführt, die auch in den spezialgesetzlichen Datenschutzbestimmungen zu verwenden sind:

- Die **Behörde** des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten wird mit «EDÖB» abgekürzt (siehe Art. 4 Abs. 1 nDSG)
- Ist dagegen die **natürliche Person** gemeint, d.h. die «Leiterin oder der Leiter des EDÖB» werden geschlechtsneutral die weibliche und männliche Form «die oder der Beauftragte» verwendet (siehe Art. 43 Abs. 1 nDSG).

Beispiel: Änderung des Parlamentsgesetzes in Ziff. 12 des Anhangs 1/II zum nDSG (nParlG)

Art. 40*a* Abs. 1 Bst. d nParlG: «Die Gerichtskommission ist zuständig für die Vorbereitung der Wahl und Amtsenthebung: *der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragte oder Beauftragter)*».

Art. 142 Abs. 2 nParlG: «Er [Der Bundesrat] nimmt die Entwürfe für den Voranschlag sowie die Rechnungen der Bundesversammlung, der eidgenössischen Gerichte, der Eidgenössischen Finanzkontrolle, der Bundesanwaltschaft, der Aufsichtsbehörde über die Bundesanwaltschaft und *des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)* unverändert in seinen Entwurf für den Voranschlag und in die Rechnung des Bundes auf».

4.4.2 Inhaber der Datensammlung / Datensammlung

- Der Begriff des «**Inhabers der Datensammlung**» wird durch «**Verantwortlicher**» ersetzt: vgl. dazu Ziff. 4.1.

- Ausserdem wird im nDSG auf den Begriff der «**Datensammlung**» verzichtet. Das heutige DSG, welches verschiedene Rechte und Pflichten an die Voraussetzung knüpft, dass eine Datensammlung vorliegt (z.B. das Auskunftsrecht nach Art. 8 DSG), definiert den Begriff in Art. 3 Bst. g als «Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind». Diese Umschreibung stammt aus einer Zeit, als Datensammlungen noch vorwiegend Karteikärtchensysteme und Ordnerablagen waren. Angesichts der heutigen technologischen (Such-)Möglichkeiten ist davon auszugehen, dass praktisch jede elektronische Ablage eine Datensammlung im Sinne des DSG darstellt. Der Begriff ist folglich überholt. Inskünftig wird die datenschutzrechtliche Verantwortung deshalb an die Tatsache der Bearbeitung von Personendaten angeknüpft. Im Anhang 1/II zum nDSG wurde der Begriff der «Datensammlung» in den bereichsspezifischen Datenschutzbestimmungen systematisch aufgehoben und durch einen zum jeweiligen Kontext passenden Ausdruck ersetzt.

  Beispiele: Personendaten (...) bearbeiten, Datenbearbeitung(stätigkeiten), Datenbank, elektronische Infrastruktur, Informationssystem, Datenbeschaffung.

  Es ist darauf zu achten, dass der Begriff der Datensammlung auch in neuen oder zu revidierenden Datenschutzbestimmungen möglichst nicht mehr verwendet wird.

4.4.3 Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen

Die Modernisierung der Terminologie in Art. 5 Bst. c Ziff. 5 nDSG (Definition der besonders schützenswerten Personendaten) betrifft nur die deutsche Fassung. Statt «Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen» (Art. 3 Bst. c Ziff. 4 DSG) heisst es neu «Daten über *verwaltungs-* und strafrechtliche Verfolgungen oder Sanktionen». Diese Anpassung ist auch in den spezialgesetzlichen Datenschutzbestimmungen zu berücksichtigen.

Beispiele: Art. 65 Abs. 2, Art. 101 Abs. 1 und Art. 110 des revidierten Geldspielgesetzes (Ziff. 90 des Anhangs 1/II zum nDSG).

4.5 Übersicht zu den weiteren Inhalten der Totalrevision des DSG

Neben den vorangehend dargestellten Änderungen, welche für Rechtsetzungsprojekte der Bundesverwaltung besonders relevant sind, bringt die Totalrevision des DSG zahlreiche weitere Neuerungen für den Datenschutz mit sich (summarische, nicht abschliessende Übersicht):

- **Geltungsbereich des nDSG**:
  - *Sachlicher Geltungsbereich*:
    - Mit der Totalrevision des DSG wird die **Bearbeitung von Daten juristischer Personen** vom sachlichen Anwendungsbereich des Datenschutzgesetzes ausgenommen: ► Ziff. 3.
    - Für (hängige) Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren wird keine Ausnahme vom Geltungsbereich des Datenschutzgesetzes mehr vorgesehen. Stattdessen regelt Art. 2 Abs. 3 nDSG das **Verhältnis zwischen Verfahrensrecht und Datenschutzgesetz**: Die Bearbeitung von Personendaten und die Rechte der betroffenen Personen in Gerichtsverfahren und in Verfahren nach bundesrechtlichen Verfahrensordnungen wird durch das jeweils anwendbare Verfahrensrecht geregelt. Auf erstinstanzliche Verwaltungsverfahren sind die Bestimmungen des nDSG anwendbar (wie dies heute auch für das DSG gilt). Vgl. dazu die Erläuterungen in der Botschaft des Bundesrates vom 15. September 2017: ► BBl **2017** 6941, 7013 ff. Zu den Ausnahmen von der Aufsicht des EDÖB vgl. Art. 4 Abs. 2 Bst. c – e nDSG.
    - Auch für die **öffentlichen Register des Privatrechtverkehrs** enthält das nDSG keine Ausnahme vom Geltungsbereich mehr. Art. 2 Abs. 4 nDSG sieht aber vor, dass diese Register (insbesondere der Zugang zu den Registern und die Rechte der betroffenen Personen) durch die Spezialbestimmungen des anwendbaren Bundesrechts geregelt werden. Enthalten die Spezialbestimmungen keine Regelung, so ist das nDSG anwendbar. Vgl. dazu die Erläuterungen in der Botschaft des Bundesrates vom 15. September 2017: ► BBl **2017** 6941, 7015 f. Öffentliche Register des Privatrechtverkehrs, die von Bundesbehörden geführt werden, unterstehen neu der Aufsicht des EDÖB (Art. 4 Abs. 1 nDSG).
  - *Räumlicher Geltungsbereich*: Das Parlament hat in Art. 3 nDSG neu eine ausdrückliche Regelung zum **räumlichen Geltungsbereich** des Datenschutzgesetzes aufgenommen: Diese Bestimmung bringt aber voraussichtlich keine materiellen Änderungen. Für die *privatrechtlichen* und *strafrechtlichen Datenschutzbestimmungen* verweist Art. 3 Abs. 2 nDSG deklaratorisch auf die schon heute vorhandenen Kollisionsnormen im Bundesgesetz über das Internationale Privatrecht (Art. 139 IPRG) und im Strafgesetzbuch (Art. 3 ff. StGB). Für die *öffentlich-rechtlichen Datenschutzbestimmungen* (einschliesslich der Aufsicht durch den EDÖB) hält Art. 3 Abs. 1 nDSG 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, sondern lediglich eine Kodifizierung der Gerichtspraxis zum Territorialitäts- und Auswirkungsprinzip im öffentlichen Recht.[60]
  - *Persönlicher Geltungsbereich*: Keine Änderung.

    Wie bisher gilt das nDSG für die Bearbeitung von Personendaten durch *private Personen* und *Bundesorgane* (Art. 2 Abs. 1 Bst. a und b nDSG). Bundesorgane sind Behörden oder Dienststellen des Bundes oder Personen, die mit öffentlichen Aufgaben des Bundes betraut sind (Art. 5 Bst. i nDSG). Die Datenbearbeitung

[60] Vgl. für das Datenschutzrecht BGE **138** II 346 i.S. «Google Street View».

durch *kantonale oder kommunale Behörden* untersteht dem kantonalen Datenschutzrecht, unabhängig davon, ob die Behörden diese Daten direkt beschafft oder über einen Online-Zugriff auf eine Datenbank des Bundes abgerufen haben. Die Bearbeitung von Daten durch kantonale Organe beim Vollzug von Bundesrecht untersteht grundsätzlich ebenfalls dem kantonalen Recht.[61] In einigen Bereichen, für die der Bund zuständig ist, besteht eine besondere Datenschutzregelung, die – zum Beispiel im Bereich der Sozialversicherungen – sowohl für die zuständigen Bundesbehörden wie auch für die mit dem Vollzug des Bundesrechts beauftragten kantonalen Behörden gilt. Allerdings hat der Bund dabei auf das kantonale Organisationsrecht Rücksicht zu nehmen.[62]

- **Verzeichnis der Bearbeitungstätigkeiten statt Datensammlungen**: Zukünftig müssen private Datenbearbeiter und Bundesorgane ein Verzeichnis ihrer Bearbeitungstätigkeiten erstellen. Bundesorgane müssen diese Verzeichnisse ausserdem an den EDÖB melden (Art. 12 Abs. 1 und 4 nDSG). Der EDÖB führt dazu ein öffentliches Register (Art. 56 nDSG).

  Das Verzeichnis der Bearbeitungstätigkeiten ersetzt die bisherige Anmeldung von Datensammlungen beim EDÖB (Art. 11*a* DSG). Der Mindestinhalt des Verzeichnisses wird in Art. 12 Abs. 2 (Verantwortlicher) und Abs. 3 nDSG (Auftragsbearbeiter) festgelegt. Dabei gehen die Angaben, die im Bearbeitungsverzeichnis des Verantwortlichen enthalten sein müssen, etwas weiter als heute bei der Anmeldung von Datensammlungen. So müssen nicht nur der Bearbeitungszweck, die Kategorien der bearbeiteten Personendaten und der Datenempfänger, sondern – wenn möglich – auch Angaben zur Aufbewahrungsdauer, zur Gewährleistung der Datensicherheit und zu allfälligen Schutzgarantien bei der Datenbekanntgabe ins Ausland enthalten sein.

  Anders als für die die privaten Datenbearbeiter (Art. 12 Abs. 5 nDSG und Art. 24 DSV) sieht das nDSG für Bundesorgane keine Ausnahmen von der Verzeichnispflicht vor. Soll ein Bundesorgan von der Führung eines Bearbeitungsverzeichnisses oder von der Pflicht zur Meldung des Verzeichnisses an den EDÖB ausgenommen werden, muss dies im jeweiligen Spezialgesetz geregelt werden.

  Beispiele: Art. 11 Abs. 2 des Geoinformationsgesetzes (Ziff. 41 des Anhangs 1/II zum nDSG) sowie Art. 99 Abs. 3 Bst. d und Art. 100 Abs. 4 Bst. c Ziff. 2 des Militärgesetzes (Ziff. 40 des Anhangs 1/II zum nDSG).

- **Erweiterung der Pflichten der Verantwortlichen**:

  – *Informationspflicht bei der Beschaffung von Personendaten*: Die Informationspflicht wird mit der Totalrevision des DSG auf die Beschaffung *aller Arten von Personendaten* ausgedehnt (Art. 19 Abs. 1 nDSG). Für Bundesorgane ist dies nichts Neues (Art. 18*a* DSG). Die Änderung betrifft vor allem private Datenbearbeiter, die heute nur über die Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen informieren müssen. Wie bisher gilt die Informationspflicht auch dann, wenn die Daten nicht bei der betroffenen Person, sondern bei Dritten beschafft werden. Gemäss Art. 19 Abs. 2 Einleitungssatz nDSG müssen der betroffenen Person grundsätzlich all diejenigen Informationen mitgeteilt werden, die erforderlich sind, damit sie ihre Rechte nach dem nDSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Art. 19 Abs. 2 Bst. a – c, Abs. 3 und 4 nDSG konkretisieren diesen Grundsatz sodann durch verschiedene Mindestangaben. Mit diesem Konzept lässt sich die Informationspflicht flexibel und risikobasiert handhaben. *Ausnahmen und Einschränkungen zur Informationspflicht* sind in Art. 20 nDSG vorgesehen. Für

[61] Der bisherige Art. 37 Abs. 1 DSG, wonach für das Bearbeiten von Personendaten durch kantonale Organe beim Vollzug von Bundesrecht die Artikel 1 – 11*a*, 16, 17, 18 – 22 und 25 Absätze 1 – 3 DSG gelten, soweit keine kantonalen Datenschutzvorschriften bestehen, die einen angemessenen Schutz gewährleisten, wird mit der Totalrevision des DSG aufgehoben.

[62] Vgl. den Bericht des Bundesrates in Erfüllung des Postulates Lustenberger 07.3682 «Austausch personenbezogener Daten zwischen Behörden des Bundes und der Kantone» vom 22. Dezember 2010 (BBl **2011** 645, 653 f.).

Bundesorgane ist insbesondere Art. 20 Abs. 1 Bst. b nDSG von Bedeutung. Danach entfällt die Informationspflicht für eine Datenbearbeitung, die gesetzlich vorgesehen ist. Es ist deshalb zentral, dass die Eckwerte der Datenbearbeitung für die betroffene Person aus der gesetzlichen Grundlage erkennbar sind (► Ziff. 2).

- *Datenschutz-Folgenabschätzung:* ► Ziff. 4.3.

- *Pflicht zur Meldung von Verletzungen der Datensicherheit*: Art. 24 Abs. 1 nDSG sieht neu vor, dass Verletzungen der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, so rasch als möglich dem EDÖB gemeldet werden müssen. Unter gewissen Umständen sind auch die betroffenen Personen direkt zu informieren (Art. 24 Abs. 4 nDSG). Was eine Verletzung der Datensicherheit ist, wird in Art. 5 Bst. h nDSG definiert: «eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder geändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden».

- *Besondere Pflichten bei automatisierten Einzelentscheidungen*: ► Ziff. 2.2.1 Bst. c).

- **Rechte der betroffenen Personen**:

  - *Auskunftsrecht*: Das Auskunftsrecht in Art. 25 ff. nDSG entspricht weitgehend den heutigen Art. 8 ff. DSG. Allerdings wird der *Katalog der zu erteilenden Auskünfte* in Art. 25 Abs. 2 nDSG erweitert. Inskünftig muss insbesondere auch über die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, über die Kriterien zur Festlegung dieser Dauer (Bst. d) sowie über das allfällige Vorliegen einer automatisierten Einzelentscheidung (► Ziff. 2.2.1 Bst. c)/cc) und die Logik, auf der die Entscheidung beruht (Bst. f), Auskunft erteilt werden. Neu ist ausserdem die *Ausnahme vom Auskunftsrecht* in Art. 26 Abs. 1 Bst. c nDSG. Danach kann das Auskunftsrecht verweigert, eingeschränkt oder aufgeschoben werden, wenn es offensichtlich unbegründet ist, namentlich wenn es einen *datenschutzwidrigen Zweck* verfolgt, oder offensichtlich querulatorisch ist. Ein datenschutzwidriger Zweck liegt nach der Rechtsprechung des Bundesgerichts beispielsweise vor, wenn es dazu eingesetzt wird, um eine mögliche Gegenpartei auszuforschen oder sich die Kosten einer Beweisbeschaffung zu sparen.[63]

  - *Datenportabilität*: Das Parlament hat in den Art. 28 f. nDSG ein Recht auf Datenherausgabe oder -übertragung (sog. Datenportabilität) eingeführt. Gemäss Art. 28 Abs. 1 kann die betroffene Person vom verantwortlichen Datenbearbeiter die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format verlangen. Wenn es keinen unverhältnismässigen Aufwand erfordert kann die betroffene Person ausserdem verlangen, dass der Verantwortliche ihre Personendaten einem anderen Verantwortlichen überträgt. Dabei beide Ansprüche nur dann bestehen, wenn es um Daten geht, die 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 werden, dürfte das Recht auf Datenportabilität vor allem im privatrechtlichen Bereich Anwendung finden. Einschränkungen des Rechts auf Datenherausgabe oder -übertragung sind in Art. 29 nDSG geregelt.

  - *Weitere Rechtsansprüche* sind in Art. 37 nDSG (Widerspruch gegen die Bekanntgabe von Personendaten) und Art. 41 nDSG (z.B. Recht auf Löschung oder Vernichtung wi-

[63] Vgl. BGE **138** III 425 E. 5.4 f.

derrechtlich bearbeiteter Personendaten) enthalten. Diese Rechtsansprüche entsprechen weitgehend dem geltenden Recht (Art. 20 und Art. 25 DSG). Neu ist das Recht auf Einschränkung der Datenbearbeitung (At. 41 Abs. 3 nDSG). Vgl. zu den weiteren Änderungen die Botschaft des Bundesrates vom 15. September 2017: ► BBl **2017** 6941, 7084 ff.

- **Datenschutzaufsicht (EDÖB)**:
  - **Wahl der Leiterin oder des Leiters des EDÖB**: Während die Leiterin bzw. der Leiter des EDÖB (► Ziff. 4.4.1) nach dem geltenden Recht vom Bundesrat gewählt wird und diese Wahl durch die Bundesversammlung genehmigt werden muss (Art. 26 Abs. 1 DSG), ist inskünftig die Bundesversammlung das alleinige Wahlorgan (Art. 43 Abs. 1 nDSG). Dies führt zu verschiedenen organisations- und personalrechtlichen Anpassungen, z.B. betreffend das Budget des EDÖB (Art. 45 nDSG). Ausserdem wird die Bundesversammlung eine Verordnung über das Arbeitsverhältnis der Leiterin oder des Leiters des EDÖB erlassen (vgl. dazu die parlamentarische Initiative 21.443 der SPK-N). Der EDÖB bildet aber auch weiterhin eine dezentralisierte Verwaltungseinheit (ohne Rechtspersönlichkeit), welche administrativ der Bundeskanzlei zugeordnet ist (Art. 43 Abs. 4 nDSG; Art. 2 Abs. 3 RVOG sowie Art. 7*a* Abs. 1 Bst. b und Anhang 1 Bst. A Ziff. 2.1.1 der Regierungs- und Verwaltungsorganisationsverordnung).
  - **Untersuchung von Verstössen gegen Datenschutzvorschriften**: Mit der Totalrevision des DSG werden die Aufsichtskompetenzen des EDÖB gestärkt. Inskünftig muss der EDÖB von Amtes wegen oder auf Anzeige hin eine Untersuchung eröffnen, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte (Art. 49 Abs. 1 nDSG). Dies führt insbesondere gegenüber privaten Datenbearbeitern zu mehr Interventionsbefugnissen als heute (vgl. Art. 29 Abs. 1 DSG, welcher für Abklärungen des EDÖB im Privatrechtsbereich unter anderem einen Systemfehler voraussetzt). Allerdings kann der EDÖB von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringer Bedeutung ist (Art. 49 Abs. 2 nDSG). Art. 50 nDSG erweitert die Instrumente des EDÖB zur Sachverhaltsfeststellung für den Fall, dass der Datenbearbeiter (Bundesorgan oder private Person) seinen Mitwirkungspflichten nicht nachkommt. Liegt eine Verletzung der Datenschutzvorschriften vor, so kann der EDÖB nach Art. 51 nDSG inskünftig Verwaltungsmassnahmen **verfügen** (und nicht bloss eine Empfehlung erlassen). Dies gilt sowohl bei privaten Datenbearbeitern als auch bei Bundesorganen. Das Untersuchungsverfahren und die Verfügungen des EDÖB richten sich nach dem VwVG (Art. 52 Abs. 1 nDSG).
  - **Rechtsetzung**: Wie bisher soll der EDÖB auch im Rahmen der Rechtsetzung eine wichtige Rolle spielen. Gemäss Art. 58 Abs. 1 Bst. e nDSG nimmt er Stellung zu Erlassentwürfen und Massnahmen des Bundes, die eine Datenbearbeitung zur Folge haben.
- **Ausbau der Strafbestimmungen**: In den Art. 60 ff nDSG werden die datenschutzrechtlichen Straftatbestände erweitert und die Bussenobergrenze für Verstösse von Fr. 10'000.- auf Fr. 250'000.- erhöht. Besonders hinzuweisen ist auf den neuen Art. 63 nDSG, welcher das vorsätzliche Missachten von Verfügungen des EDÖB unter Strafe stellt und dem EDÖB damit eine Art «indirekte» Sanktionsmöglichkeit einräumt. Ausserdem kann der EDÖB bei der zuständigen Strafverfolgungsbehörde Anzeige erstatten und im Strafprozess die Rechte einer Privatklägerschaft wahrnehmen (Art. 65 Abs. 2 nDSG). Diese Massnahme sind für die Bundesorgane allerdings nicht von Bedeutung, denn die Strafbestimmungen des nDSG richten sich (wie bisher im DSG) nur an die privaten Datenbearbeiter.