Transparenz durch Datenschutzerklärungen von Behörden

Florent Thouvenin*/Nadja Braun Binder**

Schlagwörter: Datenschutzerklärungen, informationelle Selbstbestimmung, Legalitätsprinzip, Transparenz, Informationspflicht

A. Einleitung

Das Datenschutzrecht ist als Reaktion auf das Sammeln und Bearbeiten von Personendaten durch staatliche Behörden entstanden. Das gilt für das schweizerische Datenschutzgesetz (DSG)[1] ebenso wie für das deutsche Bundesdatenschutzgesetz (BDSG),[2] das seinerseits ein zentraler Treiber der Entstehung des europäischen Datenschutzrechts[3] war. Obwohl in der Schweiz schon seit Anfang der 1980er Jahre an einem Datenschutzgesetz gearbeitet wurde, hat erst die sog. «Fichenaffäre» Ende der 1980er Jahre dem Anliegen den entscheidenden politischen Rückenwind verschafft.

Die ersten Datenschutzgesetze regelten allein das Bearbeiten von Personendaten durch Behörden, so namentlich das Hessische Datenschutzgesetz, das als weltweit erstes formelles Datenschutzgesetz 1970 in Kraft getreten ist. Die Anwendung des Datenschutzrechts wurde allerdings schon im deutschen Bundes-

* Professor für Informations- und Kommunikationsrecht an der Universität Zürich, Rechtsanwalt in Zürich. Vorsitzender des Leitungsausschusses des Center for Information Technology, Society, and Law (ITSL) und Direktor der Digital Society Initiative (DSI) der Universität Zürich.

** Professorin für Öffentliches Recht an der Universität Basel. Der Beitrag beruht auf einem Gutachten, das die Autoren verfasst haben. Er nimmt einen Teil der Ausführungen in diesem Gutachten auf, geht aber über dieses hinaus. Der Beitrag gibt einzig die Auffassung der Autoren wieder. Die Autoren danken Manuela Kälin, MA, für die wertvolle Unterstützung bei der Recherche und formalen Aufbereitung des Manuskripts.

1 Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).

2 Bundesdatenschutzgesetz vom 30. Juni 2017, BGBl. I, S. 2097, zuletzt geändert durch Art. 12 des Gesetzes vom 20. 11. 2019, BGBl. I, S. 1626.

3 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO).

datenschutzgesetz von 1977[4] auf Private ausgedehnt, um auch die Bearbeitung von Personendaten durch Unternehmen zu erfassen. Auch das schweizerische Datenschutzgesetz von 1992 erfasst Behörden und Private zugleich. Mit dem Siegeszug der Digitalisierung stand denn auch das Sammeln und Bearbeiten von Personendaten durch Unternehmen lange Zeit im Vordergrund, insbesondere die Tätigkeiten der grossen US-amerikanischen Technologieunternehmen («Big Tech»), deren Macht bis heute wesentlich auf ihren gigantischen Datenbeständen beruht.

Mit den sog. «Snowden Revelations»[5] hat sich die Perspektive allerdings schon vor einigen Jahren wieder zu wenden begonnen. Im Sommer 2013 hat der damalige Mitarbeiter der «Central Intelligence Agency» (CIA), Edward Snowden, öffentlich bekannt gemacht, dass die US-amerikanischen Auslandsgeheimdienste, neben der CIA namentlich auch die National Security Agency (NSA), ein umfassendes Programm zur Überwachung der weltweiten Internetkommunikation betreiben. Seither steht neben «Big Tech» das Sammeln und Analysieren von Personendaten durch staatliche Behörden wieder im Zentrum der Diskussion um den Schutz der Privatsphäre und die Abwehr einer umfassenden Überwachung der Individuen in der Informationsgesellschaft. Die jüngste Eskalationsstufe bildet das Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 («Schrems II»),[6] mit welchem das Gericht den Transfer von Personendaten aus Europa in die USA mit Blick auf den umfassenden Zugriff der US-Behörden als grundsätzlich unzulässig qualifiziert hat.

Auch in der Schweiz liegt der Fokus der (Fach-)Öffentlichkeit wieder vermehrt auf der Bearbeitung von Personendaten durch staatliche Behörden, wie etwa das letztlich nicht zustande gekommene Referendum gegen die Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF),[7] der Entscheid des Bundesgerichts über die sog. «Kabelaufklärung»[8] und die Volksabstimmung über das Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT)[9] zeigen.

---

4 Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung vom 27. Januar 1977, BGBl. I, S. 201.

5 Mit dieser Umschreibung sind die Enthüllungen von Edward Snowden betreffend die Überwachungsaktivitäten der USA gemeint. Siehe dazu z.B. ‹https://www.lawfareblog.com/snowden-revelations› (zuletzt besucht am 16. Dezember 2021).

6 EuGH, Urteil C-311/18 vom 16. Juli 2020.

7 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (BÜPF; SR 780.1). Zum gescheiterten Referendum siehe: BBl 2016 6791.

8 BGer, Urteil 1C_377/2019 vom 1. Dezember 2020; siehe hierzu auch die Medienmitteilung des Bundesgerichts vom 28. Dezember 2020, abrufbar unter ‹https://www.bger.ch/files/live/sites/bger/files/pdf/de/1c_0377_2019_2020_12_28_T_d_10_02_23.pdf› (zuletzt besucht am 16. Dezember 2021).

9 Die Bundesversammlung verabschiedete das PMT am 25. September 2020, siehe BBl 2020 7741; das Gesetz wurde am 13. Juni 2021 in der Volksabstimmung angenommen, BBl 2021 2135.

Dieser Perspektivenwechsel hat gute Gründe. «Big Tech» hat zwar gigantische Datenbestände angelegt und ist in der Lage, aus diesen Daten weitreichende Erkenntnisse zu gewinnen. Die staatlichen Behörden verfügen aber in der Summe nicht nur über vergleichbare Mengen an Daten, sie haben auch Zugriff auf höchst sensible Daten, etwa zu allfälligen Strafverfahren oder zu den familiären und finanziellen Verhältnissen der Bürgerinnen und Bürger. Vor allem aber treffen Behörden gestützt auf diese Daten hoheitliche Entscheidungen, denen sich die Bürgerinnen und Bürger nicht entziehen können. So steht es einer Person beispielsweise frei, einen bestimmten privaten Dienstleister für Angebote wie Mobiltelefonie, E-Mail- oder Social Media-Dienste zu wählen; eine Baubewilligung oder die Sozialhilfeunterstützung sind hingegen nur von der dafür zuständigen staatlichen Stelle zu erhalten. Das Sammeln und Bearbeiten von Daten durch den Staat bedarf deshalb nicht nur einer eingehenden Regelung, sondern auch einer kritischen Überwachung durch Datenschutzbeauftragte, Medien, Organisationen der Zivilgesellschaft und die betroffenen Personen selbst, also die natürlichen Personen, deren Daten durch die Behörden bearbeitet werden.

B. Problemstellung

Die Bearbeitung von Personendaten durch staatliche Behörden wird in der Schweiz auf Ebene Bund und Kantone durch die jeweiligen Datenschutzgesetze geregelt und die Einhaltung dieser Vorgaben wird durch Datenschutzbeauftragte überwacht.[10] Die Bearbeitung von Personendaten durch Bundesorgane muss unter dem geltenden DSG und unter dem revidierten Bundesgesetz über den Datenschutz (revDSG)[11] einer Reihe von Vorgaben genügen. Im Vordergrund stehen dabei die Grundsätze der Transparenz (Art. 4 Abs. 4 DSG; Art. 6 Abs. 3 revDSG), der Verhältnismässigkeit (Art. 4 Abs. 2 DSG; Art. 6 Abs. 2 revDSG), der Zweckbindung (Art. 4 Abs. 3 DSG; Art. 6 Abs. 3 revDSG) und der Datensicherheit (Art. 7 DSG; Art. 8 revDSG). Zudem dürfen Bundesorgane Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Art. 17 Abs. 1 DSG; Art. 34 Abs. 1 revDSG); diese Vorgabe entspricht

10 Für den Bund: Art. 27 DSG. Für die Kantone beispielhaft: § 34 lit. c des Zürcher Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (IDG; LS 170.4, nachstehend IDG ZH); Art. 32 Abs. 1 des Berner Datenschutzgesetzes vom 19. Februar 1986 (KDSG; BSG 152.04, nachstehend KDSG BE); § 44 Abs. 1 lit. a des Basel-Städtischen Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (IDG; SG 153.260, nachstehend IDG BS); Art. 31 Abs. 2 lit. a des Freiburger Gesetzes über den Datenschutz vom 25. November 1994 (DSchG; SR 17.1, nachstehend DSchG FR); Art. 36 Abs. 1 der Waadtländischen Loi sur la protection des données personnelles vom 11. September 2007 (LPrD; SR 172.65, nachstehend LPrD VD); Art. 56 Abs. 1 der Genfer Loi sur l'information du public, l'accès aux documents et la protection des données personnelles vom 1. März 2002 (LIPAD; SR A 2 08, nachstehend LIPAD GE).

11 Totalrevidierte Fassung vom 25. September 2020, BBl 2020 7639.

dem Grundsatz der Rechtmässigkeit (Art. 4 Abs. 1 DSG; Art. 6 Abs. 1 revDSG). Die kantonalen Datenschutzgesetze enthalten im Wesentlichen deckungsgleiche Vorgaben.[12]

Fundamentale Bedeutung für die Begrenzung der staatlichen Datenbearbeitung und für deren Überwachung durch Datenschutzbeauftragte, Medien, Zivilgesellschaft und betroffene Personen kommt den Grundsätzen der Transparenz und der Rechtmässigkeit zu. Diese Grundsätze werden in bereichsspezifischen Regelungen datenschutzrechtlicher Fragen allerdings oft miteinander verbunden, indem ein und dieselbe Rechtsnorm nicht nur eine ausreichende gesetzliche Grundlage für die Datenbearbeitung bildet, sondern zugleich auch deren Transparenz sicherstellen soll. Das allgemeine Datenschutzrecht lässt diesen Weg nicht nur zu, sondern zeichnet ihn geradezu vor, weil die Pflicht zur Information der betroffenen Personen über die Bearbeitung von Personendaten entfallen kann, wenn die Bearbeitung gesetzlich vorgesehen ist.

Nach dem geltenden Datenschutzgesetz sind Bundesorgane verpflichtet, die betroffenen Personen über die Beschaffung von Personendaten zu informieren; das gilt auch, wenn die Daten nicht bei ihnen selbst, sondern bei Dritten beschafft werden (Art. 18*a* Abs. 1 DSG). Die Pflicht zur Information entfällt, wenn die betroffenen Personen entweder bereits informiert wurden (Art. 18*a* Abs. 4 Teilsatz 1 DSG) oder wenn die Daten bei Dritten beschafft worden sind (Art. 18*a* Abs. 3 DSG) und die Speicherung oder Bekanntgabe der Daten entweder ausdrücklich im Gesetz vorgesehen (Art. 18*a* Abs. 4 lit. a DSG) oder die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist (Art. 18*a* Abs. 4 lit. b DSG). Die Transparenz wird damit grundsätzlich durch Information der betroffenen Personen und nur im eng begrenzten Fall von Art. 18*a* Abs. 4 lit. a i.V.m. Abs. 3 DSG durch das Gesetz gewährleistet.

Die Revision des Datenschutzgesetzes hat hier eine bemerkenswerte Neuerung gebracht, die im politischen Diskurs erstaunlicherweise keine Beachtung gefunden hat, obwohl sie einen eigentlichen Paradigmenwechsel bringt. Im revidierten Recht wird die Pflicht zur Information der betroffenen Personen nämlich immer entfallen, wenn die Bearbeitung von Personendaten gesetzlich vorgesehen ist (Art. 20 Abs. 1 lit. b revDSG[13]). Da Bundesorgane für die

12 Siehe dazu beispielhaft im jüngst revidierten IDG ZH: § 4 (Transparenz), § 7 (Informationssicherheit), § 8 Abs. 2 (Gesetzmässigkeit), § 9 (Zweckbindung), § 8 Abs. 1 (Verhältnismässigkeit). Im KDSG BE: Art. 5 (gesetzliche Grundlage, Zweckbindung und Verhältnismässigkeit), Art. 17 (Datensicherheit). Im IDG BS: §§ 4 und 15 (Transparenz und Erkennbarkeit der Beschaffung), § 8 (Informationssicherheit), § 9 Abs. 1 f. (Rechtmässigkeit), § 12 (Zweckbindung), §§ 9 Abs. 3 und 14 (Verhältnismässigkeit). Im DSchG FR: Art. 4 (Gesetzliche Grundlage), Art. 5 (Zweckbindung), Art. 6 (Verhältnismässigkeit), Art. 8 (Datensicherheit), Art. 9 Abs. 2 (Transparenz). In der LPrD VD: Art. 5 (Rechtmässigkeit), Art. 6 (Zweckbindung), Art. 7 (Verhältnismässigkeit), Art. 8 (Transparenz), Art. 10 (Datensicherheit). In der LIPAD GE: Art. 35 Abs. 2 (Rechtmässigkeit), Art. 37 (Datensicherheit), Art. 38 (Transparenz), Art. 35 Abs. 1 (Verhältnismässigkeit).

13 Ebenso: § 12 Abs. 3 IDG ZH und Art. 13 Abs. 3 LPrD VD. Anders aber § 15 IDG BS und Art. 38 Abs. 2 LIPAD GE, die nur Ausnahmen von der Erkennbarkeit vorsehen, wenn dadurch

Bearbeitung von Personendaten auch künftig immer eine gesetzliche Grundlage benötigen (Art. 34 Abs. 1 revDSG), werden die Bundesbehörden mit dem Inkrafttreten des revidierten Gesetzes von der Pflicht zur Information der betroffenen Personen entbunden. Das erscheint problematisch, weil sich betroffene Personen kaum durch das Lesen von Gesetzen über die Bearbeitung von Personendaten informieren und in aller Regel auch nicht in der Lage sein werden, die relevanten Bestimmungen aufzufinden und zu verstehen.[14]

Die Problematik lässt sich beispielhaft anhand der Datensammlung E-ZIVI[15] illustrieren, die alle Belange des Vollzugs des Zivildienstes unterstützt. Laut Angaben des EDÖB enthält die Datenbank 47 verschiedene Kategorien von Personendaten (z.B. AHV-Nummer, Geschlecht, Name und Adresse, Strafregisterauszüge, Disziplinarverfahren und -entscheide, vertrauensärztlicher Befund) und 27 Kategorien von Datenempfängern (z.B. Krankenkassen, Betreibungsämter, Sozialamt, Bundesamt für Polizei, Militärversicherung, SBB, Militärische Behörden, Strafjustiz- und Vollzugsbehörden, Hotelleriebetriebe).[16] Auf der Webseite von E-ZIVI sind die Kategorien von Personendaten und Datenempfängern nicht ersichtlich. Auch über den Zweck der Datenbearbeitung oder den Verantwortlichen wird auf der Webseite nicht unmittelbar informiert. Genauere Informationen erschliessen sich aus den einschlägigen gesetzlichen Grundlagen, die allerdings auf der Webseite E-ZIVI nicht genannt werden. Die gesetzlichen Grundlagen für E-ZIVI bilden Art. 80 des Zivildienstgesetzes (ZDG)[17] und die Verordnung über das Informationssystem des Zivildienstes.[18] Aus der formell-gesetzlichen Grundlage ergibt sich, dass die Vollzugsstelle ein automatisiertes Informationssystem betreibt (Art. 80 Abs. 1 ZDG), zudem werden besonders schützenswerte Personendaten (betr. Militärdiensttauglichkeit, Ausbildung sowie Eignung und Neigungen, Gesundheitszustand und die Disziplinar- und Strafverfahren nach dem ZDG) aufgezählt, die bearbeitet werden dürfen (Art. 80 Abs. 1bis ZDG). Ferner dürfen gemäss Art. 80 Abs. 1ter ZDG die AHV-Nummer systematisch verwendet und Daten über Strafurteile, hängige Strafverfahren und freiheitsentziehende Massnahmen gespeichert werden (Art. 80 Abs. 1^{quater} ZDG). Welche weiteren Daten bearbeitet werden, ist Art. 80 ZDG nicht zu entnehmen. Gemäss Art. 80 Abs. 4 ZDG regelt der Bundesrat weitere Aspekte, einschliesslich der Kategorien der zu erfassenden Daten. Die Verordnung über das Informationssystem des Zivildiens-

---

die Erfüllung der gesetzlichen Aufgaben ernsthaft gefährdet wäre. Das KDSG BE und das DSchG FR enthalten keine vergleichbare Regelung.

14 Ebenso Bruno Baeriswyl, Der „grosse Bruder" DSGVO: Übereinstimmungen und Unterschiede zum DSG im Überblick, SZW 2021, S. 13; Bertil Cottier, Transparences des traitements de données personelles opérés par les organes fédéraux: un pas en avant, deux en arrière, SZW 2021, S. 70 f.

15 Siehe dazu ‹https://www.ezivi.admin.ch/› (zuletzt besucht am 16. Dezember 2021).

16 EDÖB Datareg 3.2, Register-Nr. 199600743, abrufbar unter ‹https://www.datareg.admin.ch/› (zuletzt besucht am 16. Dezember 2021).

17 Bundesgesetz vom 6. Oktober 1995 über den zivilen Ersatzdienst (ZDG; SR 824.0).

18 Verordnung vom 20. August 2014 über das Informationssystem des Zivildienstes (SR 824.095).

tes enthält sodann zusätzliche Informationen. Art. 2 der Verordnung nennt als Verantwortlichen das Bundesamt für Zivildienst und Art. 3 der Verordnung listet die Zwecke von E-ZIVI auf. Dazu zählen z.B. die Durchführung des Zulassungsverfahrens zum Zivildienst, die Vorbereitung, die Durchführung, die Verwaltung, die Kontrolle und die Auswertung von Einsätzen, die Durchführung von Disziplinarverfahren und die Bearbeitung von Schadenersatzbegehren, Buchhaltung, Dokumentation und Statistik etc. Ferner finden sich in den beiden Anhängen zur Verordnung die Benützerinnen und Benützer der Datenbank (Anhang A) sowie die einzelnen Daten einschliesslich der Zugriffsrechte darauf (Anhang B). Insgesamt lassen sich aus den gesetzlichen Grundlagen demnach zwar die zur Herstellung von Transparenz nach dem DSG erforderlichen Informationen zusammentragen. Allerdings ist dies mit einigem Aufwand verbunden – vor allem aber erfordert das Zusammentragen der Informationen vertiefte juristische Kenntnisse. Dies gilt erst recht für Datenbearbeitungen, deren Rechtsgrundlage sich nicht im nationalen Recht finden.[19]

Allein dieses Beispiel zeigt, dass die Schaffung von Transparenz über die gesetzliche Grundlage für die betroffenen Personen nicht sinnvoll ist. Mit Blick auf die zunehmende Digitalisierung in der öffentlichen Verwaltung, die Nutzung grosser Datenbestände («Big Data») und die Überlegungen zum Einsatz von Künstlicher Intelligenz («KI»), könnte ein solches Vorgehen gar kontraproduktiv sein.[20] Die Herstellung von Transparenz im Gesetz könnte angesichts

19 Siehe dazu z.B. die Datensammlung «Applicable Legislation Portal Switzerland (ALPS)», abrufbar unter ‹https://www.eak.admin.ch/eak/de/home/Firmen/arbeiten_im_ausland/alps.html› (zuletzt besucht am 16. Dezember 2021), die sich auf verschiedene internationale Verträge abstützt. Konkret auf die Folgenden: Abkommen vom 21. Juni 1999 zwischen der Schweizerischen Eidgenossenschaft einerseits und der Europäischen Gemeinschaft und ihren Mitgliedstaaten andererseits über die Freizügigkeit (SR 0.142.112.681); Verordnung (EG) Nr. 883/2004 vom 29. April 2004 des Europäischen Parlaments und des Rates vom 29. April 2004 zur Koordinierung der Systeme der sozialen Sicherheit. Geändert durch: Verordnung (EG) Nr. 988/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 (Abl. L 284 vom 30. Oktober 2009, S. 43). In der Fassung von Anhang II zum Abkommen zwischen der Europäischen Gemeinschaft und ihren Mitgliedstaaten einerseits und der schweizerischen Eidgenossenschaft andererseits über die Freizügigkeit (SR 0.831.109.268.1); sowie Verordnung (EG) Nr. 987/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 zur Festlegung der Modalitäten für die Durchführung der Verordnung (EG) Nr. 883/2004 über die Koordinierung der Systeme der sozialen Sicherheit (SR 0.831.109.268.11). Siehe dazu EDÖB Datareg 3.2, Register-Nr. 201700023, abrufbar unter ‹https://www.datareg.admin.ch/› (zuletzt besucht am 16. Dezember 2021).

20 Zu den Entwicklungen der Digitalisierung in der Verwaltung sowie der Nutzung von KI und Big Data auf Bundesebene siehe etwa den Bericht der interdepartementalen Arbeitsgruppe «Künstliche Intelligenz» an den Bundesrat vom 13. Dezember 2019 zum Thema «Herausforderungen der künstlichen Intelligenz» sowie die Leitlinien «Künstliche Intelligenz» für den Bund des Bundesrates vom 25. November 2020. Beide Dokumente sind abrufbar unter ‹https://www.sbfi.admin.ch/sbfi/de/home/bfi-politik/bfi-2021–2024/transversale-themen/digitalisierung-bfi/kuenstliche-intelligenz.html› (zuletzt besucht am 16. Dezember 2021). Siehe dazu ferner die Organisation zur Umsetzung der E-Government-Strategie Schweiz, abrufbar unter ‹https://www.egovernment.ch/de› (zuletzt besucht am 16. Dezember 2021), oder das Kompetenzzentrum für Datenwissenschaft des Bundesamtes für Statistik, abrufbar unter ‹https://www.bfs.admin.ch/bfs/de/home/dscc/dscc.html› (zuletzt besucht am 16. Dezember 2021). Ab 2022 soll für die

der zunehmenden Vielfalt und Vielzahl von Datenbearbeitungen im Resultat dazu führen, dass für betroffene Personen die Kenntnisnahme der für sie relevanten Informationen noch weiter erschwert wird. Dieses Ergebnis steht im offenen Widerspruch zum zentralen Anliegen der Revision des Datenschutzgesetzes, die Transparenz der Bearbeitung von Daten und die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten zu verbessern.[21]

C. Gesetzliche Grundlage

Nach dem Legalitätsprinzip (Art. 5 BV), das auch als Grundsatz der Gesetzmässigkeit bezeichnet wird, bedarf alles staatliche Handeln einer gesetzlichen Grundlage.[22] Bundesorgane dürfen deshalb Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. Das ergibt sich im Datenschutzrecht aus dem Grundsatz der Rechtmässigkeit der Datenbearbeitung (Art. 6 Abs. 1 revDSG)[23] und wird im 6. Kapitel des DSG, das die besonderen Bestimmungen zur Datenbearbeitung durch Bundesorgane enthält, in Art. 34 Abs. 1 revDSG ausdrücklich geregelt.[24] Entsprechende Bestimmungen finden sich auch in den kantonalen Datenschutzgesetzen.[25] Nach dem Willen des Gesetzgebers bestimmt sich der Detaillierungsgrad der gesetzlichen Grundlagen auch im Datenschutzrecht nach den allgemeinen Grundsätzen, unter besonderer Berücksichtigung der aus der Einschränkung von Grundrechten fliessenden Anforderungen.[26] Art. 34 Abs. 1 revDSG enthält damit weder nach dem Wortlaut noch

---

Bundesverwaltung zudem ein Kompetenznetzwerk KI aktiv werden, siehe ‹https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-84840.html›.

21 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, S. 6943.

22 Giovanni Biaggini, Bundesverfassung der Schweizerischen Eidgenossenschaft, Kommentar, 2. Aufl., Zürich 2017, N 7 zu Art. 5 BV; Astrid Epiney, in: Bernhard Waldmann/Eva Maria Belser/Astrid Epiney (Hrsg.), Bundesverfassung, Kommentar, Basel 2015, N 40 zu Art. 5 BV; Benjamin Schindler, in: Bernhard Ehrenzeller et al. (Hrsg.), Die Schweizerische Bundesverfassung, Kommentar, Zürich/Basel/Genf 2002, N 28 zu Art. 5 BV.

23 Bruno Baeriswyl, in: Bruno Baeriswyl/Kurt Pärli (Hrsg.), Datenschutzgesetz, Kommentar, Bern 2015, N 6 zu Art. 4 DSG; Astrid Epiney, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.), Datenschutzrecht – Grundlagen und öffentliches Recht, § 9 N 1; David Rosenthal, in David Rosenthal/Yvonne Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich 2008, N 4 Art. 4 DSG.

24 Diese Regelung entspricht der bisherigen Regelung in Art. 17 Abs. 1 DSG; siehe dazu Botschaft 2017 (Fn. 21), S. 7079.

25 Siehe dazu beispielhaft: § 8 IDG ZH; § 9 Abs. 1 f. IDG BS; Art. 4 DSchG FR; Art. 5 LPrD VD; Art. 35 Abs. 2 LIPAD GE.

26 Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz (DSG), BBl 1988 II 413, S. 467; hier zu Art. 14 Abs. 1 aDSG, der dem späteren Art. 17 Abs. 1 DSG entspricht. Der Formulierung von Art. 14 Abs. 1 aDSG wurde sowohl im Ständerat als auch im Nationalrat diskussionslos zugestimmt (Amtl. Bull. 1990 StR 149; Amtl. Bull. 1991 NR 970).

nach dem Willen des Gesetzgebers einen eigenständigen, über die Anforderungen des Legalitätsprinzips nach Art. 5 Abs. 1 BV hinausgehenden Gehalt.

Aus dem Legalitätsprinzip folgt, dass alle für ein Gemeinwesen grundlegenden Rechtsnormen in einem Gesetz im formellen Sinn enthalten sein müssen. Diese Anforderung an die Normstufe ergibt sich auf Bundesebene aus Art. 164 Abs. 1 BV, wonach alle wichtigen rechtsetzenden Bestimmungen als Bundesgesetze zu erlassen sind.[27] Die Kantonsverfassungen enthalten teilweise ähnliche Bestimmungen.[28] Mit Blick auf die Einschränkung von Grundrechten (hier insbesondere Art. 13 Abs. 2 BV) entspricht der Gehalt von Art. 164 Abs. 1 lit. b BV der Vorgabe in Art. 36 Abs. 1 Satz 2 BV, wonach schwerwiegende Einschränkungen von Grundrechten in einem Gesetz im formellen Sinn vorgesehen sein müssen.[29] Ob ein Eingriff als schwerwiegend zu qualifizieren ist, beurteilt sich nach der Intensität der Zurückbindung grundrechtlicher Ansprüche.[30]

Diese verfassungsrechtlichen Vorgaben werden vom revDSG im Wesentlichen übernommen.[31] Gemäss Art. 34 revDSG ist nicht nur bei der Bearbeitung von besonders schützenswerten Personendaten grundsätzlich[32] eine formell-gesetzliche Grundlage erforderlich, sondern auch beim sog. Profiling (Art. 34 Abs. 2 lit. b revDSG); dasselbe gilt, wenn der Zweck oder die Art und Weise der Datenbearbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der Betroffenen führen können (Art. 34 Abs. 2 lit. c revDSG).[33] Auch auf kantonaler Ebene finden sich Bestimmungen, die für die Bearbeitung von besonders schützenswerten Personendaten eine formell-gesetzliche Grundlage verlangen.[34]

Die erforderliche Normdichte lässt sich nicht abstrakt bestimmen, sondern nur im Einzelfall ermitteln. Sie hängt nach der Rechtsprechung des Bundesgerichts unter anderem von der Vielfalt der zu ordnenden Sachverhalte, der Komplexität und der erst bei der Konkretisierung im Einzelfall möglichen,

---

27 Pierre Tschannen, in: Ehrenzeller et al. (Hrsg.) (Fn. 22), N 6 zu Art. 164 BV.

28 Siehe dazu beispielhaft: Art. 38 Verfassung des Kantons Zürich vom 27. Februar 2005 (SR 131.211); Art. 69 Abs. 4 Verfassung des Kantons Bern vom 6. Juni 1993 (SR 131.212); Art. 90 Abs. 1 Verfassung des Kantons Uri vom 28. Oktober 1984 (SR 131.214); § 83 Abs. 1 Verfassung des Kantons Basel-Stadt vom 5. März 2005 (SR 131.222.1); § 63 Abs. 1 Verfassung des Kantons Basel-Landschaft (SR 131.222.2). Siehe allgemein zu den Unterschieden und der Entwicklung der verfassungsrechtlichen Verankerung des Inhalts formeller Gesetze in den Kantonsverfassungen Andreas Auer, Staatsrecht der schweizerischen Kantone, Bern 2016, Rz. 665 ff.

29 Tschannen (Fn. 27), N 18 zu Art. 164 BV. Auf den Vorbehalt der polizeilichen Generalklausel ist in diesem Kontext nicht weiter einzugehen.

30 Regina Kiener/Walter Kälin/Judith Wyttenbach, Grundrechte, 3. Aufl., Bern 2018, § 9 N 34.

31 Zu diesbezüglicher Kritik am noch geltenden DSG siehe etwa Eva Maria Belser, in: Belser/Epiney/Waldmann (Fn. 23), § 6 N 128.

32 Zu den Ausnahmen siehe Art. 34 Abs. 3 f. revDSG.

33 Siehe auch Botschaft 2017 (Fn. 21), S. 7079 f.

34 Siehe dazu beispielhaft: § 8 Abs. 2 IDG ZH; § 9 Abs. 2 IDG BS; Art. 5 Abs. 2 LPrD VD; Art. 35 Abs. 2 LIPAD GE. Das DSchG FR enthält keine entsprechende Vorschrift.

sachgerechten Entscheidung ab.[35] Weitere Faktoren sind die Vorhersehbarkeit der im Einzelfall erforderlichen Entscheidung, die Normadressaten und die Schwere des Eingriffs in Grundrechte.[36] Die allgemeinen Anforderungen an die Normdichte gelten auch im Datenschutzrecht[37]; relevante Faktoren sind insbesondere, «ob und wie weit mit einer Datenbearbeitung in die Grundrechte der Bürger eingegriffen wird, die Art der bearbeiteten Daten, der Kreis der betroffenen Personen, aber auch die Organisation des Informationssystems und der allfällige Einbezug kantonaler oder privater Stellen in die Bearbeitung».[38] Die Anforderungen an den Bestimmtheitsgrad der gesetzlichen Grundlage sind allerdings nicht allzu hoch. Zwar müssen Zweck, beteiligte Organe und Ausmass der Datenbearbeitung in den Grundzügen festgelegt sein. In der Regel ist allerdings ausreichend, dass eine Datenbearbeitung in einem einsichtigen sachlichen Zusammenhang mit der Aufgabe der betreffenden Behörde steht.[39] Auch bei der Bearbeitung besonders schützenswerter Personendaten reicht der blosse Hinweis, dass solche Daten bearbeitet werden. Welche Arten besonders schützenswerter Personendaten bearbeitet werden, muss nach der Rechtsprechung des Bundesgerichts nicht in einem Gesetz im formellen Sinn spezifiziert werden.[40]

D. Transparenz

I. Verfassungsrechtliche Anknüpfung

Das Datenschutzrecht unterliegt einer grundrechtlichen Prägung. Die schweizerische Bundesverfassung schützt das Recht auf Privatsphäre (Art. 13 Abs. 1 BV) und sieht ein Recht auf Schutz vor Missbrauch der persönlichen Daten vor (Art. 13 Abs. 2 BV). Nach ständiger Rechtsprechung des Bundesgerichts umfasst Art. 13 Abs. 2 BV ein Grundrecht auf informationelle Selbstbestimmung.[41] Die Gewährleistung eines solchen Rechts wird auch in der Lehre als

35 BGE 144 I 126 E. 6.1 S. 137 f., m.w.H.; BGE 143 I 253 E. 6.1 S. 264, m.w.H.

36 BGE 141 I 201 E. 4.1 S. 203 f., m.w.H.; BGE 128 I 327 E. 4.2 S. 340.

37 Siehe dazu nur BGE 143 I 253 E. 6.1 S. 264, m.w.H.

38 Botschaft 1988 (Fn. 26), S. 467; ebenso: Sarah Ballenegger, in: Urs Maurer-Lambrou/Gabor-Paul Blechta (Hrsg.), Datenschutzgesetz, Öffentlichkeitsgesetz, Kommentar, 3. Aufl., Basel 2014, N 14 zu Art. 17 DSG; Yvonne Jöhri, in: Rosenthal/Jöhri (Hrsg.) (Fn. 23), N 11 zu Art. 17 DSG; Claudia Mund, in: Baeriswyl/Pärli (Hrsg.) (Fn. 23), N 10 zu Art. 17 DSG; Bernhard Waldmann/Jürg Bickel, in: Belser/Epiney/Waldmann (Hrsg.) (Fn. 23), § 12 N 45.

39 Botschaft 1988 (Fn. 26), S. 4675; ebenso: Ballenegger (Fn. 38), N 18 zu Art. 17 DSG; Waldmann/Bickel (Fn. 38), § 12 N 46; siehe auch Mund (Fn. 38), N 8 zu Art. 17 DSG, welche sich dafür ausspricht, dass eine solche «mittelbare gesetzliche Grundlage» nicht leichtfertig für die Legitimierung einer Datenbearbeitung angenommen werden dürfe. Siehe dazu ferner BGE 133 V 359, E. 6.4. S. 362, BGE 143 I 253, E. 6.5.2 S. 266 f. und BGE 144 I 126, E. 6.2. S. 139.

40 Siehe dazu etwa BGE 133 V 359, E. 6.4. S. 362; BGE 143 I 253, E. 6.5.2. S. 266 f.

41 BGE 146 I 11 E. 3.1.1 S. 13; BGE 145 IV 42 E. 4.2 S. 46 f.; BGE 144 I 126 E. 4.1 S. 131; BGE 143 I 253 E. 4.8 S. 263; BGE 142 II 340 E. 4.2 S. 347; BGE 140 I 2 E. 9.1 S. 22 (hier in Verbin-

Teilgehalt des Rechts auf Schutz vor Missbrauch der persönlichen Daten fast einhellig anerkannt.[42] Das Bundesgericht hat in jüngerer Zeit regelmässig festgehalten, dass die betroffenen Personen nicht nur gegenüber staatlicher, sondern auch gegenüber privater Bearbeitung «ihrer» Personendaten ein Recht auf informationelle Selbstbestimmung haben.[43] Diese Ausdehnung, die vom Bundesgericht erstaunlicherweise nicht einmal ansatzweise begründet wird, entspricht zwar der überwiegenden Lehre;[44] ob es unter Privaten ein Recht auf informationelle Selbstbestimmung geben kann, ist aber umstritten.[45]

Die Ausübung des Grundrechts auf informationelle Selbstbestimmung setzt voraus, dass die betroffenen Personen um die Bearbeitung ihrer Personendaten wissen. Dieses Wissen umfasst nicht nur den blossen Umstand der Datenbearbeitung, sondern auch Informationen über die Art der bearbeiteten Daten, den Zweck der Bearbeitung und die verantwortliche Behörde sowie allfällige Empfänger der Personendaten. Da informationelle Selbstbestimmung ohne diese Informationen nicht möglich ist, kommt dem Grundsatz der Transparenz der Datenbearbeitung, der auch als Grundsatz der Erkennbarkeit bezeichnet wird, Verfassungsrang zu.[46] Im aDSG vom 19. Juni 1992 war das Erfordernis der Transparenz zwar nicht als allgemeiner Grundsatz normiert, der für die Datenbearbeitung durch Private und Bundesorgane gilt. Für die Bearbeitung durch

---

dung mit dem Recht auf persönliche Freiheit (Art. 10 Abs. 2 BV); BGE 128 II 259 E. 3.2 S. 268; ebenso Botschaft 2017 (Fn. 21), S. 7010.

42 Siehe dazu allgemein: Biaggini (Fn. 22), N 11 zu Art. 13 BV; Rainer J. Schweizer, in: Ehrenzeller et al. (Hrsg.) (Fn. 22), N 72 zu Art. 13, BV m.w.H.; siehe auch Oliver Diggelmann, in: Waldmann/Belser/Epiney (Hrsg.) (Fn. 22), N 32 zu Art. 13 BV, der diese in Anlehnung an das deutsche Bundesverfassungsgericht verwendete Terminologie als «unschön» bezeichnet, sich aber nicht grundsätzlich kritisch dazu äussert. Für das Datenschutzrecht: Baeriswyl (Fn. 23), N 1 zu Vorbemerkungen zu Art. 1–3 DSG; Urs Maurer-Lambrou/Simon Kunz, in: Maurer-Lambrou/Blechta (Hrsg.) (Fn. 38), N 18 ff. zu Art. 1 DSG; Rosenthal (Fn. 23), N 2 f. zu Art. 1 DSG.

43 BGE 146 I 11 E. 3.1.1 S. 13; BGE 144 I 126 E. 4.1 S. 131; BGE 142 II 340 E. 4.2 S. 347; BGE 140 I 2 E. 9.1 S. 22.

44 Belser (Fn. 31), § 6 N 60; Hussein Noureddine, in: Nicolas Passadelis/David Rosenthal/Hanspeter Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, § 3 N 3.105; Schweizer (Fn. 42), N 84 zu Art. 13 BV.

45 Kritisch namentlich: Florent Thouvenin, Informational Self-Determination: A Convincing Rationale for Data Protection Law?, JIPITEC 2021 (erscheint demnächst).

46 So zählt Rainer J. Schweizer in der Erstauflage des St. Galler Kommentars den «Grundsatz der Offenheit und Transparenz der Bearbeitung» zu den verfassungsrechtlich garantierten Grundsätzen der Bearbeitung von Personendaten; Schweizer (Fn. 42), N 43 zu Art. 13. Ebenso: Giovanni Biaggini, Ein Personenidentifikator im Lichte des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 13 BV), Rechtsgutachten zu Handen des EDÖB, Zürich 2002, S. 20, abrufbar unter: ‹https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2006/11/ein_personenidentifikatorimlichtedesverfassungsrechtlichenpersoe.pdf.download.pdf/ein_personenidentifikatorimlichtedesverfassungsrechtlichenpersoe.pdf› (zuletzt besucht am 16. Dezember 2021). In Lehre und Rechtsprechung wurde diese Frage soweit ersichtlich allerdings nicht weiter aufgegriffen; siehe etwa die Kommentierung zu Art. 13 Abs. 2 BV von Rainer J. Schweizer in der Drittauflage des St. Galler Kommentars, in der er den Grundsatz der Erkennbarkeit der Datenbearbeitung nicht mehr erwähnt.

Bundesorgane sah Art. 18 Abs. 2 aDSG aber vor, dass das Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen für die betroffenen Personen erkennbar sein muss. Dennoch war anerkannt, dass das Erfordernis der Erkennbarkeit der Bearbeitung durch Bundesorgane für alle Personendaten gilt.[47] Mit der Teilrevision 2006 wurde Art. 18*a* Abs. 2 aDSG aufgehoben und die Erkennbarkeit als allgemeiner Grundsatz in Art. 4 Abs. 4 DSG geregelt.[48] Das derzeit geltende Recht stellt damit klar, dass die Beschaffung von Personendaten und der Zweck der Bearbeitung für die betroffenen Personen erkennbar sein müssen. Das gilt auch für die kantonalen Datenschutzgesetze, die diesen Grundsatz meist ebenfalls ausdrücklich normieren.[49]

Das revDSG enthält keine ausdrückliche Regelung des Grundsatzes der Transparenz. Dies erstaunt insofern, als der Bundesrat schon im ersten Satz der Botschaft festgehalten hat, das Ziel der Revision bestehe darin, den Datenschutz zu stärken, «indem die Transparenz der Bearbeitung von Daten und die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten verbessert werden».[50] Hinzu kommt, dass mit der Revision des Datenschutzgesetzes den Entwicklungen im Europarat und in der EU Rechnung getragen werden sollte, indem die revidierte Fassung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (sog. Konvention 108) ratifiziert wird, die erforderlichen Anpassungen im schweizerischen Recht vorgenommen werden und sichergestellt wird, dass das Schweizer Datenschutzgesetz ein Schutzniveau erreicht, das jenem der Europäischen Datenschutzgrundverordnung (DSGVO) entspricht.[51] Das Erfordernis der Transparenz ist in der DSGVO prominent normiert und auch in der modernisierten

47 So etwa Botschaft vom 19. Februar 2003 zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenermittlung, BBl 2003 2101, S. 2110 f.; Yvonne Jöhri/Marcel Studer, in: Urs Maurer-Lambrou/Nedim Peter Vogt (Hrsg.), Datenschutzgesetz, Kommentar, 2. Aufl., Basel 2006, N 10 f. zu Art. 10 DSG; Rosenthal (Fn. 23), N 65 Art. 4 DSG sowie N 14 zu Art. 18 DSG; Rainer J. Schweizer, Die Revision des Datenschutzgesetzes, in: Astrid Epiney/Patrick Hobi (Hrsg.), Forum Europarecht, Band/Nr. 14, 2009, S. 38; a.M. wohl Urs Maurer-Lambrou/Andrea Steiner, in: Maurer-Lambrou/Blechta (Hrsg.) (Fn. 38), N 16a zu Art. 4 DSG.

48 Siehe Botschaft 2003 (Fn. 47), S. 2144.

49 Siehe dazu beispielhaft: § 15 IDG BS; Art. 9 Abs. 2 DschG FR; Art. 8 LPrD VD; Art. 38 Abs. 1 LIPAD GE; implizit § 12 IDG ZH, wonach das öffentliche Organ die betroffenen Personen über die Beschaffung von Personendaten informiert. Keine Regelung hierzu enthält das KDSG BE.

50 Botschaft 2017 (Fn. 21), S. 6943; siehe dazu auch S. 6972 f., wo klargestellt wird, dass die Transparenz durch die Einführung einer allgemeinen Informationspflicht und durch eine Erweiterung des Auskunftsrechts erhöht werden soll.

51 Botschaft 2017 (Fn. 21), S. 6970; ebenso schon Bundesamt für Justiz (BJ), Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 18; siehe dazu auch Baeriswyl, (Fn. 14), S. 8 ff.

Europarats-Konvention 108 (Konvention 108+) vorgesehen.[52] Es ist deshalb erstaunlich, dass das revDSG keine vergleichbare Regelung enthält. Dass der Grundsatz der Transparenz der Datenbearbeitung im künftigen Gesetz nicht mehr ausdrücklich genannt wird, ändert allerdings nichts an dessen Geltung.

Dies ergibt sich nicht nur aus den Materialien,[53] sondern auch aus mehreren Normen des revDSG: Nach Art. 6 Abs. 3 revDSG dürfen Personendaten nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck bearbeitet werden; die gesetzliche Regelung der Erkennbarkeit des Zwecks der Datenbearbeitung setzt dabei zwingend voraus, dass auch die Datenbearbeitung als solche erkennbar ist. Nach Art. 6 Abs. 2 revDSG muss die Bearbeitung von Personendaten nach Treu und Glauben erfolgen. Aus diesem Grundsatz wurde schon im aDSG derjenige der Transparenz abgeleitet;[54] ebendies wird nun in der Lehre auch für das revidierte Gesetz vertreten.[55] Hinzu kommt, dass zentrale Bestimmungen des revDSG mit aller Deutlichkeit zeigen, dass das Gesetz auf dem Grundsatz der Transparenz beruht, so namentlich die Regelung der Informationspflichten (Art. 19 ff. revDSG) und des Auskunftsrechts (Art. 25 ff. revDSG).[56]

II. Informationspflicht und Auskunftsrecht

Der Grundsatz der Transparenz liegt den Regelungen der Informationspflicht (Art. 19 ff. revDSG) und des Auskunftsrechts (Art. 25 ff. revDSG) zugrunde und wird in diesen konkretisiert.[57] Das gilt grundsätzlich auch für das kantonale Recht.[58] Die Bestimmungen zu Informationspflicht und Auskunftsrecht des revDSG sind auf private Personen ebenso anwendbar wie auf Bundesorgane;

---

52 Art. 5 Abs. 1 Bst. a der Datenschutz-Grundverordnung der Europäischen Union (DSGVO); Art. 8 Konvention 108+; für die englische Fassung siehe: Convention 108+, Convention for the Protection of individuals with regard to the processing of personal data: ‹https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1› (zuletzt besucht am 16. Dezember 2021).

53 Botschaft 2017 (Fn. 21), S. 7024 f., wo explizit festgehalten wird, dass die «neue Formulierung im Vergleich zum geltenden Recht keine materiellen Änderungen zur Folge [hat]»; ebenso bereits *BJ* (Fn. 51), S. 46.

54 Botschaft 1988 (Fn. 26), S. 449; Epiney (Fn. 23), § 9 N 22; Maurer-Lambrou/Steiner (Fn. 47), N 8 und N 16a zu Art. 4 DSG.

55 David Rosenthal, Das neue Datenschutzgesetz, Jusletter vom 16. November 2020, N 15; Christine Schweikard/David Vasella, Datenschutzerklärungen und AGB, digma 2020, S. 88.

56 Zur Konkretisierung der Erkennbarkeit in den Normen des DSG siehe auch: Astrid Epiney/Tobias Fasnacht, in: Belser/Epiney/Waldmann (Hrsg.) (Fn. 23), § 11 N 46; Beat Rudin, in: Baeriswyl/Pärli (Hrsg.) (Fn. 23), N 1 zu Art. 8 DSG.

57 Ebenso: Epiney/Fasnacht (Fn. 56), § 11 N 46; Rudin (Fn. 56), N 1 zu Art. 8 DSG.

58 Siehe dazu beispielhaft: § 12 IDG ZH (Informationspflicht) und § 20 IDG ZH (Auskunftsrecht); § 15 Abs. 3 IDG BS (Informationspflicht, aber nur bei Beschaffung besonderer Personendaten) und § 26 IDG BS (Auskunftsrecht); Art. 13 f. LPrD VD (Informationspflicht) und Art. 25 ff. LPrD VD (Auskunftsrecht). Im Berner, Freiburger und Genfer Recht wird dagegen nur das Aus-

gewisse Unterschiede bestehen nur, aber immerhin, bei der Regelung der Ausnahmen.[59] Die Regelung der Informationspflicht sieht vor, dass die Verantwortlichen den betroffenen Personen gewisse Informationen vermitteln müssen. Das bedeutet allerdings nicht, dass sie die Informationen zustellen oder aktiv anzeigen müssen (bspw. per Mail oder durch ein *Pop-up*-Fenster auf einer Webseite). Vielmehr genügt es, wenn die betroffenen Personen auf einfache Weise selbst auf die Informationen zugreifen können, bspw. auf eine Datenschutzerklärung, die auf einer Webseite zugänglich gemacht wird.[60]

Nach dem Wortlaut der Regelung hat der Verantwortliche die betroffenen Personen «angemessen» über die Beschaffung von Personendaten zu informieren (Art. 19 Abs. 1 Teilsatz 1 revDSG).[61] Der Begriff «angemessen» ist auslegungsbedürftig. Nach dem allgemeinen Wortgebrauch bedeutet er, dass etwas den Verhältnissen entsprechend zu erfolgen hat. Das gilt für Inhalt und Umfang der Information ebenso wie für die Adressaten und die Zugänglichkeit. Mit Blick auf Inhalt und Umfang bedeutet dies, dass nicht einfach «möglichst viel Informationen» bereitzustellen sind, sondern diejenigen Informationen, die dem Sinn und Zweck der Transparenz entsprechen.[62] Bezüglich der betroffenen Personen als Adressaten ist die Angemessenheit so zu verstehen, dass die Informationen adressatengerecht sein, also so vermittelt werden müssen, dass die betroffenen Personen in der Lage sind, sie zu verstehen[63]. Handelt es sich bei den betroffenen Personen um Fachpersonen, kann die Information z.B. unter Nutzung des für diese Personen gebräuchlichen Fachvokabulars erfolgen, während die Information einer heterogenen Gruppe von Bürgerinnen und Bürgern in allgemein verständlicher Sprache erfolgen muss. Aus dem Erfordernis der Angemessenheit folgt auch, dass die Information für die betroffenen Personen leicht auffindbar und zugänglich sein muss.

---

kunftsrecht explizit geregelt: Art. 21 KDSG BE; Art. 23 ff. DschG FR und Art. 44 ff. LIPAD GE.

59 So kann der private Verantwortliche gemäss Art. 20 Abs. 3 lit. c revDSG die Mitteilung von Informationen einschränken, aufschieben oder darauf verzichten, wenn eigene überwiegende Interessen es erfordern und er die Daten nicht Dritten bekannt gibt. Dagegen kann ein Bundesorgan nach Art. 20 Abs. 3 lit. d Ziff. 1 revDSG die Mitteilung der Information einschränken, aufschieben oder darauf verzichten, wenn es wegen überwiegender öffentlicher Interessen erforderlich ist.

60 Botschaft 2017 (Fn. 21), S. 7050 f.; siehe auch Rosenthal (Fn. 55), N 37.

61 Die Formulierung dieser Bestimmung im Entwurf des Bundesrates enthielt den Ausdruck «angemessen» noch nicht, sondern lautete: «Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten (…)», vgl. Art. 17 revDSG-E in BBl 2017 7213.

62 Siehe Kap. D.III.

63 Siehe auch René Wiederkehr, Transparenz als Grundsatz rechtsstaatlichen Handelns (Art. 5 BV), ZBl 2007, 521, 528 f., mit Blick auf die Transparenz staatlicher Rechtsetzung und Information. Gemäss Wiederkehr fordert das Transparenzprinzip demnach sowohl eine allgemeine Zugänglichkeit staatlicher Informationen als auch eine gewisse Qualität der Information, zu welcher deren Verständlichkeit gehört.

Im Gegensatz zur Informationspflicht verlangt das Auskunftsrecht von den Verantwortlichen nicht, den betroffenen Personen gewisse Informationen von sich aus zur Verfügung zu stellen; vielmehr müssen die Verantwortlichen den Betroffenen die Informationen erst auf deren Anfrage zukommen lassen. Die Informationspflicht und das Auskunftsrecht gewährleisten damit gemeinsam die gesetzlich geforderte Transparenz – die Informationspflicht durch einen «Push-Mechanismus», das Auskunftsrecht durch einen «Pull-Mechanismus».

Der Unterscheidung zwischen «push» und «pull» entspricht, dass der Gehalt der zu vermittelnden Informationen unterschiedlich weit gefasst ist. Die Informationspflicht stellt sicher, dass der Verantwortliche den betroffenen Personen die zentralen Informationen über die Datenbearbeitung vermittelt, insbesondere Informationen über die Identität und die Kontaktdaten des Verantwortlichen, über den Bearbeitungszweck und gegebenenfalls über die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekannt gegeben werden (Art. 19 Abs. 2 revDSG). Wenn eine betroffene Person Näheres erfahren will, kann sie mithilfe des Auskunftsrechts vom Verantwortlichen weitere Informationen verlangen, insbesondere über die Aufbewahrungsdauer der Personendaten oder die Kriterien zu deren Festlegung (Art. 25 Abs. 2 lit. d revDSG) und über die Herkunft der Personendaten, soweit diese nicht bei den Betroffenen beschafft worden sind (Art. 25 Abs. 2 lit. e revDSG).

III. Sinn und Zweck

Sinn und Zweck des Grundsatzes der Transparenz werden in der Regelung der Informationspflicht und des Auskunftsrechts ausdrücklich normiert: Die betroffenen Personen müssen über diejenigen Informationen verfügen, die erforderlich sind, damit sie ihre Rechte nach dem DSG geltend machen können[64] und eine transparente Datenbearbeitung gewährleistet ist (Art. 19 Abs. 2 Teilsatz 1 revDSG; Art. 25 Abs. 2 Satz 1 revDSG). Nach Auffassung des Gesetzgebers ist die Transparenz damit sowohl blosses Mittel zum Zweck (Erforderlichkeit für Geltendmachung der Rechte) als auch Zweck für sich (Gewährleistung einer transparenten Datenbearbeitung). Der Zweck der Gewährleistung einer transparenten Datenbearbeitung ist allerdings kein reiner Selbstzweck. Vielmehr dient er dem übergeordneten Ziel des Datenschutzrechts, das für die Bearbeitung von Personendaten durch Behörden im Schutz der Grundrechte der betroffenen natürlichen Personen besteht (Art. 1 DSG und revDSG). Die Transparenz muss damit nur soweit gewährleistet sein, als sie erforderlich ist, um die Grundrechte der Betroffenen zu schützen. Im Vordergrund stehen dabei das

64 Ebenso zum geltenden DSG: Botschaft 2003 (Fn. 47), S. 2125; Baeriswyl (Fn. 23), N 49 f. zu Art 4 DSG.

Recht auf Privatsphäre (Art. 13 Abs. 1 BV) und das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV).[65]

Damit ist klar, dass der Grundsatz der Transparenz kein «Maximum» an Transparenz erfordert, also nicht voraussetzt, dass alle erdenklichen Informationen vermittelt werden. Die flexible Regelung der Informationspflicht soll nach den Ausführungen des Bundesrates vielmehr sicherstellen, «dass die Verantwortlichen keine unnötigen Informationen übermitteln müssen und die betroffenen Personen nur erforderliche Informationen erhalten».[66] Dies bringt zum Ausdruck, dass mehr Information nicht notwendigerweise zu mehr Transparenz führt. Vielmehr kann ein Übermass an Information auch bewirken, dass die betroffenen Personen den relevanten Informationsgehalt nicht mehr aus der Masse an Informationen herausfiltern können. Dass eine Beschränkung besteht, ergibt sich zudem aus der Regelung von Informationspflicht und Auskunftsrecht, die zwar keinen abschliessenden Katalog der zu vermittelnden Informationen enthalten, aber mit der nicht-abschliessenden Aufzählung doch klarstellen, dass der Umfang der zu vermittelnden Informationen begrenzt ist. Noch klarer wird diese Begrenzung in der Regelung der Ausnahmen und Einschränkungen von Informationspflicht und Auskunftsrecht (Art. 20 und Art. 26 f. revDSG). Hier zeigt sich mit aller Deutlichkeit, dass dem Interesse der berechtigten Personen an der Information schützenswerte Interessen der Verantwortlichen oder Dritter entgegenstehen können, die den Anspruch auf Information begrenzen.

E. Verhältnis von gesetzlicher Grundlage und Transparenz

Das Erfordernis der gesetzlichen Grundlage verfolgt ein doppeltes Ziel: Zum einen setzt es das Legalitätsprinzip (Art. 5 Abs. 1 BV) im DSG um, zum andern trägt es dem Umstand Rechnung, dass Eingriffe in Grundrechte auf einer ausreichenden gesetzlichen Grundlage beruhen müssen.[67] Die notwendigen Elemente der gesetzlichen Grundlage für die Datenbearbeitung[68] sind allerdings nicht deckungsgleich mit den Angaben, die zur Herstellung von Transparenz erforderlich sind[69]. Mit dem Bestehen einer gesetzlichen Grundlage, die den Anforderungen des Legalitätsprinzips genügt, sind deshalb nicht automatisch auch die Anforderungen erfüllt, die sich aus dem Grundsatz der Transparenz ergeben.

---

65 Ebenso: Maurer-Lambrou/Kunz (Fn. 42), N 16 ff. zu Art. 1 DSG; Rosenthal (Fn. 23), N 3 zu Art. 1 DSG; siehe auch Botschaft 1988 (Fn. 26), S. 438.

66 Botschaft 2017 (Fn. 21), S. 7051.

67 Siehe dazu allgemein: Biaggini (Fn. 22), N 9 ff. zu Art. 36 BV; Epiney (Fn. 22), N 29 ff. Art. 36 BV; Schweizer (Fn. 42), N 14 ff. zu Art. 36 BV. Für das Datenschutzrecht: Mund (Fn. 38), N 1 zu Art. 17 DSG; Jöhri (Fn. 38), N 1 zu Art. 17 DSG.

68 Siehe dazu Kap. C.

69 Siehe dazu Kap. D.

Auf dieser Hypothese beruht allerdings die mit der Revision neu eingeführte Bestimmung von Art. 20 Abs. 1 lit. b revDSG, die sich in ähnlicher Form auch in einigen kantonalen Erlassen[70] findet. Diese sieht vor, dass die Pflicht zur Information der betroffenen Personen über die Bearbeitung «ihrer» Personendaten entfällt, wenn die Bearbeitung gesetzlich vorgesehen ist. Nach dem Bundesrat beruht diese Ausnahme von der Informationspflicht nicht etwa auf einer Ausnahme vom Grundsatz der Transparenz, sondern vielmehr darauf, dass sich der gesetzlichen Grundlage «regelmässig auch die entsprechenden Informationen entnehmen»[71] lassen, wobei mit den «entsprechenden Informationen» diejenigen gemeint sind, die aufgrund der Informationspflicht nach Art. 19 revDSG zu vermitteln wären.

Dieses Verständnis wird durch die systematische Stellung von Art. 20 Abs. 1 lit. b DSG bestätigt, zumal die Informationspflicht nach Art. 20 Abs. 1 lit. a revDSG für Private und Bundesbehörden gleichermassen entfällt, wenn die betroffene Person bereits über die entsprechende Information verfügt. Der Wortlaut von Art. 20 Abs. 1 lit. b revDSG ist dabei ebenso klar wie apodiktisch. Die historische, systematische und teleologische Auslegung sprechen zwar für eine enge Auslegung, nach welcher die Ausnahme von der Informationspflicht wegen des in der Verfassung und im DSG vorgesehenen Grundsatzes der Transparenz nur greifen kann, wenn die gesetzliche Grundlage die nach Art. 19 revDSG erforderlichen Informationen tatsächlich vermittelt. Dies trifft aber in aller Regel durchaus zu, zumal namentlich jüngere Erlasse oft ausführliche Bestimmungen zur Bearbeitung von Personendaten enthalten[72]. Der Anwendungsbereich der Ausnahmebestimmung von Art. 20 Abs. 1 lit. b revDSG lässt sich damit durch Auslegung nicht in relevanter Weise einschränken. Er ist vielmehr ausserordentlich weit und erfasst praktisch jede Datenbearbeitung durch Bundesbehörden. Von einer Ausnahme kann damit eigentlich nicht die Rede sein.

Die Art. 20 Abs. 1 lit. b revDSG zugrundeliegende Hypothese, wonach mit der gesetzlichen Grundlage zugleich die Transparenz der Datenbearbeitungen sichergestellt ist, lässt sich aber auch dann nicht halten, wenn der gesetzlichen Grundlage alle erforderlichen Informationen zu entnehmen sind. Denn die erste und wichtigste Wirkung der Informationspflicht besteht darin, die betroffenen Personen über den Umstand zu informieren, dass Behörden Personendaten über sie bearbeiten. Ohne diese Information besteht für die Betroffenen kaum ein Anlass, sich anhand von Gesetzen und Verordnungen über die Bearbeitung «ihrer» Personendaten zu informieren. Hinzu kommt, dass die alleinige Infor-

70 Siehe dazu beispielhaft: § 12 Abs. 3 lit. b IDG ZH, Art. 13 Abs. 3 Satz 3 LPrD VD; anders aber IDG BS; DschG FR; LIPAD GE.

71 Botschaft 2017 (Fn. 21), S. 7053.

72 Siehe nur etwa den 4. Titel (Art. 93 f.) des Bundesgesetzes vom 20. Dezember 2019 über den Bevölkerungsschutz und den Zivilschutz, SR 520.1 sowie die Verordnung der Eidgenössischen Finanzmarktaufsicht über die Datenbearbeitung (Datenverordnung-FINMA) vom 8. September 2011, SR 956.124.

mation in einem Erlass kaum geeignet ist, die erforderliche Transparenz sicherzustellen.[73] Zwar ist nicht in Frage zu stellen, dass die betroffenen Personen sich durch ein Studium der Rechtsgrundlagen über die Bearbeitung ihrer Personendaten informieren *können*, wenn diese in Gesetzen oder Verordnungen hinreichend genau umschrieben ist. Wird die Information aber einzig in dieser Form vermittelt, dann bleibt die gesetzlich geforderte Transparenz für viele betroffene Personen blosse Theorie, weil nicht davon ausgegangen werden kann, dass alle Betroffenen die – häufig keineswegs adressatengerecht formulierten[74] – Angaben in Gesetzen und Verordnungen verstehen werden[75]. Damit besteht ein Widerspruch zwischen der rechtlich vorgespurten Herstellung von Transparenz über die gesetzliche Grundlage[76], die mit der Fiktion der Kenntnis der publizierten Gesetze durch jedermann[77] korrespondiert, und dem gesetzlich verankerten Zweck der Transparenz, der darin besteht, den betroffenen Personen diejenigen Informationen zu vermitteln, die es ihnen erlauben, ihre Rechte nach dem DSG geltend zu machen und die Transparenz der Datenbearbeitungen zu gewährleisten[78]. Auch eine enge Auslegung von Art. 20 Abs. 1 lit. b revDSG vermag diesen Widerspruch nicht zu lösen. Die Bestimmung sollte deshalb ersatzlos gestrichen werden.

Die Bedeutung von Art. 20 Abs. 1 lit. b revDSG ist allerdings in anderer Hinsicht zu relativieren. Denn die Bestimmung sieht nur eine Ausnahme von der Informationspflicht vor, nicht aber eine Ausnahme vom Grundsatz der Transparenz. Das ergibt sich aus dem Verfassungsgrundsatz der Transparenz[79] und aus der Systematik des revDSG, welches die Grundsätze der Datenbearbeitung (Art. 6 revDSG) und die Pflichten der Verantwortlichen, insb. die Informationspflicht (Art. 19 revDSG) und die davon bestehenden Ausnahmen (Art. 20 revDSG), in separaten Kapiteln regelt. Die Behörden müssen damit trotz der gesetzlich vorgesehenen Ausnahme von der Informationspflicht Transparenz über die Bearbeitung von Personendaten schaffen. Eine umfassende Transparenz ist denn auch unverzichtbar, weil nur so das Vertrauen der Bürgerinnen und Bürger in die staatliche Datenbearbeitung gewährleistet werden kann.

---

73 Baeriswyl (Fn. 14), S. 13; *Cottier* (Fn. 14), S. 70 f.

74 Siehe etwa Art. 101, 102, 102*a* und 102*b* des Bundesgesetzes vom 16. Dezember 2005 über die Ausländerinnen und Ausländer und über die Integration, SR 142.20 in Verbindung mit Art. 87 ff. der Verordnung vom 24. Oktober 2007 über Zulassung, Aufenthalt und Erwerbstätigkeit, SR 142.201, deren Formulierungen in der Regel kaum geeignet sein dürften, von den betroffenen ausländischen Personen verstanden zu werden. Auch das Beispiel der Rechtsgrundlagen für das System E-ZIVI belegt diese Problematik, siehe Kap. B.

75 Im Ergebnis ebenso Cottier (Fn. 14), S. 71: «Par le biais d'une large extension de l'exemption pour les traitements fondés sur une base légale, le législateur a laminé le devoir d'informer des organes fédéraux.».

76 Siehe dazu Kap. B.

77 Siehe dazu nur: Peter Forstmoser/Hans-Ueli Vogt, Einführung in das Recht, 5. Aufl., Bern 2012, Rz. 297 ff.

78 Siehe dazu Kap. D.III.

79 Siehe dazu Kap. D.I.

F. Transparenz durch Datenschutzerklärungen

I. Ausgangslage

Weder der Grundsatz der Transparenz noch die Informationspflicht oder das Auskunftsrecht verlangen, dass die zur Schaffung von Transparenz erforderliche Information in einer bestimmten Form vermittelt wird.[80] Die Botschaft zum revDSG hält denn auch fest, dass die aufgrund der Informationspflicht zu vermittelnde Information «keinem Formerfordernis unterworfen» ist.[81] Entscheidend ist vielmehr, dass «insgesamt eine Form zu wählen [ist], welche dem Zweck einer transparenten Datenbearbeitung gerecht wird».[82] Diese Aussagen beziehen sich zwar nicht ausdrücklich auf Bundesorgane, die Botschaft enthält aber auch keinerlei Hinweise, dass sie nur für Private gelten sollen. Auch Bundesorgane sind damit frei, das geeignete Mittel zu wählen, um die Transparenz ihrer Datenbearbeitungen zu gewährleisten. Dasselbe muss für die kantonalen Behörden gelten.

Das allgemein anerkannte und weltweit etablierte Mittel für das Schaffen von Transparenz durch private Datenbearbeiter ist die Datenschutzerklärung.[83] Diese dient dazu, den betroffenen Personen in einfach verständlicher Weise die wesentlichen Informationen über die Bearbeitung ihrer Personendaten zu vermitteln.

II. Datenschutzerklärungen von Privaten

Datenschutzerklärungen von Schweizer Unternehmen enthalten zumindest die gesetzlich geforderten Informationen über die Kategorien der bearbeiteten Daten, den Zweck der Datenbearbeitung, den Verantwortlichen, die allfällige Weitergabe der Daten an Dritte und allfällige automatisierte Einzelentscheidungen. Mit der Vermittlung dieser Informationen in einer Datenschutzerklärung («Push-Mechanismus») werden die Vorgaben der Informationspflicht (Art. 19 revDSG) erfüllt. Darüber hinaus vermitteln Datenschutzerklärungen meist noch weitere Informationen, etwa zur Art der bearbeiteten Personendaten (z.B. Standortdaten, Gesundheitsdaten, Finanzdaten, biometrische Daten), zur Rechtsgrundlage der Bearbeitung (insbesondere Einwilligung der betroffenen Person oder überwiegendes Interesse des Unternehmens), zur Verwendung von Daten zwecks Profiling, zur Dauer der Speicherung oder zur Frage, ob das

80 Epiney/Fasnacht (Fn. 56), § 11 N 8 sowie N 16; Mund (Fn. 38), N 6 zu Art 18a DSG; Corrado Rampini/Philippe Fuchs, in: Maurer-Lambrou/Blechta (Hrsg.) (Fn. 38), N 13 zu Art. 14 DSG; Amédéo Wermelinger, in: Baeriswyl/Pärli (Hrsg.) (Fn. 23), N 4 zu Art. 14 DSG; Michael Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.) (Fn. 44), § 4 N 4.24.

81 Botschaft 2017 (Fn. 21), S. 7051. Ebenso schon Botschaft 2003 (Fn. 47), S. 2131 f.

82 Botschaft 2017 (Fn. 21), S. 7051.

83 Rosenthal (Fn. 55), N 39; siehe ferner Botschaft 2017 (Fn. 21), S. 7050; Lukas Bühlmann/Michael Schüepp, in: Passadelis/Rosenthal/Thür (Hrsg.) (Fn. 44), § 19 N 19.42.

Unternehmen nur selbst erhobene Daten bearbeitet oder auch solche, die es von Dritten erhalten hat. Zudem finden sich regelmässig Angaben zu den Rechten der betroffenen Personen, etwa zum Auskunftsrecht.

Datenschutzerklärungen werden meist als eigenständige Dokumente auf der Webseite des Unternehmens zugänglich gemacht, manchmal werden sie den Kundinnen und Kunden auch auf Papier zur Verfügung gestellt. Die meisten Unternehmen verwenden eine einzige Datenschutzerklärung, grössere Unternehmen kombinieren bisweilen eine allgemeine Datenschutzerklärung mit spezifischen Erklärungen, die nur für bestimmte Geschäftsbereiche oder Dienste gelten. So verwendet bspw. die Migros eine allgemeine Datenschutzerklärung, die für alle Geschäftsbereiche des Migros-Genossenschafts-Bundes gilt, und besondere Datenschutzerklärungen, bspw. für die Cumulus-Karte.[84]

Neben dem traditionellen Ansatz, bei dem den betroffenen Personen alle Informationen in Textform in einem einzigen (oder allenfalls mehreren) Dokument(en) zur Verfügung gestellt werden, wird zunehmend ein differenzierter Ansatz verfolgt, der meist als *layered approach* bezeichnet wird.[85] Ausgehend von der Erkenntnis, dass die meisten Betroffenen Datenschutzerklärungen nicht lesen,[86] werden Kundinnen und Kunden auf zwei oder drei Ebenen unterschiedlich detaillierte Informationen zugänglich gemacht. Auf einer ersten Ebene finden sich Angaben zu den wichtigsten Eckpunkten der Datenbearbeitungen, bspw. mithilfe von Symbolen, die es den Kundinnen und Kunden erlauben, sich innert weniger Sekunden einen Überblick zu verschaffen.[87] Auf einer zweiten Ebene werden die Datenbearbeitungen in kurzen Texten und mit einfachen Worten erklärt und auf einer dritten Ebene finden sich detaillierte und technisch hinreichend präzise Informationen. Alle drei Ebenen bilden zusammen die Datenschutzerklärung. Gemeinsam vermögen sie eine hohe Transparenz zu gewährleisten, indem sie dem Bedürfnis nach rascher und einfacher sowie detaillierter und technischer Information zugleich Rechnung tragen.

---

84 Für die allgemeine Datenschutzerklärung siehe: ‹https://www.migros.ch/de/datenschutz.html›. Für die besonderen Angaben zur Cumulus-Karte siehe: ‹https://www.migros.ch/de/cumulus/ueber-cumulus/datenschutz.html› (beide Seiten zuletzt besucht am 16. Dezember 2021).

85 Siehe dazu: Botschaft 2017 (Fn. 21), S. 7050; Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), 24. Tätigkeitsbericht 2016/2017, Bern 2017, S. 18.

86 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers, FTC Report, März 2012, 2, S. 61; Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, Harvard Law Review 7/2013, S. 1884 ff.; Jonathan A. Obar/Anne Oeldorf-Hirsch, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, Information, Communication & Society 23/2020, S. 140 ff.; Aleecia M. McDonald/Lorrie Faith Cranor, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society 2008, S. 565, schätzen, dass ein US-Internetnutzer jährlich 201 Stunden mit dem Lesen von Datenschutzerklärungen der von ihm genutzten Services verbringen würde.

87 Siehe dazu Florent Thouvenin et al., Privacy Icons: Transparenz auf einen Blick, Jusletter vom 30. November 2020, *passim*.

Zumindest für diejenigen Personen, die sich für die Bearbeitung «ihrer» Personendaten interessieren, sind Datenschutzerklärungen damit ein geeignetes Mittel, um die gesetzlich geforderte Transparenz sicherzustellen.

III. Datenschutzerklärungen von Behörden

Auch Bundesorganen steht es frei, zur Herstellung der Transparenz ihrer Datenbearbeitungen Datenschutzerklärungen einzusetzen. Dasselbe gilt für kantonale Behörden.[88]

1. Inhalt

Entscheidet sich eine Behörde dafür, ihrer Informationspflicht bei der Beschaffung von Personendaten in einer Datenschutzerklärung nachzukommen, richtet sich deren Inhalt für die Behörden des Bundes nach Art. 19 revDSG. Für kantonale Behörden gelten die entsprechenden Vorgaben in den jeweiligen kantonalen Datenschutzgesetzen.[89] Als Mindestangaben sind nach dem Bundesrecht Informationen zum Zweck der Datenbearbeitung, zum Verantwortlichen und zur allfälligen Weitergabe der Daten aufzunehmen. Werden die Daten nicht bei den betroffenen Personen erhoben, sind auch die Kategorien der bearbeiteten Personendaten anzugeben (Art. 19 Abs. 3 revDSG). Darüber hinaus können weitere Informationen aufgenommen werden, etwa Informationen über das Fällen automatisierter Entscheidungen in einem bestimmten Bereich,[90] zur Art der bearbeiteten Personendaten, zur Rechtsgrundlage oder zur Dauer der Speicherung.

2. Rechtsnatur

In Lehre und Rechtsprechung ist allgemein anerkannt, dass das Erteilen einer Auskunft durch eine Behörde ein tatsächliches Verwaltungshandeln darstellt.[91] Dasselbe gilt für die Information der Bevölkerung durch Behörden.[92] Im Be-

88 Siehe dazu Kap. F.I.

89 Siehe dazu beispielhaft: § 12 IDG ZH; § 15 Abs. 2 f. IDG BS; Art. 9 Abs. 3 DschG FR; Art. 13 Abs. 2 LPrD VD. Das KDSG BE und das LIPAD GE enthalten keine entsprechende Bestimmung.

90 Bundesorgane sind gemäss Art. 21 Abs. 4 revDSG verpflichtet, automatisierte Einzelentscheide zu kennzeichnen, so dass darüber nicht zwingend in einer Datenschutzerklärung zu informieren ist.

91 Alain Griffel, Allgemeines Verwaltungsrecht im Spiegel der Rechtsprechung, Zürich 2017, § 3 N 60; Ulrich Häfelin/Georg Müller/Felix Uhlmann, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich/St. Gallen 2020, N 730a; Pierre Tschannen/Ulrich Zimmerli/Markus Müller, Allgemeines Verwaltungsrecht, 4. Aufl., Bern 2014, S. 260; zum Begriff des tatsächlichen Verwaltungshandelns im Allgemeinen siehe auch Marianne Tschopp-Christen, Rechtsschutz gegenüber Realakten des Bundes (Artikel 25*a* VwVG), Zürich 2009, 22 ff.

92 Griffel (Fn. 90), § 3 N 60; Pierre Tschannen, Amtliche Warnungen und Empfehlungen, ZSR 118/1999, S. 412.

reich des Datenschutzrechts dürfte unzweifelhaft sein, dass das Erteilen der gesetzlich vorgesehenen Auskunft durch eine Behörde aufgrund des Auskunftsbegehrens einer betroffenen Person (Art. 25 revDSG) als tatsächliches Verwaltungshandeln zu qualifizieren ist.[93] Nichts anderes kann für das Erteilen von Informationen in einer Datenschutzerklärung gelten, zumal die Informationspflicht und das Auskunftsrecht demselben Zweck dienen, die zu vermittelnden Informationen sich inhaltlich teilweise entsprechen und der wichtigste Unterschied allein darin besteht, dass das Auskunftsrecht auf einem «Pull-Mechanismus» und die Informationspflicht auf einem «Push-Mechanismus» beruht.[94] Als Realakte entfalten Datenschutzerklärungen von Behörden keine unmittelbaren Rechtswirkungen.

3. Publikationsort

Der Publikationsort einer Datenschutzerklärung ist nach Sinn und Zweck des Grundsatzes der Transparenz so zu wählen, dass die betroffenen Personen möglichst niederschwellig Zugang zur Datenschutzerklärung haben. Damit bietet sich eine Veröffentlichung auf der Webseite der zuständigen Behörde an. Im Sinne der einfachen Auffindbarkeit ist ein verlinkter Hinweis auf der Einstiegsseite der Behörde oder im «Footer»[95] der Webseite zu fordern. Ein *layered approach*,[96] wie er von Unternehmen teilweise verwendet wird, erscheint auch bei Datenschutzerklärungen von Behörden sinnvoll.

Für Einheiten der zentralen Bundesverwaltung, der kantonalen und der kommunalen Verwaltungen wäre zu überlegen, ob für verschiedene Datenbearbeitungen die Datenschutzerklärungen (zusätzlich) gebündelt an einer zentralen Stelle (z.B. auf der Webseite des jeweiligen Bundesamtes oder Generalsekretariats oder des Kantons bzw. der Gemeinde) publiziert werden sollen. Für die Bundeskanzlei gelten analoge Erwägungen. Für Einheiten der dezentralen Bundesverwaltung und externe Träger von Verwaltungsaufgaben könnte es mit Blick auf die einfache Auffindbarkeit ebenfalls angebracht sein, die Datenschutzerklärungen – zusätzlich zur Publikation auf der eigenen Webseite – an zentraler Stelle zugänglich zu machen.

---

93 Siehe dazu Monique Sturni, in: Baeriswyl/Pärli (Hrsg.) (Fn. 23), N 3 zu Art. 25 DSG; Waldmann/Bickel (Fn. 38), § 12 N 155.

94 Siehe dazu Kap. B.II.2.

95 Der «Footer» einer Webseite ist der (meist in kleiner Schrift dargestellte) optische Abschluss einer Webseite; er enthält typischerweise Angaben zum Betreiber der Webseite (Impressum), zu dessen Adresse und Telefonnummer und Links auf die Nutzungsbedingungen (AGB) und die Datenschutzerklärung.

96 Siehe dazu Kap. F.II.

4. Nutzen

Für die Behörden bietet die Verwendung von Datenschutzerklärungen grössere Flexibilität, weil diese Erklärungen dank der Formungebundenheit ungleich einfacher angepasst werden können als Gesetze und Verordnungen. Dies würde es Behörden erlauben, die Bearbeitung von Personendaten laufend an Veränderungen in den äusseren Verhältnissen anzupassen und über diese Anpassungen umgehend in ihren Datenschutzerklärungen zu informieren. Zwar müssen sich die Veränderungen in den Datenbearbeitungen wegen des Legalitätsprinzips immer innerhalb des von der gesetzlichen Grundlage vorgegebenen Rahmens bewegen; dieser Rahmen kann aber, wie vorstehend ausgeführt,[97] recht offen gefasst werden. Während eine eher abstrakt gehaltene gesetzliche Regelung dem Legalitätsprinzip ohne weiteres zu genügen vermag, ist eine solche Regelung kaum geeignet, die gesetzlich geforderte Transparenz zu schaffen.

Für die betroffenen Personen hätte die Verwendung von Datenschutzerklärungen den grossen Vorteil, dass diese Erklärungen hinreichend konkrete Informationen enthalten und adressatengerecht formuliert werden könnten, sodass die Betroffenen auch wirklich verstehen, welche Daten von welchen Behörden zu welchen Zwecken bearbeitet werden. Aus diesem Grund sieht das europäische Datenschutzrecht denn auch vor, dass Transparenz in verständlicher Sprache zu schaffen ist. Namentlich hält Art. 12 Abs. 1 DSGVO ausdrücklich fest, dass «alle Mitteilungen (…) in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln» sind.[98] Auch der erläuternde Bericht zur Konvention 108+ des Europarats hält fest: «The information presented should be easily accessible, legible, understandable and adapted to the relevant data subjects».[99] Diese Vorgaben des europäischen Rechts machen deutlich, dass das datenschutzrechtlich zentrale Ziel der Transparenz durch eine Regelung der Datenbearbeitungen in Gesetzen und Verordnungen kaum zu erreichen ist. Ein Paradigmenwechsel weg vom Schaffen einer vermeintlichen Transparenz durch die Information in Gesetzen und Verordnungen hin zum Schaffen echter Transparenz durch die Verwendung von Datenschutzerklärungen wäre damit im Interesse aller Beteiligten – der Behörden ebenso wie der betroffenen Personen. So könnte beispielsweise für das Portal E-ZIVI eine allgemeine Datenschutzerklärung mit leicht verständlichen Informationen für alle im System geführten Personen vorgesehen und durch spezifische Merkblätter mit ausführlicheren Informationen für einzelne Anwendungsformen ergänzt werden.

---

97 Siehe dazu Kap. B.I.3.

98 Siehe dazu auch Cottier (Fn. 14), S. 68.

99 Convention 108+, Explanatory Report, N 68, abrufbar unter: ‹https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1› (zuletzt besucht am 16. Dezember 2021).

G. Erkenntnisse

Die Bearbeitung von Personendaten durch Bundesorgane muss auch unter dem revidierten Datenschutzrecht einer Reihe von Vorgaben genügen. Dasselbe gilt für das kantonale Recht. Das Erfordernis der gesetzlichen Grundlage und der Grundsatz der Transparenz sind dabei von zentraler Bedeutung. Für die Datenbearbeitung durch Behörden wurde bisher stets versucht, beiden Vorgaben «auf einen Schlag» – genauer: in einer Rechtsgrundlage – zu genügen, indem die Regelung der Datenbearbeitung in einem Gesetz oder in einer Verordnung nicht nur eine hinreichend bestimmte gesetzliche Grundlage bilden, sondern zugleich die Transparenz der Datenbearbeitung sicherstellen sollte.

Transparenz über die Datenbearbeitung von Behörden muss aber keineswegs zwingend über die Regelung in einem Erlass hergestellt werden. Durch die Umsetzung der Anforderungen an die Transparenz in der gesetzlichen Grundlage werden vielmehr zwei datenschutzrechtliche Grundsätze vermischt, die verschiedenen, komplementären Zielen dienen und auseinandergehalten werden sollten. Denn der Versuch, beide Anforderungen in einer einzigen Rechtsgrundlage zu erfüllen, kann sich doppelt negativ auswirken: Zum einen führt der Blick auf das Erfordernis der Transparenz zu höheren Anforderungen an die Bestimmtheit der gesetzlichen Grundlage; zum andern hat der Bedarf nach einer allgemein gefassten und hinreichend flexiblen gesetzlichen Grundlage zur Folge, dass sich der gesetzlichen Regelung kaum entnehmen lässt, welche Personendaten die Behörden zu welchen Zwecken bearbeiten. Damit ist weder den betroffenen Personen noch den Daten bearbeitenden Behörden gedient.

Für die Einhaltung beider datenschutzrechtlicher Grundsätze wäre viel gewonnen, wenn die Gesetzgeber in Bund und Kantonen und die rechtsanwendenden Behörden künftig bestrebt wären, diese je separat mit jeweils passenden Mitteln zu verwirklichen: Das Erfordernis der gesetzlichen Grundlage durch eine hinreichend bestimmte Regelung der Datenbearbeitung in einem Gesetz oder einer Verordnung und das Erfordernis der Transparenz durch das Vermitteln von hinreichend detaillierten Informationen in einer geeigneten Form. Die Form steht den Behörden dabei frei, sie müssen die betroffenen Personen also keineswegs in einem Erlass über die Bearbeitung der Personendaten informieren.

Datenschutzerklärungen haben sich bei privaten Datenbearbeitern längst als Mittel der Wahl etabliert. Sie sind bestens geeignet, auch die Transparenz der Datenbearbeitungen durch Behörden zu gewährleisten. Gegenüber dem heutigen Ansatz hätte die Verwendung von Datenschutzerklärungen zwei entscheidende Vorteile: Für die Behörden bieten Datenschutzerklärungen eine grössere Flexibilität, weil diese Erklärungen dank der Formungebundenheit ungleich einfacher angepasst werden können als Gesetze und Verordnungen. Für die betroffenen Personen hätte die Verwendung von Datenschutzerklärungen den grossen Vorteil, dass diese Erklärungen hinreichend konkrete Informationen

enthalten und adressatengerecht formuliert werden können, sodass die Betroffenen auch wirklich verstehen, welche Daten von welchen Behörden zu welchen Zwecken bearbeitet werden.

Die Verwendung von Datenschutzerklärungen durch Behörden wäre ein Paradigmenwechsel. Der Ansatz hat aber das Potential, den entscheidenden Schritt weg von der heute oft nur dem Schein nach bestehenden zu einer echten Transparenz staatlicher Datenbearbeitungen zu schaffen.

Zusammenfassung

Behörden dürfen Personendaten nur bearbeiten, wenn eine gesetzliche Grundlage besteht. Diese allein reicht aber nicht aus, um das Vertrauen der Bürgerinnen und Bürger in die staatliche Datenbearbeitung zu gewährleisten. Das Schaffen von Transparenz ist hierfür unverzichtbar.

Bisher haben Behörden meist versucht, den Vorgaben der gesetzlichen Grundlage und der Transparenz «auf einen Schlag» zu genügen, indem die Regelung der Datenbearbeitung in einem Gesetz oder einer Verordnung zugleich die Transparenz der Datenbearbeitung sicherstellen sollte. Diese problematische Praxis wird im revidierten Datenschutzgesetz aufgenommen, indem die Pflicht zur Information der Betroffenen entfallen soll, wenn eine Datenbearbeitung gesetzlich vorgesehen ist. Da dies bei Datenbearbeitungen von Behörden stets der Fall ist, werden diese künftig nicht mehr verpflichtet sein, die Betroffenen über ihre Datenbearbeitungen zu informieren.

Die Transparenz der Datenbearbeitung kann damit nicht hergestellt werden. Denn in vielen Fällen werden die Betroffenen mangels Information durch die Behörden gar nichts von der Datenbearbeitung wissen und damit auch keinen Anlass haben, sich durch Konsultation von Gesetzen und Verordnungen genauer zu informieren. Hinzu kommt, dass die meisten Betroffenen kaum in der Lage sind, sich die relevanten Erlasse zu beschaffen und sich durch deren Lektüre ein konkretes Bild von der Datenbearbeitung zu verschaffen.

Abhilfe würden Datenschutzerklärungen von Behörden schaffen. Diese könnten adressatengerecht formuliert und auf einer Webseite zugänglich gemacht werden. Damit liesse sich sicherstellen, dass Bürgerinnen und Bürger wirklich verstehen, welche Daten von welchen Behörden zu welchen Zwecken bearbeitet werden.

Résumé

Les autorités ne peuvent traiter des données personnelles que s'il existe une base légale. Mais celle-ci ne suffit pas à elle seule à garantir la confiance des citoyens dans le traitement des données par l'Etat. Pour cela, il est indispensable de créer de la transparence.

Jusqu'à présent, les autorités ont généralement essayé de satisfaire «d'un seul coup» aux exigences de base légale et de transparence, en ce sens que la réglementation du traitement des données dans une loi ou une ordonnance devait en même temps garantir la transparence du traitement des données. Cette pratique problématique est reprise dans la loi révisée sur la protection des données, dans la mesure où l'obligation d'informer les personnes concernées doit être supprimée lorsqu'un traitement de données est prévu par la loi. Comme c'est toujours le cas pour les traitements de données effectués par les autorités, celles-ci ne seront plus tenues d'informer les personnes concernées de leurs traitements de données.

Cela ne permet pas d'assurer la transparence du traitement des données. En effet, dans de nombreux cas, les personnes concernées ne sauront rien du traitement des données, faute d'information de la part des autorités, et n'auront donc aucune raison de s'informer plus précisément en consultant les lois et les ordonnances. De plus, la plupart des personnes concernées ne sont guère en mesure de se procurer les actes législatifs pertinents et de se faire alors une idée concrète du traitement des données en les lisant.

Des déclarations de protection des données des autorités pourraient y remédier. Celles-ci pourraient être formulées de manière adaptée aux destinataires et être mises à disposition sur un site web. Cela permettrait de garantir que les citoyens comprennent vraiment quelles données sont traitées par quelles autorités et à quelles fins.