Voßkuhle/Eifert/Möllers
Grundlagen des Verwaltungsrechts

Band I und Band II

3. Auflage

Sonderdruck

C.H.BECK

§ 22 Umgang mit personenbezogenen Informationen und Daten

Marion Albers

Übersicht

A. Der Umgang mit personenbezogenen Informationen und Daten vor dem Hintergrund der Digitalisierung

Der Umgang mit Informationen und Daten gehört zu den Konstituenzien öffentlicher Verwaltung.[1] Soweit es sich um personenbezogene Informationen und Daten handelt, betrifft er – im Vergleich zur „Transparenz der Verwaltung und Informationszugangsfreiheit",[2] den „Informationsbeziehungen in und zwischen Behörden"[3] oder den „Informationsbeziehungen im europäischen Verwaltungsverbund"[4] – einen spezifischen Aspekt, der durch den Schutzbedarf der Personen gekennzeichnet wird, auf die die Informationen und Daten verweisen. Reichweite und Tiefe der darin eingeschlossenen Informationsbeziehungen und Rechtsbindungen machen den „Datenschutz" zu einer zentralen Materie des Verwaltungsrechts. Seine Genese war von der Vorstellung einer Steuerung der Verarbeitung personenbezogener Daten in abgrenzbaren, aus der unmittelbaren Verwaltungskommunikation ausgegliederten Großrechenanlagen geprägt.[5] Mittlerweile werden – neben den Kategorien der Handlung und Handlungsformen als Rechtsformen,[6] der Entscheidung, der Verfahren[7] und der Organisation[8] – Information, Wissen und Kommunikation als „elementarer Teil jeden Verwaltens überhaupt"[9] und als zentrale Grundkategorien des Verwaltungsrechts begriffen.[10] Die dadurch veränderten Perspektiven geben Anlass für ein neues Verständnis nicht nur der traditionellen Kategorien, etwa der rechtsrelevanten Entscheidungen oder der Grenzen und internen Struktur eines Verfahrens, sondern auch der Entscheidungsprobleme überhaupt.[11] „Datenschutz" meint das **Recht des Umgangs mit personenbezogenen Informationen und Daten.** Es muss in **übergreifende Konzepte** eingebettet werden, die die Kategorien **Kommunikation, Wissen, Informationen** und **Daten** auf einer **Grundlagenebene in das Recht integrieren,** die Auswirkungen auf andere rechtliche Grundbegriffe sowie die daraus resultierenden **Innovationserfordernisse** beachten, kommunikations- oder informationsbezogene Normen 1

[1] → Bd. I *Vesting* § 20 Rn 1. ff.

[2] → Bd. I *Gusy* § 23.

[3] → Bd. I *Wischmeyer* § 24.

[4] → Bd. I *v. Bogdandy/Hering* § 25.

[5] Zur Genese *Ralf-Bernd Abel*, Geschichte des Datenschutzrechts, in: Alexander Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 2.7 Rn. 1 ff.; *Spiros Simitis/Gerrit Hornung/Indra Spiecker gen. Döhmann*, Einleitung, in: dies. (Hrsg.), Datenschutzrecht: DSGVO mit BDSG, 2019, Rn. 1 ff. Grdl. zum ursprünglichen rechtlichen Konzept *Wilhelm Steinmüller u.a.*, Grundfragen des Datenschutzes: Gutachten im Auftrag des BMI, 1971, BTDrucks VI/3826, Anl. 1, bes. S. 36 ff.

[6] → Bd. II *Hoffmann-Riem/Bäcker*, § 32 Rn. 1 ff. mit Hinweisen auf den Modernisierungsbedarf; *Schmidt-Aßmann*, Ordnungsidee, 6. Kap. Rn. 34 ff.

[7] → Bd. II *Schmidt-Aßmann/Kaufhold* § 27, *Schneider* § 28.

[8] → Bd. I *Groß* § 15, *Jestaedt* § 16, *Wißmann* § 14, *Schuppert* § 17.

[9] *Johannes Masing*, Transparente Verwaltung: Konturen eines Informationsverwaltungsrechts, VVDStRL, Bd. 63 (2004), S. 377 (433).

[10] Etwa *Ino Augsberg*, Informationsverwaltungsrecht, 2014; *Tobias Mast*, Staatsinformationsqualität, 2020; → Bd. I *Britz/Eifert*, § 26 Rn. 1.

[11] S. auch *Thomas Vesting*, Nachbarwissenschaftlich informierte und reflektierte Verwaltungsrechtswissenschaft – „Verkehrsregeln" und „Verkehrsströme", in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Methoden, 2004, S. 253 (284 ff.).

aus den **Gesamtkontexten** heraus verstehen und so zu einer angemessenen Dogmatik gelangen.[12]

2 Die **Digitalisierung**[13] und die **„onlife"-Welt**[14] prägen die gegenwärtige Gesellschaft und bedingen eine fundamentale Transformation auch des Rechts. Angesichts der weltweiten Vernetzung von Rechnern und Netzwerken, insbesondere in Gestalt des Internets, und weltweiter Datenströme müssen die traditionellen territorialen Anknüpfungspunkte für den Geltungsbereich und die Geltungsreichweite gerade auch von Datenschutzrechtsregimen rekonzeptioniert werden.[15] Machtvolle und regulierungsbedürftige Intermediäre mit „datengetriebenen" Geschäftsmodellen[16], aber auch die dadurch und durch die Digitalisierung entstehenden Arrangements zwischen privaten und staatlichen Akteuren – etwa in den Feldern der Überwachung[17] oder der Weiterverwendung staatlicher Open Data – erfordern neue Blicke auf die das Recht durchziehende Unterscheidung von Staat und (Privat-)Gesellschaft und eine passende Ausgestaltung des Datenschutzrechts. Allgegenwärtige Datenverarbeitungen, wie sie das „Internet der Dinge" und das „Internet of Bodies" noch einmal steigern werden, führen zu einer umfangreichen „Datafizierung" alltäglicher Lebensvorgänge. Die automatisierte Verknüpfung und Analyse großer Datenmengen („Big Data") oder der Einsatz Künstlicher Intelligenz werfen unter anderem Fragen der Differenzierbarkeit von Daten nach Maßgabe unterschiedlicher Rechtsregime, der Datenqualität, der Transparenz und der Nachvollziehbarkeit der Abläufe und Ergebnisse auf.

3 Auf das in der Digitalisierung liegende Potenzial und auf den Regulierungsbedarf sucht die Europäische Union durch den „Aufbau eines **gemeinsamen europäischen Datenraums**", eine umfassende **Digitalstrategie** unter dem Leitbild **„Digitale Souveränität"**, eine **europäische Datenstrategie** und ein europäisches Konzept zur **Künstlichen Intelligenz** zu antworten.[18] Als „Rahmen für Vertrau-

[12] Wie hier → Bd. I *Vesting* § 20 Rn. 6 ff. Vgl. auch *Marion Albers*, Information als neue Dimension im Recht, Rechtstheorie, Bd. 33 (2002), S. 61 (bes. S. 86 ff.).

[13] „Digitalisierung" ist zu einem Bündelungsbegriff geworden, der weit über die ursprünglich informationstechnische Bedeutung hinaus auf den gesellschaftlichen, kulturellen oder ökonomischen Wandel zielt, der durch das binäre digitale Format, die dadurch erreichten Datenverarbeitungsmöglichkeiten, die Konvergenz und das Zusammenspiel verschiedenster Techniken, umfassende Vernetzungen und die neue Rolle von Daten, Informationen und Wissen entsteht. Zu einigen der Bedeutungsdimensionen *Felix Würkert/Anika Klafki/Tina Winter*, Digitalisierung und öffentliches Recht, in: dies. (Hrsg.), Digitalisierung und Recht, 2017, S. 1 (3 ff.); umfassend *Enrico Peuker*, Verfassungswandel durch Digitalisierung, 2020, S. 11 ff.

[14] *Mireille Hildebrandt*, Smart Technologies and the End(s) of Law, 2016, S. 1 ff.; s. auch *Luciano Floridi* (Ed.), The Onlife Manifesto, Being Human in a Hyperconnected Era, 2015.

[15] S. zur einschlägigen Rechtsprechung etwa *EuGH*, Urt. v. 6.10.2015 – C-362/14, Schrems I; Urt. v. 16.7.2020 – C-311/18, Schrems II, abrufbar unter http://curia.europa.eu. Außerdem *Raoul-Darius Veit*, Safeguarding Regional Data Protection Rights on the Global Internet – The European Approach under the GDPR, in: Marion Albers/Ingo Sarlet (eds.), Personality and Data Protection Rights on the Internet, 2022 (i. E.), S. 445 (446 ff.). Vgl. auch die differenzierte Sicht zur Entterritorialisierung bei *Matthias Cornils*, Entterritorialisierung im Kommunikationsrecht, VVDStRL Bd. 76 (2017), 391 (391 ff.).

[16] Hierzu etwa *Ioannis Katsivelas*, Das Geschäft mit der Werbung: Finanzierungsmechanismen, personalisierte Werbung und Adblocker, in: Marion Albers/ders. (Hrsg.) Recht & Netz, 2018, S. 207 (bes. 221 ff.).

[17] Dazu m. w. N. *Marion Albers*, Surveillance and Data Protection Rights: Data Retention and Access to Telecommunications Data, in: dies./Sarlet (Fn. 15), S. 69 (70 ff.).

[18] S. die Mitteilungen der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau eines gemeinsamen europäischen Datenraums" vom 25.4.2018, COM(2018) 232 final, „Gestaltung der digitalen Zukunft

en im digitalen Umfeld"[19] sind die datenschutzrechtlichen Vorschriften – die Datenschutz-Grundverordnung (DSGVO)[20], die durch die Datenschutzrichtlinie für Polizei- und Strafjustiz[21], durch die e-privacy-Richtlinie[22] und durch weitere sektorspezifische Rechtsakte ergänzt wird – ein wesentliches Element. In Abgrenzung dazu, aber in Einklang mit der doppelten Finalität der DSGVO[23] steht bei nicht-personenbezogenen Daten der freie Datenverkehr im Mittelpunkt[24]; „Personenbezogenheit" wird insoweit ein ausschlaggebendes Unterscheidungskriterium[25]. Das gilt auch mit Blick auf die Open Data-Konzepte, die darauf zielen, dass bestimmte Datensätze und Dokumente des öffentlichen Sektors in offenen, maschinenlesbaren, zugänglichen, auffindbaren und weiterverwendbaren Formaten zur Verfügung gestellt werden und im privaten Sektor, gegebenenfalls gebunden an Bedingungen, weiterverwendet werden dürfen.[26] Im Grundsatz soll dies innovative datenbasierte Geschäftsmodelle oder auch Forschungen, aber auch gemeinsame Government-to-Business-Datennutzungen etwa in den Feldern des Umweltschutzes oder der Mobilität ermöglichen. Grundlegende Vorgaben für den privaten Sektor enthalten die Vorschläge der Kommission zu digitalen Märkten[27], die eine Regulierung von Gatekeepern auch im Hinblick auf deren Umgang mit Daten einschließen, und zu digitalen Diensten[28], die Pflichten von Online-Plattformen betreffen, etwa auch hinsicht-

---

Europas" vom 19.2.2020, COM(2020) 67 final, „Eine europäische Datenstrategie" vom 19.2.2020, COM(2020) 66 final, sowie das Weissbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, vom 19.2.2020, COM(2020) 65 final, und den Verordnungsvorschlag für einen „Artificial Intelligence Act", COM (2021) 206 final.

[19] Mitteilung „Aufbau eines gemeinsamen europäischen Datenraums" (Fn. 18), S. 1.

[20] 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), ABl. 2016 L 119/1.

[21] RL 2016/680/EU des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 v. 4.5.2016, S. 89.

[22] RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABlEG L 201 (v. 31.7.2002), S. 37. Zur e-privacy-Verordnung s. den Vorschlag der Europäischen Kommission v. 10.1.2017, KOM(2017) 10 endg.; zum Entwurf des Rates v. 10.2.2021 s. das Dokument unter https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[23] → Rn. 39.

[24] S. dazu die VO 2018/1807/EU des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union vom 14.11.2018, ABl. L 303 (v. 28.11.2018), S. 59, und die Leitlinien der Kommission vom 29.5.2019, die insbesondere die Abgrenzung zu den Regelungen über personenbezogene Daten in der DSGVO betreffen, COM(2019) 250 final.

[25] Zum Fokus der Personenbezogenheit und daraus resultierenden Problemen → Rn. 15ff., 41.

[26] RL 2019/1024/EU des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. L 172 v. 26.6.2019, S. 56; zur Abgrenzung im obigen Zusammenhang s. Art. 2 Abs. 1 lit h zu deren Anwendungsbereich.

[27] Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) v. 15.12.2020, COM(2020) 842 final.

[28] Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG v. 15.12.2020, COM(2020) 842 final.

lich nutzergenerierter illegaler Inhalte oder der Algorithmen im Falle des Einsatzes von Empfehlungssystemen, sowie europäische Zusammenarbeitsmechanismen und ein Europäisches Gremium für digitale Dienste vorsehen. Zur europäischen Datenstrategie gehört der Vorschlag für eine Verordnung über europäische Daten-Governance.[29] Mit dessen Bestimmungen soll die Etablierung sektoraler Datenräume vorangetrieben werden, etwa ein europäischer Raum für Gesundheitsdaten. Betroffene Personen könnten Daten für benannte (Forschungs-)Zwecke mittels Einwilligung zur Verfügung stellen. In Ergänzung der Richtlinie über offene Daten zielt der Vorschlag auch auf die Erleichterung der Weiterverwendung besonders geschützter Daten unter bestimmten Bedingungen, zu denen z.B. technische Datenschutzkonzepte zählen. Datenmittlern, also Diensten für die gemeinsame Datennutzung, die auch im Sinne von „Datentreuhändern" operieren können, und datenaltruistischen Organisationen wird eine mit einer Rahmenregulierung zu ermöglichende Schlüsselrolle zuerkannt. Das gilt unter anderem im Hinblick auf die Gewährleistung der Datenschutzrechte involvierter Personen. All dies zeigt, wie weitreichend das Recht des Umgangs mit personenbezogenen Informationen und Daten in übergreifende Zusammenhänge einzubetten sowie mit anderweitigen Regelungen zu koordinieren ist und dass es seinerseits einer dynamischen Novellierung unterliegen muss.

I. Netzwerk von Grundkategorien

4 Datenschutz dient nicht dem Schutz von Daten, sondern dem Schutz von Personen.[30] Daten sind ein eigenständiger Anknüpfungspunkt; es kommt aber auch auf ihren Aussagegehalt im Ergebnis von Verarbeitungsprozessen und als Grundlage von Wissen oder Entscheidungen an. Bereits die gegenständlichen Anknüpfungspunkte des Datenschutzes erweisen sich als komplexes Netzwerk von Grundkategorien.

1. Informationen und Daten

5 Die Regelungen zum Umgang mit personenbezogenen Informationen und Daten behandeln Informationen und Daten bisher meist als Synonyme. Darin steckt keine reflektierte Regelungsentscheidung. Erst und nur mit Hilfe der **Unterscheidung von Informationen und Daten** kann man die auf den „Daten"-Schutz betroffener Personen ausgerichteten Regelungen in der nötigen Weise in übergreifende Konzepte eingliedern.[31] Auch die Schutzerfordernisse erschließen sich erst dann in vollem Umfang, wenn man an die Unterscheidung von Informationen und Daten anknüpft oder sie zumindest im Hintergrund mitdenkt.[32]

---

[29] Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) v. 25.11.2020, COM(2020) 767 final; s. auch das Ratsdokument v. 24.9.2021, https://data.consilium.europa.eu/doc/document/ST-12124-2021-INIT/en/pdf.

[30] *Simitis/Hornung/Spiecker gen. Döhmann*, Einleitung (Fn. 5), Rn. 2ff. zur Geschichte des Begriffs „Datenschutz".

[31] → Rn. 1ff. Zum Erfordernis der Unterscheidung von Informationen und Daten s. auch *Marion Albers*, Informationelle Selbstbestimmung, 2005, S. 87ff., 141ff.

[32] Zu Schutzerfordernissen vgl. noch → Rn. 21, 25ff., 32ff.

Daten erfassen bei abstraktem Ausgangspunkt[33] ein weites Spektrum: Unterscheidbarkeit von Gegebenheiten in der Wirklichkeit, nach Messeinheiten gemessene physikalische Werte, Zahlen, Buchstaben, Texte, Kommunikationselemente oder binäre digitale Einheiten. Die Heterogenität dieser nicht abschließenden Aufzählung verdeutlicht, dass der Begriff des Datums eine Konstruktion ist, die sich je nach historischer Epoche, je nach Perspektive und je nach Rahmen unterschiedlich gestaltet.[34] Das Datenschutzrecht knüpft, schon um die Breite an Regelungs- und Fallkonstellationen zu erfassen, an verschiedenartige Beschreibungsmuster an, greift sie aber in rechtsspezifischer Weise auf und reformuliert sie aus dem rechtlich begründeten Schutzbedarf heraus. In seinem Mittelpunkt stehen Zeichen oder Zeichengebilde[35], die in einem bestimmten Format auf einem Datenträger gespeichert sind und in sozialen Kontexten informationelle Bedeutung gewinnen können. Das ist aus mehreren Gründen nicht isoliert zu verstehen. Erstens ist die Verweisungsfunktion von Daten auf eine potenzielle informationelle Bedeutung abstrakt zu verstehen; sie heißt nicht, dass mit den Daten feststehende intrinsische Bedeutungen verknüpft wären.[36] Der konkrete Bedeutungs- oder Informationsgehalt wird vielmehr durch interpretative Leistungen im Kontext und unter den sich darüber ergebenden Rahmenbedingungen immer erst erzeugt. Gerade deshalb sind Daten zweitens weniger als einzelnes Datum von Bedeutung, sondern verweisen auf Datenverarbeitungsprozesse, Datenarchitekturen oder Wissensspeicherformen, wie sie durch die Medien, Infrastrukturen und Techniken geprägt werden. Damit kann man vor dem Hintergrund komplexer digitalisierter Verarbeitungsprozesse drittens auch „virtuelle Daten"[37] rechtlich miterfassen und Daten von der potentiellen informationellen Bedeutung in bestimmtem Umfang entkoppeln: Sie können auch dann als abgegrenzte Entitäten identifiziert und zum Gegenstand des Rechts werden, **6**

[33] Von der etymologischen Wurzel her sind „Daten" etwas „Gegebenes". Entsprechend und vor dem Hintergrund seiner Erkenntnisinteressen sinnvollerweise abstrakt ist der Ausgangspunkt bei *Luciano Floridi*, Information. A Very Short Introduction, 2010, S. 23: „[...] the general definition of a datum is: Dd) datum = $_{def}$ x being distinct from y, where x and y are two uninterpreted variables and the relation of 'being distinct', as well as the domain, are left open to further interpretation."

[34] S. auch *Rob Kitchin*, The Data Revolution, 2014, S. 2 ff.; *Daniel Rosenberg*, Data before the Fact, in: Lisa Gitelman (ed.), "Raw data" is an oxymoron, 2013, S. 33 (36). Zum Konstruktionscharakter statt vieler *Sabina Leonelli*, The Philosophy of Data, in: Luciano Floridi (ed.), The Routledge Handbook of Philosophy of Information, 2016, S. 192 (192 ff.).

[35] Zu Relationalität und Verweisungsfunktion von Zeichen vgl. *Charles W. Morris*, Foundations of the theory of signs, 1938; *Umberto Eco*, Zeichen. Einführung in einen Begriff und seine Geschichte, 1977, S. 25 ff. Daten und Zeichen sind nicht deckungsgleich. Unabhängig davon gehen die unterschiedlichen theoretischen Ansätze zum Zeichenbegriff erheblich über die obigen basalen Aussagen hinaus. Enger als hier → Bd. I *Vesting* § 20 Rn. 14 ff. mit einer Beschränkung des Begriffs der „Daten", die im Kontext des Datenschutzrechts zu eng ist.

[36] S. auch → Bd. I *Vesting* § 20 Rn. 14 ff Im Akzent anders, dies auch wegen eines anderen Ausgangspunktes beim Datenbegriff *Giselher Rüpke/Kai von Lewinski/Jens Eckhardt*, Datenschutzrecht, 2018, § 3 Rn. 26 ff.; *Jan-Niklas Bunnenberg*, Privates Datenschutzrecht, 2020, S. 209 ff.

[37] Damit sind gar nicht irgendwie verkörperte Daten „zwischen" bestimmten Phasen der Verarbeitungsprozesse gemeint, s. *Marcus Burkhardt*, Digitale Datenbanken. Eine Medientheorie im Zeitalter von Big Data, 2015, S. 202, der insoweit von „virtuellen Informationen" spricht. Unabhängig davon, dass man Daten gegen Informationen, Operationen und Programme abgrenzen muss und die Erfassung einer Generierung von Daten aus Daten rechtlich unproblematisch ist, kann es in komplexeren rechnergestützten Programmabläufen unter bestimmten Umständen auch aus rechtlicher Sicht Sinn machen, Daten „zwischen" Datenverarbeitungsphasen herauszukristallisieren.

wenn sie überhaupt nur in Verbindung mit weiteren Daten oder Verarbeitungsprozessen zur Erzeugung von Informationen beitragen. Ganz ohne diesen Bezugspunkt fehlt jedoch die datenschutzrechtliche Relevanz.

7 **Informationen** sind – im Rahmen eines bereits auf soziale Systeme und rechtliche Perspektiven zugeschnittenen Verständnisses[38] – **Sinnelemente,** die in einem bestimmten sozialen Kontext als Inhalt von Beobachtungen, Mitteilungen oder Daten mit Hilfe einer Interpretationsleistung erzeugt und dann genutzt werden.[39] Aus der beständig laufenden Reproduktion von Sinn werden sie mit Hilfe von Relevanzkriterien herausgehoben. Informationsgehalt kommt aber nicht nur Neuigkeiten zu, sondern auch den Angaben, die eine Erwartung bestätigen, Wissen aktualisieren oder die routinemäßig abgearbeitet werden können.[40] Indem Informationen eine **Deutungsleistung** voraussetzen, die **im jeweiligen Kontext** und in Abhängigkeit von den je situativen Interpretationsbedingungen erfolgt, verweisen sie auf die Strukturen und Prozesse, in deren Rahmen sie sich bilden und weitergeführt werden. Daten und Informationen sind also vor allem deshalb keine Synonyme, weil Daten als Informationsgrundlagen zwar Informationen vermitteln, diese aber weit mehr voraussetzen als nur Daten. Informationen kann man nicht beschreiben, ohne in übergreifender Perspektive neben den Informationsgrundlagen Wissensstrukturen, Umsetzungsprozesse und den weiteren Kontext mitzubeobachten, in dem sie entstehen.

2. Die Strukturdimension: Das Wissen der Verwaltung

8 Auch wenn das Datenschutzrecht Daten als zentralen Anknüpfungspunkt hervorhebt, spielen in der Strukturdimension **Wissen** als **Faktor und Produkt des Kontexts,** in dem sich der Umgang mit Informationen und Daten vollzieht, und **Wissensspeicherformen** eine zentrale Rolle.[41] Wissen **ermöglicht** die **Deutungsleistungen,** weil ohne ein in irgendeiner Hinsicht bereits vorhandenes Wissen die Interpretation von Daten nicht möglich wäre, und **begrenzt** die **Deutungsmöglichkeiten,** indem es der Vielzahl theoretisch denkbarer Interpretationen Grenzen setzt.[42] Die Beteiligung des Wissens an dem Bild, das sich die Verwaltung von einem Sachverhalt oder von einer Person macht, erhellt beispielsweise schnell, dass auch fehlende Daten Informationsqualität gewinnen und Entscheidungen beeinflussen können.[43] Deswegen sind pauschale Strategien der Minimierung von Daten verfehlt.

---

[38] Zur Diskussion darum, ob es ein einheitliches begriffliches „Ur-Konzept" geben kann, *Luciano Floridi,* Information, in: ders. (Hrsg.), The Blackwell guide to the philosophy of computing and information, 2004, S. 40 (40 ff.).

[39] *Albers,* Information (Fn. 12), S. 67 ff.

[40] In diesem Punkt anders: → Bd. I *Vesting* § 20 Rn. 18, 20. Aus der Praxis vgl. *BVerwG,* NJW 2005, S. 2330 (2331).

[41] Zum Wissensverständnis *Niklas Luhmann,* Die Wissenschaft der Gesellschaft, 1. Aufl. 1990, S. 137 ff.; *Helmut Willke,* Systemisches Wissensmanagement, 2. Aufl. 2001, S. 11; treffend und umfassender auch *Hans-Heinrich Trute,* Wissen – Einleitende Bemerkungen, in: Hans C. Röhl (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, DV, Beiheft 9, 2010, S. 11 ff. Vgl. auch mit teilweise anders ansetzenden Überlegungen → Bd. I *Vesting* § 20 Rn. 26 ff.

[42] Wissen ist wegen seiner Eigenständigkeit mehr als „verarbeitete" oder „organisierte" Information.

[43] Mit Hilfe des (Vor-)Wissens können etwa Informationslücken mittels Annahmen oder Unterstellungen aufgefüllt werden.

So wie man Informationen und Daten unterscheiden muss, sind Wissen und dessen **Speicherformen** zu unterscheiden. Einerseits ist Wissen als Struktur vielschichtig, andererseits kann es im Ansatz immer nur selektiv in der jeweiligen Interpretationssituation aufgebaut werden.[44] Explizites Wissen muss aktiviert, implizites Wissen aktualisiert werden. Speicherformen, auf die unter Inanspruchnahme von Zeit und mit Hilfe von Auswahlentscheidungen zurückgegriffen werden kann, sind nicht das Wissen selbst, sondern **Wissensgrundlagen.**[45] Immer schon zählen in der Verwaltung dazu Texte, Akten, Archive, Register, aber auch institutionelle Arrangements, strukturierte Verfahrensabläufe oder rechtsdogmatische Praktiken.[46] Mit der Digitalisierung gewinnen Datenbanken, Expertensysteme und eigenständig lernende Programme an Bedeutung.[47] Neben einem „Wissen zweiter Ordnung",[48] also einem Wissen, wie man Wissen generiert, und einem Wissensmanagement wird auch ein Management des Umgangs mit Künstlicher Intelligenz erforderlich. 9

Wissen ist in den übergreifenden sozialen Kontexten zirkulär mit Handeln und Entscheiden verknüpft, so dass es diesen nicht allein vorausgeht und sie erklären oder begründen kann, sondern umgekehrt auch Handlungsmuster und die daraus resultierenden kognitiven Schemata das aktualisierte Wissen und die Sinnerzeugung mitprägen.[49] Nicht nur die Regeln und Muster, die unmittelbar die Informationserzeugung oder die Gestaltung und Nutzung von Speicherformen betreffen, auch die für die Verwaltung in Rechtsnormen verankerten sachlichen Kompetenzen und das darauf bezogene Verständnis leiten die Wissensproduktion.[50] Diese beeinflusst wiederum das Verständnis und die Wahrnehmung jener.[51] Die Verwaltung muss sowohl das administrative Ent- 10

[44] In der jeweiligen Situation kann nicht das gesamte Wissen, das (aus einer Beobachtungsperspektive) zur Verfügung stehen könnte, vergegenwärtigt werden. Wissen lässt sich deshalb nicht als Bestand und auch nicht als Vorrat von Erkenntnissen begreifen, vgl. auch *Peter Collin/Thomas Horstmann*, Das Wissen des Staates – Zugänge zu einem Forschungsthema, in: dies. (Hrsg.), Das Wissen des Staates, 2004, S. 9 (13).

[45] Die Differenzierung ist nötig, auch wenn das Wissen „mediale Möglichkeitsbedingungen" hat, vgl. dazu *Thomas Drepper*, Organisation und Wissen, in: Rainer Schützeichel (Hrsg.), Handbuch Wissenssoziologie und Wissensforschung, 2007, S. 588 (608).

[46] Vgl. *Helmut Willke*, Supervision des Staates, 1997, S. 23. Außerdem → Bd. I *Ladeur* § 21 Rn. 1 ff.

[47] Zu Datenbanken s.a. → Bd. I *Wischmeyer* § 24 Rn. 90 ff. Zu Datenbanken als soziotechnischen Systemen *Eric Töpfer*, Verheddert im Netz der DNA-Datenbanken. Prüm und die Mythen der Interoperabilität, in: Michael Plöse/Thomas Fritsche/Michael Kuhn/Sven Lüders, „Worüber reden wir eigentlich?" Festgabe für Rosemarie Will, Berlin, 2016, S. 809 (809 ff.); *Niklas Creemers*, Über Datenbanken und Datenanalysetools, in: Jonas Grutzpalk (Hrsg.), Polizeiliches Wissen, 2016, S. 101 (108 ff.).

[48] Vgl. *Nina Degele*, Informiertes Wissen, 2000, bes. S. 77 ff.

[49] *Petra Hiller*, Organisationswissen, 2005, S. 13 ff.

[50] Vgl. auch *Hansjürgen Garstka*, Zur Wissensordnung der Informationsverarbeitung – Plädoyer für ein allgemeines Informationsgesetz, in: Jürgen Taeger/Andreas Wiebe (Hrsg.), Informatik – Wirtschaft – Recht, 2004, S. 189 (191 f.): Das Rechtssystem ist selbst ein System aufeinander bezogener, normativer Informationen, eine Wissensordnung eigener Art. Analytisch muss man dieses mittels gespeicherter Normen begründete Wissen allerdings von dem mit seiner Hilfe produzierten sachverhaltsbezogenen Wissen unterscheiden, auch wenn sich beide Arten wechselseitig beeinflussen. Zur Rolle der Rechtsdogmatik etwa *Laura Münkler*, Wissen – ein blinder Fleck des Rechts?, in: dies. (Hrsg.), Dimensionen des Wissens im Recht, 2019, S. 3 (10 ff.). Zur Verknüpfung der Tatbestände und dogmatischen Figuren am Beispiel des Polizeirechts *Carsten Kremer*, Ungewissheit im Sicherheitsverwaltungsrecht, in: Ino Augsberg (Hrsg.), Extrajuridisches Wissen im Verwaltungsrecht, 2013, S. 195 (200 ff.).

[51] Vgl. auch *Ino Augsberg*, Multi-, inter-, transdisziplinär?, in: ders. (Fn. 50), S. 3 (9: Sachverhaltsfeststellung und Normkonkretisierung werden rekursiv miteinander verknüpft).

scheidungsprogramm als auch das für die Umsetzung erforderliche Wissen erarbeiten, und dies gestaltet sich zunehmend anspruchsvoll[52] und mittels eigenständiger sektorabhängiger Regeln der Wissensgenerierung.[53] Man benötigt hier insgesamt angemessene Konzepte des Organisationswissens und der Wissensgenerierung, die auch im Wechselspiel mit dem Datenschutz auszuarbeiten sind.

3. Die Prozessdimension: Verarbeitungsabläufe und -netze

11 Im Rahmen eines abgegrenzten Kontexts kann man in der Prozess- oder Zeitdimension **verschiedene Phasen** des Umgangs mit Daten und Informationen unterscheiden. Art. 4 DSGVO stellt den Begriff der Verarbeitung in den Mittelpunkt, so dass sich Verarbeitungsphasen relativ zu den jeweiligen Verarbeitungszusammenhängen ergeben. Datenverarbeitungsphasen verlaufen nicht notwendig linear und können faktisch, wie es zunehmend der Fall ist, weitgehend voneinander entkoppelt werden. Informationen bewegen sich im Rahmen von Prozessen, indem aus Informationen bei einem Abgleich mit Wissen neue Informationen erzeugt, Datenverarbeitungen zwischengeschaltet und Informationen in Entscheidungen oder Handlungen umgesetzt werden. Im Ergebnis können sehr komplexe Abläufe und Netze einer Verwobenheit von Informationen und Daten entstehen. Verarbeitungszusammenhänge, die Verarbeitungsphasen in spezifischer Weise verbinden, werden immer erst im Kontext hergestellt, dies auch nach Maßgabe rechtlicher Gestaltung.

12 Prozesse der Informations- und Datenverarbeitung können sachlichen Entscheidungen funktional zugeordnet werden. In Verwaltungsverfahren sind sie konstituierendes Element (ohne dass sie sich darin oder Verwaltungsverfahren sich in ihnen erschöpften)[54], und umgekehrt bieten die jeweiligen Verfahren den Rahmen für die Selektion und für die Produktion von Informationen. **Informations- und Datenverarbeitungsprozesse** sind deshalb eng mit dem **Verfahrenstypus** und den dahinter stehenden **sachlichen Aufgaben und Befugnissen** verknüpft. Sie müssen sich etwa bei Planungsverfahren, die durch eine umfassende Abwägung aller involvierten öffentlichen und privaten Belange gekennzeichnet sind, oder bei Strategien der Risikobewältigung anders gestalten als bei punktuellen ordnungsbehördlichen Entscheidungen. Verwaltungsverfahren können auf Zwischen- oder Abschlussentscheidungen, aber auch auf die Produktion von Wissen ausgerichtet sein und in Teilprozesse mit unterschiedlichen Funktionen oder in zeitliche Abschnitte differenziert werden.[55] Verfahren der Wissensgenerierung sind, wie der Blick auf verschiedene Regelungsfelder zeigt, mehr oder

[52] *Augsberg*, Multi-, inter-, transdisziplinär? (Fn. 51), S. 9 ff.

[53] S. auch → Bd. I *Vesting* § 20 Rn. 8 ff und → Bd. II *Röhl* § 30 Rn. 15 ff. zu den Verfahren der Wissensgenerierung. Übergreifender ansonsten *Burkard Wollenschläger*, Wissensgenerierung im Verfahren, 2009; *Indra Spiecker gen. Döhmann*, Wissensverarbeitung im Öffentlichen Recht, Rechtswissenschaft 2010, S. 247 (261 ff.); *Katharina Reiling*, Der Hybride. Administrative Wissensorganisation im privaten Bereich, 2016. Mit Blick auf Referenzgebiete *Roland Broemel*, Wissensgenerierung im Regulierungsverfahren, in: Münkler (Fn. 50), S. 139 (139 ff.); *Benjamin Rusteberg*, Wissensgenerierung in der personenbezogenen Prävention, in: Münkler (Fn. 50), S. 233 (233 ff.); und die Beiträge in *Benedikt Buchner/Karl-Heinz Ladeur* (Hrsg.), Wissensgenerierung und -verarbeitung im Gesundheits- und Sozialrecht, 2016.

[54] Zum Verständnis des Verwaltungsverfahrens → Bd. II *Schmidt-Aßmann/Kaufhold* § 27 Rn. 45 ff., *Schneider* § 28 Rn. 1 ff.

[55] → Bd. II *Schneider* § 28 Rn. 15 ff.

weniger komplex und im Umbau.[56] Sie können unter Umständen von sachlichen Aufgaben relativ entkoppelt werden, ohne dass eine vollständige Herauslösung aus jeglichen Aufgabenbezügen möglich wäre. Die beschriebenen Zusammenhänge verweisen auf zentrale Probleme des Datenschutzrechts, nämlich wie man es angemessen mit den sachlichen Aufgaben und Regelungsstrukturen abstimmt[57] und wie man das Verhältnis zwischen allgemeinen und bereichsspezifischen Regelungen gestalten kann.[58]

4. Kommunikations- und Datenverarbeitungsinfrastrukturen und -techniken

Medien, Infrastrukturen und Techniken prägen den Umgang mit Informationen und Daten und sind umgekehrt selbst in soziale Zusammenhänge und Praktiken eingebettet. **Datenschutz** war **ursprünglich** eine **Reaktion auf die Techniken automatisierter Datenverarbeitung.** Sie waren dessen Auslöser, allerdings nicht der ausschließliche Grund. Nach dem breiter ansetzenden Volkszählungsurteil des BVerfG[59] dehnte sich der Anwendungsbereich des deutschen Datenschutzrechts für die Datenverarbeitung öffentlicher Stellen auf anderweitige Formen des Umgangs mit personenbezogenen Informationen und Daten aus.[60] Die **gegenstandsbedingte Relevanz der Infrastrukturen und Techniken** ist dennoch offensichtlich. Deren **Weiterentwicklung** und die damit verbundenen **Veränderungen sozialer Beziehungen,** die mit den Schlagworten „Digitalisierung" und „Künstliche Intelligenz" umrissen werden[61], transformieren das Datenverständnis und Datenformate, Rechner- und Programmarchitekturen, Prozesse der Informations- und Wissensgenerierung oder Verarbeitungsabläufe und die damit verbundenen Zeitkonstruktionen erneut in grundlegender Weise. Aus Sicht des Datenschutzes sind die Gefährdungspotenziale einerseits explodiert; andererseits lässt sich dieser gerade auch durch Technik realisieren.[62] Zu den relevanteren Herausforderungen gehört, dass neue datengetriebene Formen der Informations- und Wissensgenerierung auf Kernprinzipien wie dasjenige der Zweckbindung[63] prallen. **13**

5. Digitalisierte Verwaltung

Die **Verwaltung als Kommunikationssystem** ist, soweit man sich in verwaltungsrechtlichen Zusammenhängen bewegt, die zentrale Bezugsebene hinsichtlich des Umgangs mit personenbezogenen Informationen und Daten.[64] Es zählt zu dessen wesentlich mitprägenden Faktoren, wie sich die maßgeblichen tatsächlichen und rechtlichen Strukturen der Aufgabenerfüllung gestalten, wie die **14**

---

[56] → Bd. I *Vesting* § 20 Rn. 50 ff.; *Rahlf*, Hybride (Fn. 53), S. 17 ff.

[57] → Rn. 67.

[58] → Rn. 63 ff.

[59] *BVerfGE* 65, 1.

[60] → Rn. 37.

[61] → Rn. 2.

[62] Näher noch → Rn. 77 ff.

[63] Zur Zweckbindung → Rn. 83 ff.

[64] In Kommunikationssystemen bilden sich Informationen – statt „im Kopf", vgl. *Matthias Rossi*, Informationszugangsfreiheit und Verfassungsrecht, 2004, S. 19 – als eigenständiges Element der Kommunikation.

Verwaltungsverfahren ablaufen und Entscheidungen getroffen werden, wie die Verwaltung organisiert ist oder wie sie nach außen kommuniziert. Der Umbau zu einer **digitalisierten Verwaltung**[65] wird zu einem deutlichen Wandel führen. Bisher wird er etwa mit der E-Government-Gesetzgebung, Onlinezugängen zu Verwaltungsleistungen und deren Vernetzung durch Portallösungen oder der Umstellung auf eine digitalisierte Aktenführung nur in begrenztem Umfang realisiert.[66] Weitergehende Formen der Automatisierung von Verwaltungsentscheidungen oder Möglichkeiten des Einsatzes Künstlicher Intelligenz, etwa in Gestalt des predictive policing, stehen aber bereits am Horizont, selbst wenn auch in diesem Zusammenhang gilt, dass soziale Praktiken die Umsetzung von Techniken mitbestimmen. Diese erfordern eine mit den bisherigen Vorschriften abgestimmte und zugleich partiell eigenständige Regulierung mittels allgemeiner oder sektor- oder technikspezifischer Vorgaben.[67] Ebenfalls einem deutlichen Wandel unterliegen die Verwaltung/Umwelt-Beziehungen zum Beispiel angesichts der Öffentlichkeitsarbeit der Verwaltung[68], unter anderem in Sozialen Medien[69], des internetvermittelten Zugangs zu Verwaltungsdokumenten über Transparenzportale oder der Open Data-Strategien mit den Möglichkeiten der Informationsweiterverwendung. All diese Umfeld- oder Kontextveränderungen führen zu neuen Anforderungen an das Recht des Umgangs mit personenbezogenen Informationen und Daten selbst und/oder an dessen Abstimmung mit anderweitigen Regelungen.

II. Der Fokus personenbezogener Informationen und Daten

15 Die **Personenbezogenheit** von Informationen und Daten ist in den datenschutzrechtlichen Regelungen und in den Abgrenzungen zu anderen Rechtsregimen das zentrale Kriterium.[70] Die besonderen Rechtsbindungen werden mit den **Schutzerfordernissen** der **Personen** begründet, auf die **Informationen und Daten** mit ihren Aussagegehalten **verweisen.**

---

[65] → Bd. I *Britz/Eifert* § 26; außerdem die Beiträge in *Margrit Seckelmann* (Hrsg.), Digitalisierte Verwaltung – Vernetztes E-Government, 2. Aufl. 2019; *Mario Martini*, Transformation der Verwaltung durch Digitalisierung, DöV 2017, S. 443 ff.

[66] Überblick über die Gesetzgebung bei *Hanno Kube*, E-Government: Ein Paradigmenwechsel in Verwaltung und Verwaltungsrecht, VVDStRL Bd. 78 (2019), S. 289 (294 ff.). Eine Beschreibung der Visionen und des ernüchternden Befunds findet sich bei *Annette Guckelberger*, E-Government: Ein Paradigmenwechsel in Verwaltung und Verwaltungsrecht?, VVDStRL Bd. 78 (2019), S. 235 (244 ff.).

[67] Zur Debatte *Guckelberger*, E-Government (Fn. 66), S. 262 ff.; *Yoan Hermstrüwer*, Fairnessprinzipien der algorithmischen Verwaltung: Diskriminierungsprävention beim staatlichen Einsatz von Machine Learning, AöR, Bd. 145 (2020), S. 479 (480 ff.); *Thomas Wischmeyer*, Regulierung intelligenter Systeme, AöR Bd. 143 (2018), S. 1 (18 ff.); *Timo Rademacher*, Predictive Policing im deutschen Polizeirecht, AöR 142 (2017), S. 365 (375 ff.); *Wolfgang Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 2017, S. 1 (2 ff.); *Hans-Heinrich Trute/Simone Kuhlmann*, Predictive Policing als Formen polizeilicher Wissensgenerierung, GSZ 2021, S. 103 (104 ff.). Übergreifender *Mario Martini*, Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, 2019, sowie die Beiträge in *Thomas Wischmeyer/Timo Rademacher* (Hrsg.), Regulating Artificial Intelligence, 2020.

[68] Übergreifend und grundlegend *Mast*, Staatsinformationsqualität (Fn. 10).

[69] Dazu etwa *Alfred G. Debus*, Verwaltung und soziale Medien, in: Seckelmann (Fn. 65), S. 473 Rn. 24 ff.; zur Nutzung von Social Media und daraus resultierenden Rechtsproblemen auch *Margrit Seckelmann*, Einsatz bei der Polizei: Twitter-Nutzung, Online-Streifen, Trojaner, Facebook-Fahndung, Biometriesoftware, (intelligente) Videoüberwachung, Predictive Policing, Body-Cams und Fotodrohnen, in: dies. (Fn. 65), S. 473 Rn. 24.

[70] Im europäischen Kontext → Rn. 3.

Personenbezogen sind, so die Legaldefinition in Art. 4 Nr. 1 DSGVO, Informationen und Daten, wenn sie sich auf eine **identifizierte oder identifizierbare** natürliche **Person** beziehen.[71] Angaben wie der persönliche Name und Daten, die regelmäßig damit verknüpft werden, etwa die Adresse, das Geburtsdatum, Familienstand, Sozialversicherungs- und Steueridentifikationsnummern, Angaben über Eigenschaften, Fingerabdrücke oder Portraitfotos sind illustrative Beispiele. Selbst in diesen überschaubaren Zusammenhängen wird freilich schnell klar, dass die Personenbezogenheit die Herstellung einer Beziehung zur betroffenen Person und oft auch den Schritt einer Verknüpfung bestimmter Daten mit Identifikationsdaten erfordert. Außerdem kann das Vor- oder Zusatzwissen es ermöglichen, Daten, die für sich genommen nicht ohne Weiteres zuordbar sind, mit einer bestimmten Person in Verbindung zu bringen. „Personenbezogenheit" ist also weder eine intrinsische Eigenschaft von Daten noch haftet sie ihnen wie ein Etikett an. Sie ist **Ergebnis einer sinngehaltszuschreibenden Leistung.** Zum einen muss beantwortet werden, welche Identifikatoren eine „Person" spezifizieren. Zum anderen gibt es im Ansatz ein sehr breites Spektrum von sachlichen Angaben, die mit einer Person verknüpft werden können und dann etwas über sie aussagen. Im Weiteren kommt hinzu, dass das Datenschutzrecht wegen seiner Schutz- und Steuerungsziele nicht erst und nur die Verarbeitungsschritte erfasst, bei denen eine unmittelbare Verknüpfung zwischen Daten und bestimmten Personen tatsächlich besteht. Solche Verknüpfungen, das dadurch entstehende Wissen über eine Person und dessen potenzielle Verwendung sollen gegebenenfalls gerade verhindert werden[72]. Möglichkeiten, dass im Laufe der Zeit mit zusätzlichen Verarbeitungsschritten oder in anderen Kontexten Verknüpfungen hergestellt werden, müssen daher in bestimmtem Umfang mitbedacht werden. Umgekehrt kann es nicht ausreichen, dass Daten von irgendwem irgendwann irgendwie mit einer Person verknüpft werden könnten, denn sonst wären sämtliche Daten als personenbezogen einzustufen; man landete bei einem „law of everything"[73]. Außerhalb reiner Identifizierungsdaten erfordert die Antwort auf die Frage, welche Daten sich auf eine Person beziehen, erstens (auch) eine Beschreibung der Qualität, die die Beziehung zwischen den Daten und der betroffenen Person haben muss, und zweitens eine Beschreibung der Kontexte, in denen sich der Umgang mit Daten und Informationen vollzieht. In beiden Hinsichten kommen wertende Beurteilungen und Wahrscheinlichkeitsannahmen oder auch Prognosen ins Spiel. Insofern ist die Personenbezogenheit weder in isolierter Betrachtung eines einzelnen Datums noch mit Blick auf die einzelne Information, sondern im übergreifenden Kontext, unter Umständen je nach Beziehung und Akteur relativ sowie mit Hilfe wertender Entscheidungen vor dem Hintergrund der Schutzgüter und -erfordernisse zu bestimmen. Der Kontext und damit die Personenbezogenheit lässt sich in bestimmtem Umfang durch rechtliche Regelungen gestalten. Trotzdem reicht das Datenschutzrecht mit dem Fokus der Personenbezogenheit weit.[74] Dieser Befund wird durch die zuneh- **16**

[71] Vgl. weiter EG 26.

[72] Vgl. auch *Tobias Herbst*, Was sind personenbezogene Daten?, NVwZ 2016, S. 902 (904).

[73] *Nadezhda Purtova*, The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation, and Technology 2018, DOI:10.1080/17579961.2018.1452176.

[74] Zur Weite des Begriffs „personenbezogene Daten" s.a. etwa *EuGH*, Rs. C-465/00, Slg. 2003, I-4989, Rn. 64 – Österreichischer Rundfunk; C-434/16; Urt. v. 19.10.2016 C-582/14, Rn. 32ff. – dyna-

mende „Datafizierung" aller Lebensbereiche ebenso verstärkt wie die Schwierigkeiten der Abgrenzbarkeit personenbezogener und nicht-personenbezogener Daten, die Verarbeitungsformen im Big-Data-Kontext oder Re-Identifikationsmöglichkeiten aufwerfen.[75]

17 Die Überlegungen zeigen, dass der Begriff der **Personenbezogenheit** den individuellen Schutzbedarf zum einen **nicht erschöpfend** beschreibt. Allein die Tatsache, dass Daten oder Informationen auf eine Person verweisen, kann jedenfalls keinen umfassend-pauschalen Schutz begründen. Die häufig zitierte Ausführung des Bundesverfassungsgerichts, es gebe „unter den Bedingungen der modernen Datenverarbeitung kein ‚belangloses Datum' mehr",[76] ist insofern richtig, als auch Daten, die für sich genommen belanglos erscheinen, in einem bestimmten Kontext oder in Verknüpfung mit anderen Daten einen Informationsgehalt erhalten können, mit Blick auf den eine Person schutzbedürftig ist. Das heißt aber nur, dass Daten nicht von vornherein aus dem Schutz herausfallen dürfen. Relativ zu einem bestimmten Kontext ist eine Beschreibung personenbezogener Daten und Informationen oder von Verarbeitungsvorgängen als „trivial" oder „belanglos" ebenso möglich wie die Feststellung eines gesteigerten Schutzbedarfs. Das eigentliche Problem liegt woanders: Daten können theoretisch in beliebige Kontexte fließen, immer wieder neu mit anderen Daten kombiniert werden und so immer wieder neue Informationen vermitteln. Aus sich heraus sind die Kontexte, die über „Trivialität" oder „Sensitivität" entscheiden, nicht bestimm- und abgrenzbar. Allerdings könnte man dieses Problem in eigenständiger Weise auf einer grundlegenden Regelungsebene durch rechtliche Rahmenbedingungen und Grenzen lösen. Auf einer zweiten Ebene ließe sich dann ein gefährdungsabhängiger Schutz entwickeln, der mehr Faktoren einbezieht als die schlichte Personenbezogenheit von Daten oder Informationen.[77] Angesichts des mit dem Schlagwort „Digitalisierung" umrissenen Wandels der Gesellschaft wird man für das Recht des Umgangs mit personenbezogenen Informationen und Daten insgesamt einen komplexeren Zugriff benötigen, der einerseits sicherstellt, dass Daten nicht von vornherein aus dem Schutz herausfallen, andererseits den Gefährdungen der vielschichtigen und vielfältigen Schutzinteressen Rechnung trägt, die hinter dem „Daten"-schutz stehen. Das verweist bereits darauf, dass dessen rechtliche Konzeptionen im **Zusammenspiel mit anderen Rechtsregimen**[78], die

---

mische IP-Adressen; Urt. v. 20.12.2017, Rn. 27 ff. – Prüfungsantworten und -anmerkungen, alle abrufbar unter http://curia.europa.eu. Vgl. ausf. auch *VG Gelsenkirchen*, Urt. v. 27.4.2020, 20 K 6392/18 – Prüfungsakte, Rn. 80 ff.

[75] Zur Debatte *Éloïse Gratton*, Understanding Personal Information: Managing Privacy Risks, 2013, S. 21 ff.; *Paul M. Schwartz/Daniel Solove*, The PII-Problem: Privacy and a New Concept of Personally Identifiable Information, New York University Law Review 86 (2011), S. 1814 (1815 ff.); *Martin Sebastian Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, bes. S. 338 ff., 450 ff.; *Tina Krügel*, Das personenbezogene Datum nach der DSGVO. Mehr Klarheit und Rechtssicherheit?, ZD 2017, S. 455 (455 ff.).

[76] *BVerfGE* 65, 1 (45). S.a. zur Reformulierung in der jüngeren Rspr. des Gerichts *BVerfG*, Beschl. v. 18 12. 2018, BvR 142/15, Rn. 38: „Insofern gibt es unter den Bedingungen der elektronischen Datenverarbeitung kein schlechthin, also ungeachtet des Verwendungskontextes, belangloses personenbezogenes Datum mehr."

[77] S.a. zur Zwei-Ebenen-Konzeption auf Grundrechtsebene noch → Rn. 26, 33. Vgl. außerdem die Überlegungen bei *Gratton*, Information (Fn. 75), S. 93 ff., 145 ff., 219 ff.

[78] Grundlegend dazu die Überlegungen bei *Anna Schimke*, Das Medienprivileg als Koordinationsmechanismus. Zum Verhältnis von Datenschutz- und Äußerungsrecht im Internet, in: Albers/

bereits Schutzmechanismen bereitstellen, im **Zusammenspiel mit den Kontexte gestaltenden Regelungen**[79] und auch hinsichtlich des **Zusammenspiels allgemeiner und bereichsspezifischer datenschutzrechtlicher Bestimmungen**[80] (weiter-)entwickelt werden muss.

Mit diesen Überlegungen stimmt überein, dass der Fokus personenbezogener Informationen und Daten zum anderen eine **spezifische Perspektive** ist, die den individuellen Schutzbedarf **nicht umfassend abdeckt.** Beispielsweise verdeutlichen Data-Warehouse- und Data-Mining-Strategien, dass auch die statistische Bündelung von Daten problematisch sein und Regelungs- oder Schutzerfordernisse hervorrufen kann.[81] Weiter reichende Schutzmechanismen erfordern auch Profilierungstechniken[82], der Einsatz lernender Algorithmen in Entscheidungsverfahren[83] oder Informations- und Wissensgenerierungsverfahren mittels automatisierter Verknüpfung und Auswertung großer Datenmengen[84]. Debatten im Zivilrecht drehen sich dementsprechend darum, wie man Schutzerfordernissen mit Hilfe ganzheitlicher Perspektiven, die etwa auch das allgemeine Zivilrecht, das Verbraucherschutzrecht, das Wettbewerbs- oder das Kartellrecht berücksichtigen, Rechnung tragen kann.[85] Es ist daher insgesamt wichtig, Datenschutzrecht im Kontext und damit zugleich in seinen Bezügen zu anderweitigen Normen zu verstehen, die ihrerseits Schutzmechanismen bereithalten können und sollten, wenn ein auf personenbezogene Daten und Informationen konzentriertes Datenschutzrecht nicht greift. **18**

Katsivelas (Fn. 16), S. 155 (155 ff.), die die Einsatzbereiche des Äußerungs- und des Datenschutzrechts mit Blick auf Schutzinteressen, Schutzmechanismen und Eignung des jeweiligen Instrumentariums gegeneinander abzugrenzen und zu koordinieren sucht. Auch das BVerfG hat in seiner jüngeren Rspr. äußerungs- und datenschutzrechtliche Stränge des Persönlichkeitsschutzes differenziert, s. noch → Rn. 32. Zum Blick auf andere Rechtsgebiete in Big Data-Zusammenhängen *Manon Oostveen*, Protecting Individuals Against the Negative Impact of Big Data, 2018, S. 180 ff.

[79] → Rn. 14, 60 ff., 67.

[80] → Rn. 63 ff.

[81] *Ira S. Rubinstein/Ronald D. Lee/Paul M. Schwartz*, Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, The University of Chicago Law Review, Bd. 75 (2008), S. 261 (262 ff., hier auch zur Verflochtenheit sach- und personenbezogener Suchmuster); *Mireille Hildebrandt*, Who is Profiling Who? Invisible Visibility, in: Serge Gutwirth u.a. (Hrsg.), Reinventing Data Protection?, 2009, S. 239 (239 ff.); *Liane Colonna*, Legal Implications of Data Mining, 2016.

[82] S. neben den N. in Fn. 81 die Beiträge in: *Mireille Hildebrandt/Serge Gutwirth* (Eds.), Profiling the European Citizen: Cross-Disciplinary Perspectives, 2008; *Bart Schermer*, Risks of Profiling and the Limits of Data Protection Law, in: Bart Custers u.a. (Eds.), Discrimination and Privacy in the Information Society, 2013, S. 37 ff.; *Francesca Bosco u.a.*, Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities, in: Serge Gutwirth/Ronald Leenes/Paul de Hert (Eds.), Reforming European Data Protection Law, 2015, S. 3 ff.; *Indra Spiecker gen. Döhmann et al.*, The Regulation of Commercial Profiling – A Comparative Analysis, EDPL 2016, S. 535 (535 ff.).

[83] Dazu die Nw in → Fn. 67; außerdem *Roland Broemel/Hans-Heinrich Trute*, Alles nur Datenschutz? Zur rechtlichen Regulierung algorithmenbasierter Wissensregulierung, in: Gregor Ritschel/Thomas Müller (Hrsg.), Big data als Theorieersatz, 2016, S. 50 (55 ff.).

[84] Vgl. die Beiträge in *Wolfgang Hoffmann-Riem* (Hrsg.), Big Data – Regulative Herausforderungen, 2018.

[85] S. die Beiträge in *Mor Bakhoum u.a.* (Eds.), Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach?, 2018.

B. Rechtsrahmen

I. Internationale Standards, insbesondere die EMRK

19 Das Recht des Umgangs mit personenbezogenen Informationen und Daten ist schon wegen der Entwicklung des Internet, des wachsenden weltweiten Datentransfers und der Probleme, die disparate Rechtsregime hervorrufen, zunehmend auf **internationale Standards** angewiesen. Deren Entwicklung ist allerdings **voraussetzungsvoll,** die **normative Kraft regelmäßig begrenzt** und das gegenwärtige **Gesamtbild fragmentiert.**[86] Auf adäquate transnational anerkannte Mindeststandards, deren Realisierung zugleich einen freien grenzüberschreitenden Datenverkehr ermöglichen soll, zielt die Datenschutzkonvention des Europarates, die im Jahre 1981 erste allgemeine Grundzüge formulierte[87] und in den letzten Jahren einem aufwändigen Modernisierungsprozess unterzogen worden ist.[88] Neben einer Reformulierung der Schutzziele enthält die neue **Datenschutzkonvention 108+** unter anderem eine Erweiterung des Anwendungsbereichs über die automatisierte Datenverarbeitung hinaus, eine Modernisierung und Erweiterung der Grundsätze, eine Präzisierung und Erweiterung der Rechte der betroffenen Person ebenso wie der Verantwortlichkeiten der datenverarbeitenden Stellen, Vorgaben zum grenzüberschreitenden Datenfluss und Maßgaben zur Etablierung von Kontrollinstitutionen. In vielen Punkten lehnt sie sich an die Vorgaben der DSGVO an, setzt aber lediglich Mindeststandards.[89]

20 Zu den in gewissem Umfang relevanten völkerrechtlichen Maßgaben zählen die **Europäische Menschenrechtskonvention** (EMRK) und die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR).[90] Das gilt unter anderem wegen der Rolle, die sie im Unionsrecht trotz dessen Eigenständigkeit spielen[91], und wegen ihres Einflusses als Auslegungshilfe für die Grundrechte des Grundgesetzes und in Form eines Berücksichtigungsgebots bei der Auslegung und Anwendung des Gesetzesrechts.[92] Das BVerfG hat die Bedeutung der EMRK noch verstärkt, indem es sie als gemeinsames Fundament der ver-

---

[86] Vgl. etwa die Resolution der Generalversammlung der UN vom 17.12.2018, Das Recht auf Privatheit im digitalen Zeitalter, A/RES/73/179. Wie fragmentiert das Bild ist, wird etwa deutlich bei *Kriangsak Kittichaisaree*, Public International Law of Cyberspace, 2017, S. 57 ff.; *Cristina Blasi Casagran*, Global Data Protection in the Field of Law Enforcement, 2017, S. 208 ff. Grds. außerdem *Michael Fehling*, Informational Privacy im Spiegel unterschiedlicher Rechtskulturen, in: ders./Utz Schliesky (Hrsg.), Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, 2016, S. 121 (121 ff.). S. ansonsten *Stephanie Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, 2012, S. 59 ff.

[87] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) des Europarats vom 28.1.1981, BGBl II (1985), S. 538.

[88] S. die Präambel der Datenschutzkonvention 108+, abrufbar unter https://rm.coe.int/16808ade9d.

[89] Die Bundesrepublik Deutschland hat das Änderungsprotokoll im Oktober 2018 unterzeichnet; s. im Anschluss das Vertragsgesetz zum Änderungsprotokoll Datenschutzkonvention.

[90] Allgemein zur Rolle des EGMR *Marion Albers*, Höchstrichterliche Rechtsfindung und Auslegung gerichtlicher Entscheidungen, VVDStRL, Bd. 71 (2012), S. 258 (283 ff.).

[91] → Rn. 25, 27.

[92] *BVerfGE* 111, 307 (315 ff.); 128, 326 (366 ff.); *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 16/13, www.bverfg.de, Rn. 58.

schiedenen mitgliedstaatlichen Grundrechtsordnungen ebenso wie der EU-Grundrechtecharta einstuft.[93] Im Hinblick auf den Umgang mit personenbezogenen Informationen und Daten spielt der **Anspruch auf Achtung des Privatlebens in Art. 8 Abs. 1 EMRK** eine zentrale Rolle.

Die Rechtsprechung des EGMR hat sich in den letzten Jahren in unterschiedlichen Feldern unter verschiedenen Aspekten aufgefächert. Danach schützt Art. 8 EMRK mit dem „Privatleben" ein durchaus **breites Interessenspektrum.** Er schließt dabei in gewissem Umfang soziale Beziehungen und öffentliche Aktivitäten ein. In der Rechtsprechung ist es immer eine gefestigte Sicht gewesen, dass der Anspruch auf Achtung des Privatlebens neben **Eingriffsabwehrrechten** auch **Leistungsrechte,** insbesondere **Schutzpflichten und -ansprüche,** hergibt.[94] Den Schutz im Hinblick auf den Umgang mit personenbezogenen Informationen und Daten hat der Gerichtshof explizit anerkannt[95] und fallspezifisch eine Reihe von Schutzpositionen hergeleitet.[96] Gegenständlich wird ein breites Spektrum erfasst, etwa Steuerdaten, medizinische Daten und Informationen oder die IP-Adresse, aber auch Fotos und Videoaufnahmen oder DNA-Proben als Datenträger.[97] Dass Daten öffentlich zugänglich sind, schließt den Schutz nicht aus. Das gilt etwa im Falle einer systematischen Sammlung und Speicherung durch staatliche Behörden oder im Falle einer Zusammenstellung, Verwendung oder anderweitig gestalteten Veröffentlichung personenbezogener Daten, die von der betroffenen Person normalerweise so nicht erwartet zu werden braucht.[98] Verarbeitungsphasen werden differenziert und gegebenenfalls eigenständig beurteilt.[99] Das Sammeln, Aufzeichnen, Nutzen oder Veröffentlichen kann eine Beeinträchtigung sein, ohne dass es darauf ankommt, ob die Daten sensitiv sind oder ob der Betroffene konkrete Nachteile hatte.[100] Allerdings spielen potentiell beein- 21

[93] *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 16/13, www.bverfg.de, Rn. 56 f.

[94] Aus der Rechtsprechung des EGMR s. etwa Urt. v. 4.12. 2008, Nr. 30562/04 – S. and Marper, Rn. 66 ff., Urt. v. 12.11.2013, Nr. 5786/08 – Söderman, Rn. 78 ff.; Urt. v. 5.9.2017, Nr. 61496/08 – Bărbulescu, Rn. 108 ff.; jeweils abrufbar unter https://hudoc.echr.coe.int.

[95] Vgl. etwa *EGMR*, Urt. v. 27.6.2017, Nr. 931/13 – Satakunnan, insbes. Rn. 137; Urt. v. 30.1.2020, Nr. 50001/12 – Breyer, Rn. 74 ff.

[96] Ausf. Analysen bei *Albers*, Selbstbestimmung (Fn. 31), S. 288 ff.; *Birte Siemen*, Datenschutz als europäisches Grundrecht, 2006, S. 51 ff.; *Rainer Schweizer*, Die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zum Persönlichkeits- und Datenschutz, DuD 2009, S. 462 (464 ff.); *Paul De Hert/Serge Gutwirth*, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in: Gutwirth u. a. (Fn. 81), S. 3 (14 ff.).

[97] Exemplarisch *EGMR*, Urt. v. 12.12.2013, Nr. 20383/04 – Khmel, Rn. 41 ff., 49; Urt. v. 27.6.2017, Nr. 931/13 – Satakunnan, Rn. 133 ff.; Urt. v. 27.2.2018, Nr. 66490/09 – Gesundheitsdaten, Rn. 93 f.; Urt. v. 24.4.2018, Nr. 62357/14 – IP-Adresse und TK-Bestandsdaten, Rn. 100 ff., 107 ff.; Urt. v. 30.1.2020, Nr. 50001/12 – Breyer, Rn. 76 ff.; Urt. v. 14.4.2020, Nr. 75229/10 – DNA-Sample, Rn. 69, 79; jeweils abrufbar unter https://hudoc.echr.coe.int.

[98] *EGMR*, Urt. v. 4.5.2000, Nr. 28341/95 – Rotaru, Rn. 43 f.; Urt. v. 6.6.2006, Nr. 62332/00 – Segerstedt-Wiberg, Rn. 72; Urt. v. 13.11.2012, Nr. 24029/07 – M.M., Rn. 188; Urt. v. 27.6.2017, Nr. 931/13 – Satakunnan, Rn. 134 ff.; abrufbar unter https://hudoc.echr.coe.int.

[99] *EGMR*, Urt. v. 12.12.2013, Nr. 20383/04 – Khmel, Rn. 40 ff.; Urt. v. 26.1.2017, Nr. 42788/06 – Surikov, Rn. 75, 84 ff.; Urt. v. 27.6.2017, Nr. 931/13 – Satakunnan, Rn. 134 ff.; abrufbar unter https://hudoc.echr.coe.int.

[100] *EGMR*, Urt. v. 26.3.1987, Nr. 9248/81 – Leander, Rn. 48; Urt. v. 16.2.2000, Nr. 27798/95 – Amann, Rn. 44 ff.; Urt. v. 4.5.2000, Nr. 28341/95 – Rotaru, Rn. 42 ff.; Urt. v. 25.9.2001, Nr. 44787/98 – P.G., Rn. 57 ff., Urt. v. 28.1.2003, Nr. 44647/98 – Peck, Rn. 57 ff.; Urt. v. 11.1.2005, Nr. 50774/99 – Sciacca, Rn. 26 ff.; Urt. v. 6.6.2006, Nr. 62332/00 – Segerstedt-Wiberg, Rn. 69 ff.; Urt. v. 4.12.2008, Nr. 30562/04 – S. and Marper, Rn. 58 ff.; alle abrufbar unter https://hudoc.echr.coe.int.

trächtigende Folgen für die rechtliche Beurteilung des Schutzes durchaus eine Rolle.[101] Nähere Anforderungen an die notwendigen gesetzlichen Grundlagen präzisiert der EGMR inzwischen je nach Kontext und Schutzdimension unter Anerkennung mehr oder weniger weit reichender Gestaltungsspielräume der Vertragsstaaten sehr differenziert. So erfordern staatliche Überwachungsmaßnahmen, insbesondere wenn sie in bestimmten Stadien geheim sind, eine Reihe aufeinander abgestimmter gesetzlicher Mindestvorkehrungen.[102] Und seine Schutzpflichten erfüllt der Staat nicht hinreichend, solange er nicht die Achtung des Privatlebens unter Privaten dadurch sicherstellt, dass er einen gesetzlichen Rahmen schafft, der den unterschiedlichen Schutzinteressen in einem bestimmten Kontext Rechnung trägt.[103] Mit Rücksicht auf die Funktionen des persönlichen Wissens über das personenbezogene Wissen der sozialen Umwelt kann Art. 8 EMRK zudem (eingrenzbare) Kenntnisrechte hergeben, etwa Auskunfts- oder Akteneinsichtsansprüche hinsichtlich der bei Behörden vorhandenen personenbezogenen Daten oder Unterlagen.[104] Mit dieser sich **zunehmend verfeinernden Rechtsprechung** steigen die **Anforderungen an die Abstimmung mit dem unionalen und nationalen Recht.**

III. Primärrechtliche Vorgaben der Europäischen Union

1. Kompetenzzuweisungen

22 Seit dem Vertrag von Lissabon bietet **Art. 16 Abs. 2 AEUV**, mit der Ausnahme für den Bereich der Gemeinsamen Außen- und Sicherheitspolitik in Art. 39 S. 1 EUV, eine **einheitliche Kompetenzgrundlage** zur Regelung von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und über den freien Datenverkehr.[105] Sein Normtext erfasst die Datenverarbeitung durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten „im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrecht fallen". Das Normverständnis des EuGH orientiert sich an eher extensiven Kriterien.[106] Vor dem Hintergrund der engen Bezüge zwischen Datenverarbeitungen und den Strukturen des jeweiligen Sachgebiets sowie der entsprechenden Abstimmungserfordernisse ergeben sich aus der Norm jedoch Kompetenzgrenzen, auf die man nicht verzich-

[101] S. *EGMR*, Urt. v. 21.1.2016, Nr. 29908/11 – Ivanovski, Rn. 177 (vermischt mit der Beeinträchtigungsintensität); Urt. v. 27.2.2018, Nr. 66490/09 – Gesundheitsdaten, Rn. 93; abrufbar unter https://hudoc.echr.coe.int.

[102] Vgl. *EGMR*, Urt. v. 4.12.2015, Nr. 47143/06 – Zakharov, Rn. 228ff., Urt. v. 12.1.2016, Nr. 37138/14 – Szabó and Vissy, Rn. 52ff.; *EGMR (GK)*, Urt. v. 25.5.2021, Nr. 58170/13 u.a. – Big Brother Watch, Rn. 332ff., hier auch mit einer Prüfung des Art. 10 EMRK; vgl. auch Urt. v. 30.1.2020, Nr. 50001/12 – Breyer, Rn. 83ff.; alle abrufbar unter https://hudoc.echr.coe.int.

[103] Vgl. *EGMR*, Urt. v. 5.9.2017, Nr. 61496/08 – Bărbulescu, Rn. 115 m.w.N. und weiter mit der Ausarbeitung näherer Maßgaben für den Kontext des zu entscheidenden Falles in Rn. 120ff., abrufbar unter https://hudoc.echr.coe.int.

[104] *EGMR*, Urt. v. 7.7.1989, Nr. 10454/83 – Gaskin, Rn. 37; Urt. v. 6.6.2006, Nr. 62332/00 – Segerstedt-Wiberg, Rn. 99ff.; abrufbar unter https://hudoc.echr.coe.int.

[105] Die Kompetenz, mit Drittländern oder internationalen Organisationen Übereinkünfte u.a. im Bereich des Datenschutzes zu schließen, findet sich in Art. 216 Abs. 1 AEUV.

[106] Näher dazu *Rüpke/von Lewinski/Eckhardt*, Datenschutzrecht (Fn. 36), § 7 Rn. 1ff.

ten kann, damit sich das Verhältnis zwischen Union und Mitgliedstaaten nicht über das Datenschutzrecht deutlich verschiebt. Art. 16 Abs. 2 AEUV **findet einen Kompetenzenrahmen vor,** in den **er sich einfügt.**[107] Allerdings kann der Grundsatz der praktischen Wirksamkeit des Unionsrechts in bestimmtem Umfang eine überschießende Dynamik auslösen und weiter reichende Regelungen rechtfertigen.[108] Auch wenn man die Grenzen deutlicher herausarbeitet, trägt Art. 16 Abs. 2 AEUV, zumal wenn man ihn nicht zuletzt vor dem Hintergrund des Internets als Gewährleistungs- oder Schutzverpflichtung versteht, wesentlich zur Europäisierung des Datenschutzes bei.

2. Datenschutz als Gegenstand europäischer Grundrechte

a) Anwendbarkeit unionaler Grundrechte

Unionsgrundrechte binden die Organe der Europäischen Union, aber auch die Mitgliedstaaten, namentlich bei der Umsetzung sekundärrechtlicher Vorgaben sowie als Maßstäbe, anhand derer umsetzendes nationales Recht unionsrechtskonform auszulegen ist. Inwieweit die europäischen Grundrechte greifen, richtet sich danach, ob ein Mitgliedstaat im Anwendungsbereich oder „in Durchführung" (Art. 51 Abs. 1 S. 1 GRCh) des Rechts der Union handelt. Ob der für ein **Handeln im Anwendungsbereich des Unionsrechts** notwendige Zusammenhang zwischen einem Unionsrechtsakt und nationalen Maßnahmen gegeben ist, ist nach einem Kriterienbündel zu bestimmen.[109] Im Übrigen kommt es auf die Abgrenzung des Anwendungsbereichs der allgemeinen und bereichsspezifischen Vorschriften der Europäischen Union und auf deren Interpretation an. Im Ausgangspunkt reicht nicht nur der Anwendungsbereich der EU-Datenschutzgrundverordnung, sondern oft auch derjenige bereichsspezifischer Datenschutznormen weit. So hat der EuGH im Kontext der e-privacy-Richtlinie ausgeführt, dass darunter nicht nur Rechtsvorschriften fielen, die den Betreibern elektronischer Kommunikationsdienste eine Speicherung bestimmter Verkehrs- und Standortdaten vorschrieben. Vielmehr erfasst die Richtlinie auch die den Betreibern auferlegten Rechtspflichten, bestimmten Sicherheitsbehörden Zugang zu diesen Daten zu gewähren, selbst wenn der Geltungsbereich der Richtlinie mitgliedstaatliche Tätigkeiten im Sicherheitsbereich ausklammert.[110] Da Verar- 23

[107] So *Raoul-Darius Veit*, Einheit und Vielfalt im europäischen Datenschutzrecht, 2021 (i.E.), Teil 1 C 2. Vgl. darüber hinaus, wenn auch in den Abgrenzungskriterien wenig deutlich *Thorsten Kingreen*, in: Callies/Ruffert (Hrsg.) EUV/AEUV, Art. 16 Rn. 2 ff. Ausführlich zu Art. 16 Abs. 2 AEUV mit einer allerdings sehr extensiven Sicht *Hielke Hijmans*, The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU, 2016. Eine umfassende Supranationalisierungskompetenz sehen, allerdings ohne problemsensible Begründung, *Jürgen Kühling/Johannes Raab*, in: Jürgen Kühling/Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung – BDSG, 3. Aufl. 2020, Einführung, Rn. 8.

[108] Näher dazu *Veit*, Einheit (Fn. 107), Teil 1 C 2 b. Ähnlich, aber i. Erg. extensiver *Nikolaus Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 336 ff.

[109] Weit gefasst noch *EuGH*, Urt. v. 26.2.2013, C-617/10, Rn. 16 ff. – Åkerberg Fransson; enger dann mit einem etwa einengenden Kriterienbündel die Folgerechtsprechung, etwa *EuGH*, Urt. v. 6.3.2014, C-206/13, Rn. 20 ff.; Urt. v. 10.7.2014, C-198/13, Rn. 34 ff. Aus jüngerer Zeit s. etwa *EuGH*, Urt. v. 13.6.2017, C-258/14, Rn. 44 ff.

[110] *EuGH*, Urt. v. 6.10.2020, C-511, 512 u. 520/18, Rn. 87 ff. – Quadrature du Net u.a.; Urt. v. 6.10.2020, C-623/17, Rn. 30 ff. – Privacy International, beide abrufbar unter http://curia.europa.eu.

beitungsphasen, hier die Zugangsgewähr, als Elemente von Verarbeitungsabläufen und insofern im Zusammenhang zu sehen sind[111], ist die Argumentation durchaus stimmig. Eingesetzt hat der EuGH sie im Weiteren auch mit Blick auf Art. 2 Abs. 2 lit. d DSGVO, der sachliche Ausnahmen aus deren Anwendungsbereich in Sicherheitsfeldern vorsieht, und Art. 23 Abs. 1 DSGVO, der Möglichkeiten u.a. der Mitgliedstaaten regelt, die in der DSGVO eingeräumten Pflichten und Rechte zu Gunsten der öffentlichen Sicherheit zu beschränken.[112] Angesichts der Reichweite der Anwendungsbereiche wird entscheidend, inwieweit die Vorschriften auf eine vollständige Determination oder auf mitgliedstaatliche Regelungsaufträge oder Spielräume gerichtet sind und inwieweit innerhalb solcher Aufträge oder Spielräume unionsrechtliche Vorgaben „durchgeführt" werden. Eine diesen letzten Punkt näher klärende **„Spielraumdogmatik"** ist ein **Desiderat.** Das gilt um so mehr, als sich gerade die Vorgaben im Recht des Umgangs mit personenbezogenen Informationen und Daten durch bestimmte Spielraumformen auszeichnen. Für die EU-Datenschutzgrundverordnung zeigen dies insbesondere, aber nicht nur die Öffnungen für mitgliedstaatliches Recht.[113]

24 Im Falle **unionsrechtlich vollvereinheitlichter Regelungen** greifen in aller Regel allein die Unionsgrundrechte.[114] Allerdings hat sich das BVerfG hier in aktueller Rechtsprechung die Kompetenz zuerkannt, die „richtige Anwendung vollvereinheitlichten Unionsrechts" durch deutsche staatliche Stellen in Wahrnehmung seiner „Integrationsverantwortung" und in Kooperation mit dem EuGH, hier insbesondere auch unter Beachtung der Vorlageverpflichtung aus Art. 267 Abs. 3 AEUV, am Maßstab der Unionsgrundrechte zu prüfen.[115] Bei **mitgliedstaatlichen Spielräumen** nimmt der *EuGH* an, dass jedenfalls in bestimmtem Umfang immer auch Unionsrecht durchgeführt wird[116]. Insoweit greifen immer auch die europäischen Grundrechte und die Bindungen mitgliedstaatlicher Grundrechte treten hinzu, sofern dadurch weder das Schutzniveau der Charta noch der Vorrang, die Einheit und die Wirksamkeit des Unionsrechts beeinträchtigt werden.[117] Das *BVerfG* vertritt demgegenüber die Position, dass

---

[111] → Rn. 11.

[112] *EuGH*, Urt. v. 6.10.2020, C-511, 512 u. 520/18, Rn. 102 – Quadrature du Net u.a.; Urt. v. 6.10.2020, C-623/17, Rn. 47 – Privacy International, beide abrufbar unter http://curia.europa.eu.

[113] Dazu → Rn. 59.

[114] Das *BVerfG* stellt die alleinige Anwendung der Unionsgrundrechte unter bestimmte Vorbehalte, vgl. näher *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 276/17 – Recht auf Vergessen II, www.bverfg.de, Rn. 47ff.

[115] Im Einzelnen: *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 276/17 – Recht auf Vergessen II, www.bverfg.de, Rn. 50ff. Zuvor mit Vorschlägen *Eike M. Frenzel*, Die Charta der Grundrechte als Maßstab für mitgliedstaatliches Handeln zwischen Effektivierung und Hyperintegration, Der Staat Bd. 53 (2014), S. 1 (18ff.); *Matthias Bäcker*, Das Grundgesetz als Implementationsgarant der Unionsgrundrechte, EuR 2015, S. 389 (410ff.).

[116] Für die DSRiL s. *EuGH*, Urt. v. 24.11.2011, C-468/10 u. C-469/10, abrufbar unter http://curia.europa.eu, Rn. 29ff., 35 – Spanisches Datenschutzrecht: Dabei hat der EuGH zwar Flexibilitäten der Richtlinienvorgaben etwa in Art. 7 EU-DSRL anerkannt, jedoch zwischen (unzulässigen) nationalen Maßnahmen, die die Tragweite dieser Vorgaben verändern, und (zulässigen) nationalen Maßnahmen, die die Vorgaben nur näher bestimmen, differenziert. Allgemein für Vorschriften, die den Mitgliedstaaten Ermessen einräumen, s. *EuGH*, Urt. v. 13.6.2017, C-258/14, Rn. 48.

[117] S. etwa *EuGH*, Urt. v. 26.2.2013, C-617/10, Rn. 29 – Åkerberg Fransson; Urt. v. 29.7.2019, C-469/17, Rn. 30ff. – Funke Medien; Urt. v. 24.9.2019, C-507/17, Rn. 72 – räumliche Reichweite des

die mitgliedstaatlichen Grundrechte regelmäßig den ausschließlichen Prüfungsmaßstab hergeben. Es begründet dies mittlerweile damit, dass diese Grundrechte das Schutzniveau der unionalen Grundrechte, von Ausnahmen abgesehen, in sich einschlössen.[118]

b) Recht auf Datenschutz und weitere Gewährleistungen

Primärrechtlich verankert zum einen Art. 16 Abs. 1 AEUV das **Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten.** Mit gleicher normtextlicher Formulierung wird dieses Recht in maßgeblicher Weise[119] zum anderen in **Art. 8 Abs. 1 GRCh** abgesichert. Hinzu tritt Art. 7 GRCh, der das Recht jeder Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation normiert. Wegen des weit gehenden Gleichklangs mit Art. 8 Abs. 1 EMRK, der Klausel des Art. 52 Abs. 3 GRCh und des Befunds, dass der Europäische Gerichtshof für Menschenrechte keine explizite Norm zur Verfügung und Art. 8 EMRK zur zentralen Grundlage näherer Maßgaben zum Umgang mit personenbezogenen Informationen und Daten ausgebaut hat, tauchen **Abgrenzungsschwierigkeiten zwischen den Schutzgehalten des Art. 7 und des Art. 8 GRCh** auf. Allerdings hat der EuGH mittlerweile hervorgehoben, dass die EMRK, solange die Union ihr nicht beigetreten ist, „kein Rechtsinstrument darstellt, das förmlich in die Unionsrechtsordnung übernommen wurde", dass deshalb Sekundärrechtsakte „einzig und allein anhand der durch die Charta garantierten Grundrechte auszulegen" seien, dass Art. 52 Abs. 3 GRCh einem weitergehenden unionsrechtlichen Schutz nicht entgegenstehe und dass Art. 8 GRCh „ein anderes als das in ihrem Art. 7 verankerte Grundrecht" sei, für das es in der EMRK keine Entsprechung gebe.[120] Vor diesem Hintergrund und in teleologischer Reduktion steht Art. 52 Abs. 3 GRCh einer relativ eigenständigen unionsrechtlichen Interpretation des Art. 7 GRCh und des Art. 8 GRCh somit nicht entgegen. Inhaltlich ist dieser nicht etwa pauschal lex specialis zu jenem.[121] Die sinnvollste Lösung liegt vielmehr darin, einen **partiell spezifischen Gehalt von Art. 7 GRCh,** eine Abgrenzung nicht erfordernde **Schnittmenge** beider Grundrechte und einen **partiell eigenständigen Gehalt von Art. 8 GRCh** zu Grunde zu legen.[122] Dies ermöglicht eine mit der Rechtsprechung des EGMR abgestimmte, gleichwohl unionsrechtlich

25

Rechts auf Auslistung, beide abrufbar unter http://curia.europa.eu. Vgl. übergreifender auch *Claudio Franzius*, Strategien der Grundrechtsoptimierung in Europa, EuGRZ 2015, S. 139 (143 f.).

[118] → Rn. 31.

[119] Die Abstimmungsschwierigkeiten zwischen Art. 16 Abs. 1 AEUV, Art. 8, Art. 52 Abs. 1 und Art. 52 Abs. 2 GRCh sind mit einer teleologischen Reduktion des Art. 52 Abs. 2 GRCh zu lösen. Vgl. auch *EuGH*, Gutachten v. 26.7.2017, 1/15 – PNR-Abkommen, Rn. 120.

[120] So etwa *EuGH*, Urt. v. 21.12.2016, C-203/15 u. C-698/15 – Tele2 Sverige, Rn. 127 f.

[121] So aber etwa *Ino Augsberg*, in: v. d. Groeben/Schwarze/Hatje (Hrsg.), Unionsrecht, Art. 8 GRC Rn. 1; *Jürgen Kühling/Manuel Klar/Florian Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 50.

[122] Vgl. hierzu, wenn auch mit unterschiedlichen Akzenten, *Gratton*, Information (Fn. 75), S. 202 ff.; *Colonna*, Implications (Fn. 81), S. 122 ff.; *Gloria Fuster González*, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, S. 268 ff.; *Maria Tzanou*, The Fundamental Right to Data Protection, S. 7 ff.; *Olga Lynskey*, Deconstructing data protection: the ‚added-value' of a right to data protection in the EU legal order, International and Comparative Law Quarterly 2014, S. 569 (581 ff.); *Herke Kranenborg*, in: Steve Peers/Tamara Hervey/Jeff Kenner/Angela Ward (eds.), The EU charter of fundamental rights, 2014, Art. 8 GRCh Rn. 176 (als Ergebnis).

zugeschnittene dynamisch-innovative Entfaltung der Schutzgehalte. Dabei lassen sich sowohl der Achtungsanspruch des Art. 7 GRCh als auch der Schutzanspruch des Art. 8 Abs. 1 GRCh mehrdimensional entfalten.

26 Art. 8 GRCh bleibt hinsichtlich des **Schutzguts** relativ vage. Darin liegt angesichts der Anforderungen, die der Gegenstand – Schutz im Hinblick auf den Umgang mit personenbezogenen Informationen und Daten – stellt[123], aber gerade seine Stärke. Denn die Norm lässt sich inhaltlich und dogmatisch eigenständig und damit gegenstandsgerecht entwickeln. Weder schließt sie sich lediglich an den Schutz des Art. 7 GRCh an[124] noch schützt sie pauschal die „Herrschaft über die eigenen Daten"[125]. Vielmehr gibt sie mit dem „Recht auf Schutz" Regulierungs- und Schutzanforderungen her, die sich primär auf einer konkreten Konstellationen vorgelagerten Ebene bewegen und hier bestimmten Schutzerfordernissen der betroffenen Personen Rechnung tragen.[126] Dazu gehört, dass erstens die Verarbeitung personenbezogener Daten mit einem passenden Rechtsrahmen grundlegend begrenzt, sachgerecht strukturiert sowie transparent gestaltet wird. Dabei sind insbesondere auch die informations- und datenverarbeitenden Stellen, bei denen sich der Umgang mit personenbezogenen Informationen und Daten vollzieht, mit einem Spektrum an Pflichten zu adressieren. Bereits angesichts des Regelungsgegenstandes versteht es sich im Übrigen von selbst, dass der erforderliche Rechtsrahmen ein vielschichtiges, sich dynamisch weiterentwickelndes Gefüge von Normen unterschiedlicher Provenienz sein muss. Zweitens müssen grundlegende gegenstands- und schutzbedarfsgerechte Rechtspositionen der betroffenen Personen gewährleistet werden, insbesondere Kenntnis-, Partizipations- und Einflussmöglichkeiten der Betroffenen im Hinblick auf den sie angehenden Umgang mit Informationen und Daten. Wegen der gegenstandsbedingten Leistungsgrenzen individuell-subjektiver Rechte müssen drittens institutionelle Gewährleistungs- und Kontrollmechanismen hinzutreten.[127] Diese Überlegungen stimmen damit überein, dass Art. 8 Abs. 2 und 3 GRCh einige Vorgaben präzisieren: Personenbezogene Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder aufgrund einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften soll von einer unabhängigen Stelle überwacht werden. Bei der Einordnung dieser Vorgaben ist zu berücksichtigen, dass es sich dabei um eine eher unsystematische Zusammenstellung mehrerer Faktoren unterschiedlicher Provenienz

[123] → Rn. 4 ff.

[124] So aber *Rainer Stentzel*, Das Grundrecht auf …?, PinG 2015, S. 185 (189 f.), vor dem Hintergrund der Vagheit des Art. 8 Abs. 1 GRCh.

[125] So etwa *Thorsten Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 8 GRCh, Rn. 9.

[126] Vgl. zu solchen Ansätzen mit im Einzelnen unterschiedlichen Überlegungen die Ausarbeitungen zu den deutschen Grundrechtsgewährleistungen bei *Albers*, Selbstbestimmung (Fn. 31), bes. S. 353 ff.; bei *Marsch*, Datenschutzgrundrecht (Fn. 108), bes. S. 127 ff.; und – vor allem im Aufgreifen der Aussagen des Art. 8 GRCh – bei *Jörn Reinhardt*, Konturen des europäischen Datenschutzgrundrechts, AöR, Bd. 142 (2017), S. 528 (540 ff.).

[127] Insgesamt zum Grundansatz, dies für die deutschen Grundrechtsgewährleistungen, *Albers*, Selbstbestimmung (Fn. 31), bes. S. 454 ff. Das unionale Grundrecht auf Datenschutz kann diesen Ansatz abbilden.

handelt[128] und dass damit auch nicht etwa der Kerngehalt des „Rechts auf Schutz personenbezogener Daten" erschöpfend beschrieben wird. Im Ergebnis gibt Art. 8 GRCh ein Bündel vielschichtiger Anforderungen her. Auf der Grundlage, die durch die Regulierung nach Maßgabe dieser Anforderungen entsteht, treten andere Verbürgungen mit ihren Freiheits- und Schutzversprechen hinzu, und zwar keineswegs nur Art. 7 GRCh, sondern auch andere unter Umständen einschlägige Gewährleistungen. Denn es liegt schon vom Gegenstand her nahe, eine **breite normative Basis zur Konkretisierung unionsgrundrechtlicher Vorgaben für den Umgang mit personenbezogenen Informationen und Daten** zu nutzen, beispielsweise die Rechte auf geistige Unversehrtheit (Art. 3 Abs. 1 GRCh), auf Gedanken-, Gewissens- und Religionsfreiheit (Art. 10 Abs. 1 GRCh), auf Meinungsäußerungs- und Versammlungsfreiheit (Art. 11 und 12 Abs. 1 GRCh) oder auf Berufsfreiheit (Art. 15 Abs. 1 GRCh).[129] Für Regelungs- und Einschränkungsmöglichkeiten greift der „hinter die Klammer" gestellte Art. 52 Abs. 1 GRCh.

Die **Rechtsprechung des Europäischen Gerichtshofs** zum informations- und datenbezogenen Grundrechtsschutz ist in den letzten Jahren **zunehmend ausgebaut** worden, aber noch entwicklungsbedürftig.[130] Die vor allem in der Anfangszeit unzulängliche Differenzierung zwischen Art. 7 GRCh und Art. 8 GRCh[131] ist noch nicht überwunden, obwohl der EuGH mittlerweile teilweise betont, dass Art. 7 und Art. 8 GRCh zumindest partiell eigenständige Inhalte haben[132]. Die Gehalte des Art. 8 GRCh bleiben im Ansatz eher unbestimmt, gewinnen in manchen Entscheidungen dann aber im fallspezifischen Kontext durchaus an Substanz. Zu den zentralen Anknüpfungspunkten zählen „personenbezogene Daten" und deren Verarbeitung, ohne dass – dies im Anschluss an die Rechtsprechung des EGMR – ein sensibler Charakter der aus den Daten gewinnbaren Informationen oder erlittene Nachteile eine Rolle spielten.[133] Verarbeitungsphasen werden differenziert und in ihrem Gefährdungsgehalt gesondert – allerdings nicht isoliert, sondern als jeweilige Elemente eines Verarbeitungszusammenhanges – beurteilt.[134] Im näheren Kontext finden sich dann gelegentlich Präzisierungen der Schutzinteressen und Beeinträchtigungen, hier etwa Erfordernisse des Schutzes vor einer umfassenden Profilbildung oder ständigen Überwachung, vor erwartungsvermittelten Einschränkungen eigentlich geschützten Verhaltens, vor einem Unterlaufen des Berufsgeheimnisses oder

27

[128] Zu den Komponenten des Art. 8 Abs. 2 GRCh *Marsch*, Datenschutzgrundrecht (Fn. 108), S. 150 ff. m. w. N. Der stimmige Anschluss von Art. 52 Abs. 1 GRCh bereitet teilweise Probleme.

[129] Zur Konkretisierung der Grundrechte des GG → Rn. 32 ff.

[130] Überblicke bei *Thomas von Danwitz*, Die Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten, DuD 2015, S. 581 (581 ff.); *Vassilios Skouris*, Leitlinien der Rechtsprechung des EuGH zum Datenschutz, NVwZ 2016, S. 1359 (1360 ff.).

[131] Für umfangreichere Analysen der älteren Rechtsprechung vgl. *Siemen*, Datenschutz (Fn. 96), S. 251 ff.; *De Hert/Gutwirth*, Data (Fn. 96) S. 29 ff.

[132] Etwa *EuGH*, Urt. v. 8.4.2014 – C-293/12 und C-594/12 – Digital Rights Ireland, Rn. 25 ff.; Urt. v. 21.12.2016, C-203/15 u. C-698/15 – Tele2 Sverige, Rn. 129.

[133] *EuGH*, Urt. v. 6.10.2020, C-511, 512 u. 520/18, Rn. 87 ff. – Quadrature du Net u. a.; Urt. v. 6.10.2020, C-623/17, Rn. 30 ff. – Privacy International, alle abrufbar unter http://curia.europa.eu.

[134] *EuGH*, Urt. v. 8.4.2014 – C-293/12 und C-594/12 – Digital Rights Ireland, Rn. 34 f.; Urt. v. 6.10.2020, C-511, 512 u. 520/18, Rn. 87 ff. – Quadrature du Net u. a.; Urt. v. 6.10.2020, C-623/17, Rn. 30 ff. – Privacy International, alle abrufbar unter http://curia.europa.eu.

des Informantenschutzes oder vor Datenmissbrauch.[135] Bei diesen Schutzinteressen zieht der EuGH weitere unionale Grundrechte, aber auch Schutzinteressen aus sekundärrechtlichen oder nationalen Regelungen hinzu.[136] Das ist durchaus stimmig, wenn man Art. 8 GRCh mit einem Bündel von Schutzgütern verknüpft und ihm Regulierungs- und Schutzanforderungen entnimmt, die zunächst an die Gesetzgebung gerichtet sind, welche den Schutz personenbezogener Daten konsistent gestalten und einpassen müssen.[137] Dazu passt, dass der EuGH dogmatisch unterschiedliche Schutzdimensionen anerkennt, neben Eingriffsabwehrrechten also etwa auch Leistungsrechte, Schutzrechte oder, nicht ganz deutlich, eine mittelbare Horizontalwirkung im Verhältnis unter Privaten.[138] Im Übrigen macht er viele Maßgaben am Verhältnismäßigkeitsgrundsatz fest, dem er eine Beschränkung der Einschränkungen des Schutzes personenbezogener Daten „auf das absolut Notwendige"[139] entnimmt – ein Stichwort, aus dem dann in nicht mehr unbedingt stringenter Herleitung eine Palette festzulegender verschiedenartiger Vorkehrungen im Falle von Beschränkungen entwickelt wird.[140] Sofern passend, wird auch auf die Vorgaben des Art. 8 Abs. 2 und 3 GRCh hingewiesen. Die Maßgaben und Vorkehrungen reichen von Anforderungen an die Systemgestaltung über Schwellen für die jeweilige Verarbeitungsphase, Prüfpflichten, Entscheidungsvorbehalte oder Datensicherheitsanforderungen bis hin zu eingriffsakzessorischen Benachrichtigungsrechten.[141]

28 Die Rechtsprechung des EuGH lässt somit eine **vielschichtige Konzeption der Grundrechtsaussagen** erkennen, ohne dass diese bereits einen inhaltlich und dogmatisch gesicherten Bestand ergäben. Man wird dies auch nur in begrenztem Umfang erwarten können. Nicht nur bleibt der EuGH in seinen Entscheidungsgründen vor dem Hintergrund der unterschiedlichen Rechtskulturen in den Mitgliedstaaten oft apodiktisch.[142] Vor allem sind die Aussagen des „Datenschutzgrundrechts" kontextualisierungsbedürftig, sobald man es näher mit Substanz

---

[135] S. etwa *EuGH*, Urt. v. 13.5.2014 – C-131/12, Google Spain, Rn. 80; Urt. v. 24.9.2019 – C-136/17, GC u.a., Rn. 36; Urt. v. 6.10.2020, C-511, 512 u. 520/18, Rn. 87ff. – Quadrature du Net u.a.; Urt. v. 6.10.2020, C-623/17, Rn. 30ff. – Privacy International, alle abrufbar unter http://curia.europa.eu.

[136] Vgl. *EuGH*, Urt. v. 6.10.2015 – C-362/14, Schrems I, Rn. 72; Urt. v. 6.10.2020, C-511, 512 u. 520/18, Rn. 87ff. – Quadrature du Net u.a.; Urt. v. 6.10.2020, C-623/17, Rn. 30ff. – Privacy International, jeweils abrufbar unter http://curia.europa.eu.

[137] Vgl. auch die Ausführung in *EuGH*, Urt. v. 6.10.2020, C-511, 512 u. 520/18, Rn. 109 – Quadrature du Net u.a: „Durch den Erlass dieser Richtlinie hat der Unionsgesetzgeber somit die in den Art. 7 und 8 der Charta verankerten Rechte konkretisiert, so dass die Nutzer elektronischer Kommunikationsmittel grundsätzlich erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Verkehrsdaten anonym bleiben und nicht gespeichert werden dürfen, es sei denn, sie haben darin eingewilligt."

[138] S. zu Letzterem *Reinhardt*, Konturen (Fn. 126), S. 544ff.

[139] St. Rspr.; s. nur zuletzt *EuGH*, Urt. v. 2.3.2021, C-746/18, Rn. 38ff. – H.K. m.w.N.; abrufbar unter http://curia.europa.eu.

[140] Kritisch zur Überfrachtung des Verhältnismäßigkeitsgrundsatzes im Rahmen der einschlägigen Rspr. des BVerfG *Marion Albers*, Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, in: Michael Friedewald/Jörn Lamla/Alexander Roßnagel (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, 2017, S. 11 (19ff.).

[141] S. dazu etwa *EuGH*, Urt. v. 8.4.2014 – C-293/12 und C-594/12 – Digital Rights Ireland, Rn. 53ff., 68; Urt. v. 6.10.2015 – C-362/14, Schrems I, Rn. 91ff.; Urt. v. 24.9.2019 – C-136/17, GC u.a., Rn. 49ff.; Urt. v. 6.10.2020, C-511, 512 u. 520/18, Rn. 87ff. – Quadrature du Net u. a.; Urt. v. 6.10.2020, C-623/17, Rn. 30ff. – Privacy International, Urt. v. 2.3.2021, C-746/18, Rn. 51ff. – H.K.; alle abrufbar unter http://curia.europa.eu.

[142] Dazu etwa *Albers*, Rechtsfindung (Fn. 90), S. 281 m.w.N.

füllen möchte und muss. Gerade in diesem Bereich wäre eine in jeder Hinsicht **zentralistisch-hierarchische Positionierung des EuGH** deswegen **verfehlt.**

III. Vorgaben des Grundgesetzes

1. Kompetenzverteilung

Im Grundgesetz, dessen Kompetenzverteilung auch hinsichtlich der noch ausfüllungs- oder umsetzungsbedürftigen sekundärrechtlichen Datenschutzbestimmungen der Union maßgeblich ist, werden Datenschutzregelungen nicht durch eine ausdrücklich darauf gerichtete Gesetzgebungskompetenz abgedeckt. Angesichts der Verflochtenheit mit den jeweiligen Sachbereichen sind jedoch **Kompetenzen kraft Sachzusammenhanges** und **Annexkompetenzen** zu Gunsten des Bundes im Anschluss an die in Art. 73 und 74 GG aufgezählten Sachkompetenzen anzuerkennen[143]. Das betrifft die öffentliche Verwaltung des Bundes, die notwendig Bundesgesetze ausführt und für die der Datenschutz – neben den sekundärrechtlichen Vorgaben – deswegen entweder in sektorspezifischen Bundesgesetzen oder in einem Querschnitts- und Auffanggesetz wie dem Bundesdatenschutzgesetz geregelt werden kann. Die öffentliche Verwaltung der Länder kann im Anwendungsbereich sektorspezifischer Bundesgesetze den hierin oder ggf. auch im Bundesdatenschutzgesetz enthaltenen Datenschutzregelungen des Bundes unterliegen. Im Übrigen greifen für sie, wiederum neben den sekundärrechtlichen Vorgaben, bereichsspezifische Ländergesetze oder die Landesdatenschutzgesetze. 29

Die Bundesgesetzgebungskompetenz für datenschutzrechtliche Regelungen reicht jeweils so weit, wie diese kraft Sachzusammenhanges oder als Annex mitzuregeln sind. Auf die Beurteilung der „notwendigerweise" mitzuregelnden Aspekte wirken sich freilich der Prozesscharakter der Daten- und Informationsverarbeitung und die Wechselbeziehungen zwischen den einzelnen Schritten aus[144]. Betrachtet man Verarbeitungsabläufe insgesamt, können sie auch hinsichtlich einzelner Phasen teils der Bundes-, teils der Landesgesetzgebungskompetenz unterliegen. So kann der Bund zum Beispiel im Sicherheitsbereich unter bestimmten Voraussetzungen eine Übermittlung personenbezogener Daten an Landesbehörden zulassen, die die Daten weiter nach Maßgabe landesrechtlicher Vorschriften auf der Basis einer Landesgesetzgebungskompetenz verwenden. Über die Kompetenz hinsichtlich der Übermittlungsvorschrift hinaus steht dem Bund hier die Kompetenz zu, diejenigen Beschränkungen für die Datenverwendung bundesrechtlich vorzugeben, die wegen des Zusammenhanges zwischen Datenerhebung und Datenverwendung geboten sind, etwa wenn die Datenerhebung mittels eingriffsintensiver Erhebungsmethoden erfolgt ist und mit Rücksicht darauf für die weitere Verwendung besondere Einschränkungen gelten müssen. Die Datenverarbeitung durch die Landesbehörden unterliegt dann diesen bundesrechtlichen Vorgaben und im Übrigen dem Landesrecht[145]. 30

[143] S. *BVerfG*, Beschl. v. 27.5.2020 – 1 BvR 1873/13 u. 2618/13 – Bestandsdatenauskunft II, www.bverfg.de, Rn. 110 ff.

[144] → Oben Rn. 11.

[145] S. dazu *BVerfGE* 125, 260 (315 f., 344 ff., 355 f.); *BVerfG*, Beschl. v. 27.5.2020 – 1 BvR 1873/13 u. 2618/13 – Bestandsdatenauskunft II, www.bverfg.de, Rn. 130 ff.

2. Grundrechtsgewährleistungen

a) Anwendbarkeit nationaler Grundrechte

31 Soweit es sich im Datenschutzrecht um **unionsrechtlich vollvereinheitlichte Regelungen** handelt, greifen in aller Regel allein die Unionsgrundrechte. Sofern unionale Vorgaben mitgliedstaatliche **Regelungsaufträge oder Spielräume** enthalten, geht der *EuGH* davon aus, dass zu den Bindungen der europäischen Grundrechte unter bestimmten Voraussetzungen diejenigen mitgliedstaatlicher Grundrechte hinzutreten können.[146] Das *BVerfG* hat sich nunmehr so positioniert, dass mitgliedstaatliche Regelungen in Fällen, in denen das unionale Fachrecht der mitgliedstaatlichen Gestaltung einen hinreichend gehaltvollen Rahmen setzt, der erkennbar auch unter Beachtung der Unionsgrundrechte konkretisiert werden soll, zwar als Durchführung des Unionsrechts zu beurteilen sein könnten.[147] In solchen Fällen träten aber die Unionsgrundrechte zu den Grundrechten des GG hinzu, denn gestaltungsoffene Regelungen eröffneten Raum für Vielfalt. Das bedeute, dass primär diese Grundrechte anzuwenden seien, die auch „im Lichte" jener Grundrechte auszulegen seien.[148] Das Schutzniveau der Charta werde dabei in der Regel mitgewährleistet. Sofern sich diese Vermutung als widerlegt erweise, sei eine – dem BVerfG zustehende[149] – Prüfung auch am Maßstab der Unionsgrundrechte vorzunehmen.[150] Diese neue Linie des BVerfG hat Schwächen im Detail, ist aber in den Grundzügen überzeugend.[151] Seine beiden Entscheidungen zum „Recht auf Vergessen" werden auf jeden Fall dazu führen, dass das Datenschutzrecht aus zu engen Vorstellungen einer zentralistischen Harmonisierung gelöst und damit pluralistischer, dynamischer und anpassungsfähiger werden kann. Gerade auch **im Bereich der öffentlichen Verwaltung** verbleibt den **grundgesetzlichen Gewährleistungen** ein **beachtlicher Raum.**[152]

b) Inhalte und Zusammenspiel

32 Bei den grundgesetzlichen Gewährleistungsinhalten steht die **informationelle Selbstbestimmung** im Mittelpunkt. Im Volkszählungsurteil hat das BVerfG den Schutzbereich des aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleiteten Rechts auf informationelle Selbstbestimmung als die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu

---

[146] → Rn. 24.

[147] Zum Folgenden *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, www.bverfg.de, Rn. 45 ff. = BVerfGE 152, 152. Zur Linie zuvor vgl. *BVerfGE* 133, 277 – Antiterrordatei-Gesetz, Rn. 88 ff.

[148] Näher dazu, auch zu den methodischen Besonderheiten, *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, www.bverfg.de, Rn. 60 ff. Vgl. auch *Johannes Masing*, Einheit und Vielfalt des Europäischen Grundrechtsschutzes, JZ 2015, S. 477 (bes. 486).

[149] *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, www.bverfg.de, Rn. 72, unter Verweis auf *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 276/17 – Recht auf Vergessen II = BVerfGE 152, 216, s.a. → Rn. 24.

[150] *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, www.bverfg.de, Rn. 63 ff.

[151] Übergreifender *Masing*, Einheit (Fn. 148), S. 477 ff.

[152] Vgl. auch die Ausführungen in *BVerfG*, Beschl. v. 27.5.2020 – 1 BvR 1873/13 u. 2618/13 – Bestandsdatenauskunft II, www.bverfg.de, Rn. 83 ff.; Beschl. v. 10.11.2020 – 1 BvR 3214/15 – Antiterrordatei II, www.bverfg.de, Rn. 63 ff.; Beschl. v. 8.6.2021 – 1 BvR 2771/18, Rn. 23, 26 ff.

bestimmen"[153] beschrieben.[154] Dem Gegenstand nach ist dieses im Kern **abwehrrechtlich geschützte individuelle Entscheidungsrecht** daten- und informationsorientiert, der Reichweite nach ist es prozess- und verarbeitungsorientiert. Beim Eingriff ist es angesichts der nicht-linearen, vernetzten und vielschichtigen Prozesse der Informations- und Datenverarbeitung eine eigenständige Leistung herauszuarbeiten, welcher Schritt eigentlich als rechtsrelevante Aktion herauszukristallisieren ist.[155] Im Hinblick auf die Verfassungsmäßigkeit der erforderlichen gesetzlichen Ermächtigungsgrundlagen hat das BVerfG im Laufe seiner Rechtsprechung eine Fülle von Maßgaben entwickelt, zu denen die Grundsätze der Zweckfestlegung und der Zweckbindung, Kennzeichnungspflichten oder auch Datensicherheitsstandards gehören.[156] Nicht selten werden Maßgaben in wenig überzeugender Weise dem Übermaßverbot zugeordnet.[157] Das lange Zeit in dieser Fassung recht fest etablierte Recht auf informationelle Selbstbestimmung ist allerdings auch in der verfassungsgerichtlichen Rechtsprechung **mittlerweile im Fluss.** Zunächst haben sich die genetischen Grundlagen, die sich in der dem Volkszählungsurteil vorausgehenden Rechtsprechung finden, an zentralen Stellen verändert.[158] Dann haben einige Entscheidungen die Schutzfunktionen und die Schutzreichweite in mehr oder weniger geglückter Weise austariert.[159] Zuletzt hat das Gericht das Recht auf informationelle Selbstbestimmung deutlich modifiziert: Im Verhältnis zwischen Privaten[160] gewährleistet es kein allgemeines oder gar umfassendes Selbstbestimmungsrecht über die Nutzung der eigenen Daten, sondern „die Möglichkeit, in differenzierter Weise darauf Einfluss zu nehmen, in welchem Kontext und auf welche Weise die eigenen Daten anderen zugänglich sind und von ihnen genutzt werden, und so über der eigenen Person geltende Zuschreibungen selbst substantiell mitzuentscheiden".[161]

---

[153] *BVerfGE* 65, 1 (42 f.). Zum Schutz auch juristischer Personen *BVerfGE* 118, 168 (203 f.). Im Anschluss an das Volkszählungsurteil haben die Landesverfassungen einen solchen Schutz in unterschiedlichen Textfassungen verankert: Art. 33 BerlinVerf, 11 BrandenbVerf, 12 Abs. 3–5 BremVerf., 6 Abs. 1–2 MecklenbVorpVerf, 4 Abs. 2 NWVerf, 4a RheinlPfalzVerf, 2 S. 2 SaarlVerf, 33 SächsVerf, 6 Abs. 1 SachsAnhVerf, 6 Abs. 2–4 ThürVerf.

[154] Ausf. Analyse bei *Albers*, Selbstbestimmung (Fn. 31) m. w. N.

[155] Vgl. *BVerfGE* 100, 313 (366 f.); *BVerfG*, Beschl. v. 18.12.2018, 1 BvR 142/15 – Automatisierte Kennzeichenkontrolle, www.bverfg.de, Rn. 42 ff.

[156] Zu den Maßgaben etwa *BVerfGE* 115, 320 (359 ff.); 120, 378 (407 ff.); 125, 260 (325 ff.); *BVerfG*, Urt. v. 20.4.2016, 1 BvR 966/09 u. 1140/09, www.bverfg.de, Rn. 103 ff.; Beschl. v. 18.12.2018, 1 BvR 142/15, www.bverfg.de, Rn. 92 ff. Vgl. näher zum Erfordernis der Zweckfestlegung und ihren Funktionen *BVerfGE* 118, 168 (187 f.); 120, 378 (408 ff., 429, 431 f.); zur Gewährleistung eines besonders hohen Standards der Datensicherheit durch Verpflichtungen Privater im Falle der „vorsorglich anlasslosen" Datenspeicherung *BVerfGE* 125, 260 (325 ff.). Zum Schutz eines Kernbereichs privater Lebensgestaltung s. *BVerfGE* 120, 274 (335 ff.); *BVerfG*, Urt. v. 20.4.2016, 1 BvR 966/09 u. 1140/09, www.bverfg.de, Rn. 119 ff. Zu Kenntnisrechten BVerfGE 120, 351 (362 ff.); *BVerfG*, Urt. v. 20.4.2016, 1 BvR 966/09 u. 1140/09, www.bverfg.de, Rn. 134 ff.

[157] Kritisch *Albers*, Bündel (Fn 140), S. 19.

[158] *BVerfGE* 97, 125 (146 ff.); 97, 391 (403 ff.); 101, 361 (382); 120, 180 (199); vgl. dazu *Marion Albers*, Grundrechtsschutz der Privatheit, DVBl 2010, S. 1061 (1065 f.).

[159] *BVerfGE* 115, 320 (342 ff.); 118, 168 (184 f.); 120, 274 (312, 344 f.); 120, 351 (360 ff.).

[160] Auch unter Berücksichtigung der Dogmatik „mittelbarer Drittwirkung" hat ein individuelles Entscheidungsrecht über die Preisgabe und Verwendung persönlicher Daten hier immer inhaltliche und dogmatische Probleme bereitet.

[161] *BVerfG*, Beschl. v. 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, www.bverfg.de, Leitsatz 3 und Rn. 83 ff. Zur Abgrenzung von Datenschutz- und Äußerungsrecht zuvor auch *Schimke*, Medienprivileg (Fn. 78), S. 155 (bes. 157 ff.).

Diese Formulierung ist allerdings ihrerseits nur vor dem Hintergrund des entschiedenen Falles zu verstehen. In der verfassungsgerichtlichen Abgrenzung der Aussagen im Hinblick auf das Verhältnis unter Privaten gegen diejenigen im Hinblick auf das Verhältnis zum Staat scheint ein zu traditionelles Staatsverständnis durch. Auch hier sind allerdings Modifikationen erkennbar.[162] Die Grundrechtsgewährleistungen müssen noch passender ausgearbeitet werden.

33 Auch angesichts der Koordinationserfordernisse mit den unionalen Grundrechtsvorgaben ist es insgesamt sinnvoll, ein **vielschichtiges Bündel von Maßgaben und Rechten** auszuarbeiten, das über das Zusammenspiel mehrerer Gewährleistungen im Rahmen einer Zwei-Ebenen-Konzeption entwickelbar ist.[163] In der Sache hat man nämlich mit **verschiedenartigen Schutzerfordernissen** zu tun. In grober Differenzierung geht es auf einer grundlegend-vorgelagerten Ebene um das Problem allumfassender, unbegrenzter und intransparenter Informations- und Datenverarbeitungen, das von Anbeginn an zu den zentralen Themen des Datenschutzes gehörte.[164] Hinzu kommen Schutzerfordernisse wegen der Gefährdungslagen in konkreten Kontexten, die sich erst dann präzise erfassen lassen, wenn jenes Problem gelöst ist. Auf der **grundlegend-vorgelagerten Ebene** schützt die Kombination des **Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG**[165] die Grundrechtsträger vor Informations- und Datenverarbeitungen, die weitgehend ungebunden, grenzenlos und undurchschaubar in immer neuen Zusammenhängen stattfinden und die sich ihren Kenntnis-, Einfluss- und Partizipationschancen entziehen, obwohl die Informationen von ihnen handeln. Daraus resultieren **Regulierungsanforderungen an die Gesetzgebung** und im Folgeschritt **Anforderungen an die Verwaltung**, die mehrdimensional, problembezogen-vielfältig und dynamisch zu entwickeln und zu konkretisieren sind.[166] Ihre Umsetzung führt dazu, dass **auf einer zweiten Ebene** thematisch spezifizierte **Freiheitsgewährleistungen**, die man nunmehr kontext- und folgenorientiert konkretisieren kann, Vorgaben an genau der Stelle der Verarbeitungsprozesse setzen, an der ein von ihnen abgedeckter Schutzbedarf besteht.

34 Im Ergebnis hat man mit einer **breiten Basis grundrechtlicher Gewährleistungen** und mit deren **Zusammenspiel** zu tun.[167] Vor dem Hintergrund des

---

[162] S. die Formulierungen in *BVerfG*, Beschl. v. 18.12.2018 – 1 BvR 142/15 – Automatisierte Kennzeichenkontrolle, www.bverfg.de, Rn. 37 ff.; Beschl. v. 27.5.2020 – 1 BvR 1873/13 u. 2618/13 – Bestandsdatenauskunft II, www.bverfg.de, Rn. 92; Beschl. v. 10.11.2020 – 1 BvR 3214/15 – Antiterrordatei II, www.bverfg.de, Rn. 71; Beschl. v. 1.12.2020 – 2 BvR 916/11 u. 636/12 – elektronische Fußfessel, www.bverfg.de, Rn. 198.

[163] Ausf. zum Ansatz *Albers*, Selbstbestimmung (Fn. 31), S. 353 ff.; *Marion Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR, 2. Aufl., Bd. II, 2012, § 22 Rn. 69 ff.

[164] S. auch *Daniel Solove*, Privacy and Power: Computer Databases and Metaphors for Information Privacy, Stanford Law Review Vol. 53 (2001), S. 1393 (1413 ff.).

[165] Es versteht sich, dass die Aussagen dieser Normenkombination bei diesem Ansatz nicht im Sinne der verfassungsgerichtlichen Konzeption des Rechts auf informationelle Selbstbestimmung, sondern in inhaltlich und dogmatisch eigenständiger Weise zu lesen sind.

[166] Die Herleitung subjektiver Rechte ist mit diesem Ansatz nicht aus-, sondern in vielfältiger Form eingeschlossen, ausf. *Albers*, Selbstbestimmung (Fn. 31), S. 39 ff., 484 ff., m. w. N. Vgl. ansonsten auch zu den Vorgaben des Art. 8 GRCh → Rn. 26.

[167] Auch das BVerfG zieht, freilich oft ohne vertiefende Erörterung, weitere Freiheitsgewährleistungen heran, bspw. *BVerfGE* 100, 313 (365); 122, 342 (359, 368 ff.); *BVerfG*, Urt. v. 19.5.2020, 1 BvR 2835/17, www.bverfg.de, Rn. 111. Ansonsten sind auch spezielle Facetten des Persönlichkeitsschut-

Internets spielt vor allem das **Telekommunikationsgeheimnis** des Art. 10 GG eine zunehmende und relativ eigenständige Rolle. Die Norm gewährleistet – dies in bestimmten Schutzdimensionen auch im Hinblick auf Ausländer im Ausland[168] – die Freiheit und Unverletzlichkeit der auf Vermittlungstechniken und -netze sowie auf Vermittlungsleistungen Dritter angewiesenen Individualkommunikation.[169] In Eingriffsfällen stellt das Bundesverfassungsgericht Anforderungen im Hinblick auf Zweckfestlegung und Zweckbindung, Einschreit-, Erhebungs-, Speicherungs- oder Übermittlungsschwellen, Schutzvorkehrungen im Verarbeitungszusammenhang, technische und organisatorische Vorkehrungen etwa zwecks Datensicherheit, Wissensrechte der Grundrechtsträger oder eine institutionelle Kontrolle.[170] Die nicht zuletzt aus der Privatisierungsfolgenverantwortung resultierenden Ausgestaltungs- und Schutzpflichten spiegeln sich in Vorschriften wider, die zur Beachtung des Fernmeldegeheimnisses verpflichten, Anforderungen an den Umgang mit Bestands- und Verkehrsdaten stellen oder Vorgaben zur Möglichkeit einer anonymen oder pseudonymen Nutzung von Telemediendiensten treffen.[171] Die **mehrdimensionalen und vielfältigen Regelungs- und Konkretisierungserfordernisse,** die sich aus den Grundrechtsnormen ergeben, sind schon für sich genommen und erst recht im Zusammenspiel mit dem unionalen Recht anspruchsvoll.

C. Regulierung und Gestaltung des Umgangs mit personenbezogenen Informationen und Daten

I. Strukturen und Regelungsmuster

1. Zusammenspiel unionalen und mitgliedstaatlichen Rechts

Die mit der zunehmenden Europäisierung entstandenen Regelungsstrukturen zeichnen sich durch ein komplexes Zusammenspiel unionaler und mitgliedstaatlicher Vorgaben aus. Das Recht des Umgangs mit personenbezogenen Informationen und Daten ist auf unionaler Ebene in einen übergreifenden Regelungskomplex eingebettet.[172] Es selbst setzt sich – neben den Vorgaben unionaler Grundrechte – aus **allgemeinen** und **infrastrukturbezogenen oder sektoralen sekundärrechtlichen Vorschriften** zusammen. Angesichts der Gestaltungsspiel- 35

zes relevant, etwa das Recht auf Achtung der Privatsphäre, das Recht am eigenen Bild, das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, dazu *BVerfGE* 120, 274 (302ff.); BVerfG, Beschl. v. 8.6.2021, 1 BvR 2771/18, Rn. 29, 33ff.; *Markus Hauser*, Das IT-Grundrecht, 2015, oder das Recht auf Vergessen(werden), s. BVerfGE 152, 152, und 152, 261; außerdem *Anna Schimke*, Vergessen als neue Kategorie im Recht, in: Arnold Autengruber et al., Zeit im Recht – Recht in der Zeit, 2016, S. 87ff.

[168] *BVerfG*, Urt. v. 19.5.2020, 1 BvR 2835/17, www.bverfg.de, Rn. 87ff.

[169] Der eingriffsabwehrrechtliche Schutz der Geheimnisqualität der Kommunikationsinhalte und -umstände greift gerade und nur in der Vermittlungsphase, erstreckt sich mit diesem Bezugspunkt in der Reichweite dann aber über die Kenntnisnahme hinaus auf die daran anknüpfenden Informations- und Datenverarbeitungen. Im Rahmen des Internet kann die Abgrenzung der Anwendungsbereiche der einschlägigen Grundrechte erhebliche Schwierigkeiten bereiten. Zur Schutzdimension des Art. 10 GG BVerfG, Beschl. v. 8.6.2021, 1 BvR 2771/18, Rn. 32.

[170] Zu Eingriffen und Anforderungen z.B. *BVerfGE* 100, 313 (373ff.); 125, 260 (325ff.); 129, 208 (240ff.); 130, 151 (183ff.); *BVerfG*, Urt. v. 19.5.2020, 1 BvR 2835/17, www.bverfg.de, Rn. 155ff.

[171] Vgl. §§ 201ff. StGB, §§ 3ff. TTDSG.

[172] → Rn. 3.

räume, die den Mitgliedstaaten in der DSGVO und in anderweitigem Sekundärrecht eingeräumt sind, treten zu den EU-Vorgaben das **Bundes- und Landesdatenschutzrecht** hinzu. Dazu gehören die **allgemeinen Datenschutzgesetze**, also das angepasste BDSG[173] und die jeweils reformierten LDSGe, und zahlreiche **bereichsspezifische Bestimmungen.** Die einschlägigen Vorschriften sind somit zusammen zu lesen. Dabei kann die kompetenzgerechte Abgrenzung der Anwendungsbereiche erhebliche Schwierigkeiten bereiten.

36 Die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU wird in der **Verordnung (EU) Nr. 2018/1725** geregelt.[174] Für die Mitgliedstaaten liefert die **DSGVO** die allgemeinen unionsrechtlichen Vorgaben[175]. Als Verordnung im Sinne des Art. 288 Abs. 2 AEUV ist sie grundsätzlich unmittelbar anwendbar. Sie zeichnet sich aber dadurch aus, dass sie den Mitgliedstaaten mittels Öffnungen zahlreiche Regelungsaufträge, Regelungsmöglichkeiten und Gestaltungsspielräume zuweist.[176] Neben der DSGVO gibt es zahlreiche **bereichsspezifische** Vorgaben. Nicht immer, aber häufig haben sie Richtlinienform und sind umsetzungsbedürftig. Beispielhaft hervorheben kann man hier die **e-privacy-Richtlinie**[177], die den Bereich der elektronischen Kommunikation betrifft und künftig durch eine Verordnung abgelöst werden soll. Soweit sie hinsichtlich der Verarbeitung der Daten natürlicher Personen abschließende Pflichten enthält, die dasselbe Ziel verfolgen wie die Vorgaben der DSGVO, geht sie dieser vor[178]. Seit der Nichtigkeitserklärung der Vorratsdatenspeicherungsrichtlinie durch den EuGH wird die einschlägige Rechtslage durch Art. 15 dieser Richtlinie geprägt[179]. Die **Datenschutzrichtlinie für Polizei und Strafjustiz**[180], die zu den zahlreichen sekundärrechtlichen Datenschutzvorschriften im zunehmend europäisierten Feld des Sicherheitsrechts gehört, ist in den Grundmustern an die DSGVO angelehnt und zeitlich parallel in das Rechtsetzungsverfahren gebracht worden. Sie setzt Mindeststandards unter anderem für die Festlegung von Gegenstand und Zwecken der Datenverarbeitung, für die Erforderlichkeit, für Zweckänderungen, für die Verarbeitung sensitiver Daten, für die kategoriale Differenzierung in Anspruch genommener Personen, für automatisierte Einzelentscheidungen und Profilingmaßnahmen, für Datenübermittlungen vor allem an Drittstaaten und in-

---

[173] Art. 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU- DSAnpUG-EU) vom 30.6.2017, BGBl I 2097.

[174] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates v. 23.10.2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr […], ABlEU L 295 v. 21.11.2018, S. 39. Nähere Erörterungen im Kontext des Whistleblowings bei *Christoph Aust*, Der Schutz personenbezogener Daten eines Whistleblowers in der Europäischen Kommission, 2020, S. 88 ff.

[175] → Fn. 20.

[176] Gelegentlich wird sie daher als „Hybrid" aus Verordnung und Richtlinie bezeichnet, so *Jürgen Kühling/Mario Martini*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, S. 448 (449). Zu den Öffnungen → Rn. 59.

[177] → Fn. 22.

[178] Art. 95 DSGVO.

[179] *EuGH* (GK), Urt. v. 8.4.2014, C-293/12 and C-594/12, sowie zu Art. 15 RL 2002/58/EG die Folgeentscheidungen *EuGH* (GK), Urt. v. 21.21.2016, C-203/15 und C-698/15 – Tele2 Sverige u.a.; Urt. v. 6.10.2020, C-511, 512 u. 520/18 – Quadrature du Net u. a.; Urt. v. 2.3.2021, C-746/18, Rn. 51 ff. – H. K.; alle abrufbar unter http://curia.europa.eu.; s. dazu insgesamt auch *Albers*, Surveillance (Fn. 17), S. 94 ff.

[180] → Fn. 21.

ternationale Organisationen, für Informationsrechte betroffener Personen und für die Befugnisse der Datenschutzaufsichtsbehörden.[181] Für die Bundespolizeien und andere Stellen i.S.d. § 45 BDSG ist sie hinsichtlich „vor die Klammer" gezogener Bestimmungen im BDSG, ansonsten im bereichsspezifischen Recht umgesetzt worden.[182] Mittelbar relevant sind etwa die **NIS-Richtlinie** oder der **Rechtsakt zur Cybersicherheit.**[183]

Im mitgliedstaatlichen Datenschutzrecht enthalten das **Bundes-** und **die Landesdatenschutzgesetze** die allgemeinen Vorgaben. Dabei hat das BDSG in Bezug auf öffentliche Stellen des Bundes einen gegenüber der DSGVO erweiterten sachlichen Anwendungsbereich, indem es nicht darauf ankommt, ob Daten manuell, in Akten oder elektronisch verarbeitet werden.[184] Es bezieht sich nicht nur auf die DSGVO, sondern auch auf die Datenschutzrichtlinie für Polizei und Strafjustiz und auf andere Felder. §§ 1 bis 21 BDSG regeln gemeinsame Bestimmungen, etwa die allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen und Vorschriften zu dem oder der Bundesbeauftragten für den Datenschutz. §§ 22 bis 44 BDSG enthalten Bestimmungen zur Ergänzung der DSGVO und zur Ausfüllung ihrer Öffnungsklauseln und impliziten Öffnungen, etwa Regelungen für die Verarbeitung besonderer Kategorien personenbezogener Daten, für besondere Verarbeitungssituationen, zu den Betroffenenrechten und zu Sanktionen. Die partielle Wiedergabe der Vorgaben der DSGVO in nationalen Regelungen lässt sich meist mit Kohärenz-und Verständlichkeitserwägungen rechtfertigen und verstößt daher nicht gegen das Normwiederholungsverbot.[185] Die Umsetzung der Datenschutzrichtlinie für Polizei und Strafjustiz leisten – neben den einschlägigen gemeinsamen Bestimmungen – die Vorschriften des dritten Teils des BDSG, soweit sie nicht in bereichsspezifischen Gesetzen erfolgt und nicht Ländersache ist. Für 37

[181] Übergreifender dazu *Marion Albers*, Datenschutzbestimmungen der Polizei- und Nachrichtendienstgesetze des Bundes, in: Heinrich A. Wolff/Stefan Brink (Hrsg.); Beck'scher Online-Kommentar Datenschutzrecht, Stand 11/2021 (38. Ed.), DSGVO, Syst. L, Rn. 46 ff.; *Matthias Bäcker*, Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hermann Hill/Dieter Kugelmann/Mario Martini (Hrsg.), Perspektiven der digitalen Lebenswelt, Baden-Baden, 2017, S. 63 (68 ff.); *Robert Weinhold/Paul C. Johannes*, Europäischer Datenschutz in Strafverfolgung und Gefahrenabwehr – Die neue Datenschutz-Richtlinie im Bereich Polizei und Justiz sowie deren Konsequenzen für deutsche Gesetzgebung und Praxis, DVBl 2016, S. 1501 (1501 ff.).

[182] Zu inhaltlichen Fragen, Bestimmtheitsproblemen und Koordinationsschwierigkeiten hinsichtlich der Umsetzung *Marion Albers/Anna Schimke*, in: BeckOK (Fn. 181), BDSG, § 48, Rn. 6 ff.; § 49, Rn. 7 ff.

[183] RL 2016/1184/EU des Europäischen Parlaments und des Rates v. 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABlEU L 194 (v. 19.7.2016), S. 1; Verordnung (EU)2019/881des Europäischen Parlaments und des Rates vom 17. 4 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik [...], ABlEU L 151/15 (v. 7.6.2019).

[184] S. § 1 Abs. 1 BDSG. Diese Differenz relativiert sich allerdings durch die Entwicklung einer digitalisierten Verwaltung, dazu → Rn. 14 m.N.

[185] Dass dem nationalen Gesetzgeber eine wörtliche Wiederholung auch nur von Teilen einer unionalen Verordnung grdstzl. nicht erlaubt ist, soll u.a. eine Verschleierung der Herkunft von Regelungen verhindern. Wörtliche Übernahmen sind jedoch möglich, sofern sie notwendig sind, um die Kohärenz der mitgliedstaatlichen Normen zu ermöglichen oder deren Verständlichkeit im jeweiligen Zusammenhang zu erleichtern. Vgl. auch *Holger Greve*, Das neue Bundesdatenschutzgesetz, NVwZ 2017, S. 737 (743).

die öffentlichen Stellen der Länder wird das BDSG regelmäßig durch die allgemeinen **Landesdatenschutzgesetze** verdrängt.[186] Deren grundlegende Bausteine orientieren sich primär an den Vorgaben der DSGVO. Im Rahmen der verbleibenden Gestaltungsspielräume lehnen sie sich teilweise an Muster des BDSG an; allerdings sind durchaus auch landesspezifische Modifikationen und gelegentlich eine detailliertere Ausgestaltung der Anforderungen zu verzeichnen.[187]

38 Auf Bundes- und auf Landesebene gibt es im Übrigen **zahlreiche bereichsspezifische Datenschutzbestimmungen**, etwa im Telekommunikations- und Telemediendatenschutzrecht, im Recht der Nachrichtendienste und im Polizeirecht, im Pass- und im Personalausweisrecht oder im Sozialrecht. Diese speziellen Bestimmungen werden ebenfalls erheblich durch Unionsrecht beeinflusst, sei es durch Maßgaben der DSGVO, sei es durch solche bereichsspezifischer Verordnungen oder Richtlinien, und sie müssen daran angepasst und unionsrechtskonform ausgelegt werden. Bereichsspezifische Vorschriften verdrängen das allgemeine Datenschutzrecht, soweit sie abschließende und erschöpfende Vorgaben enthalten.

2. Regelungsmuster der DSGVO

a) Schutzzwecke und Ziele

39 Die **„doppelte Finalität"**, die die Zielbeschreibung des Art. 1 Abs. 1 DSGVO kennzeichnet – zum einen die Sicherstellung des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum anderen der freie Verkehr personenbezogener Daten innerhalb der EU – gewinnt durch die Einbettung in die Gesamtstrategie der Union noch einmal einen reicheren Gehalt. Hinter ihr stehen nicht zuletzt Kompetenzgründe und die Entstehungsgeschichte europäischen Datenschutzes.[188] In ihr steckt kein schlichtes Nebeneinander und auch kein grundsätzliches Spannungsverhältnis.[189] „Daten"-schutz umfasst ein grundrechtlich geprägtes und zudem durch Gesetzgebungsentscheidungen ergänzbares Bündel an Schutzgütern, das sich keineswegs auf eine Privatsphäre im Sinne einer Abschottung beschränkt.[190] Datenverkehr ist dabei nicht notwendig aus-, sondern unter Umständen eingeschlossen, dies dann allerdings in bestimmter Gestalt. Zielkonflikte tauchen freilich ebenfalls auf. Der DSGVO geht es vor allem auch darum, ein gleichwertiges Datenschutzniveau in allen Mitgliedsstaaten sicherzustellen, damit der für den Binnenmarkt, aber auch für die sonst zusammenwachsende Union wichtige grenzüberschreitende Austausch personenbezogener Daten möglich ist. Dass es angesichts der Konkretisierungs- und Abstimmungserfordernisse und der Öffnungen für mitgliedstaatliches Recht keinen vollständig einheitlichen Rechtsraum gibt, ist Folge

---

[186] Zu den jeweiligen Anwendungsbereichen s. § 1 Abs. 1 S. 1 Nr. 2 BDSG.

[187] Näher zu den Möglichkeiten und Problemen *Dieter Kugelmann*, Anwendungsbereich und Spielräume der Landesdatenschutzgesetze, in: Seckelmann (Fn. 65), S. 423 ff.

[188] Ausf., auch mit Hinweis auf Folgeprobleme *Orla Lynskey*, The foundations of EU data protection law, 2015, S. 46 ff.

[189] S. auch *Hornung/Spiecker gen. Döhmann* (Fn. 5), Art. 1 Rn. 20 ff.

[190] → Rn. 19 ff., 25 ff., 32 ff. Vgl. außerdem die auf die Ausarbeitung relevanter Risiken gerichteten Analysen und Überlegungen bei *Stefan Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014.

sowohl der Struktur der Union als auch der Charakteristika des Datenschutzrechts. Das neue BDSG enthält keine übergreifende Zielbeschreibung mehr.

b) Anwendungsbereiche

Nach Art. 2 Abs. 1 DSGVO gilt die Verordnung für die **ganz oder teilweise automatisierte Verarbeitung** personenbezogener Daten sowie für die **nichtautomatisierte Verarbeitung** personenbezogener Daten, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen.[191] Der Begriff der Verarbeitung wird in Art. 4 Nr. 2 DSGVO als Oberbegriff konzipiert, dem gegeneinander abgrenzbare Verarbeitungsphasen zu- und untergeordnet werden.[192] Die in der Legaldefinition aufgelisteten Phasen sind nicht zu starr und nicht abschließend zu verstehen. Wie man Phasen beschreibt und welche Phasen rechtlich relevant sind, hängt nicht zuletzt von der eingesetzten Technik und vom Kontext ab.[193] Ausgenommen aus der Geltung sind Verarbeitungen im Rahmen von Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrecht fallen.[194] Ebenfalls ausgeklammert, aber Gegenstand bereichsspezifischer Vorgaben sind Verarbeitungen im Rahmen von Tätigkeiten, die in den Bereich der gemeinsamen Außen- und Sicherheitspolitik fallen, und Verarbeitungen im Bereich der Straftatenbekämpfung und Gefahrenabwehr.[195] 40

Die Verordnung gilt für die Verarbeitung gerade **personenbezogener Daten.** Art. 4 Nr. 1 DSGVO liefert die Legaldefinition: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen und die insofern „betroffene Person" ist.[196] Als identifizierbar wird nach dem Normtext des Art. 4 Nr. 1 DSGVO eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, identifiziert werden kann. Mit den in der Norm aufgelisteten Beispielen für eine Kennung werden freilich nur Identifikatoren benannt. Die Legaldefinition und die Erwägungsgründe deuten darauf hin, dass das wesentliche Problem in der Identifizierbarkeit einer Person gesehen wurde[197]. Das kann sich simpel gestalten, wenn beispielsweise bestimmte Angaben unmittelbar mit Identifikatoren wie dem Namen verknüpft werden.[198] Sofern ein Personenbezug über mehrere Operationen unter Beteili- 41

[191] Zum Dateisystem Art. 4 Nr. 6 DSGVO. Der EuGH legt ein sehr weites Verständnis der letztgenannten Fallgruppe zu Grunde: Urt. v. 10.7.2018, C-25/17 – Zeugen Jehovas, abrufbar unter http://curia.europa.eu. Zu den Abgrenzungsstreitigkeiten in der Literatur etwa *Rüpke/von Lewinski/Eckhardt*, Datenschutzrecht (Fn. 36), § 8 Rn. 22 ff.

[192] Vgl. (zur entsprechenden Regelung der DSRL) *Christopher Kuner*, European Data Protection Law: Corporate Compliance and Regulation, 2. Aufl. 2007, S. 74: "it is difficult to conceive of any operation performed on personal data in electronic commerce which would not be covered by it".

[193] S. → Rn. 11.

[194] Zur darauf bezogenen Rechtsprechung des *EuGH* s. bereits → Rn. 23. Näher noch *EuGH*, Urt. v. 22.6. 2021, C-439/19, Rn. 61 ff., http://curia.europa.eu.

[195] S. Art. 2 Abs. 2 DSGVO.

[196] Für juristische Personen greift die DSGVO grundsätzlich nicht, vgl. EG 14. Eine Ausnahme hiervon soll lediglich gelten, sofern, wie bei einer Ein-Personen-Gesellschaft, die Trennung von geschäftlichen und personenbezogenen Daten nicht möglich ist.

[197] Vgl. EG 26. Deutlich breiter dagegen die *Art.-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", angenommen am 20.6.2007, 01248/07/DE, WP136.

[198] S. hierzu *EuGH*, C-465/00, Slg. 2003, I-4989, Rn. 64 – Österreichischer Rundfunk: Offenlegung der Einkommensdaten von Arbeitnehmern gegenüber dem Rechnungshof; *EuGH*, Gutachten v. 26.7.2017, 1/15 – PNR-Abkommen, Rn. 121 f. für Passagierdaten.

gung unterschiedlicher Akteure hergestellt werden kann, kann es dagegen schwer fallen zu entscheiden, unter welchen Voraussetzungen die hinter bestimmten Daten stehende Person im datenschutzrechtlichen Sinne in Bezug auf welchen Akteur als bestimmbar anzusehen ist. Beispiele sind die IP-Adresse oder nicknames.[199] Aufmerksamkeit verdient jedoch darüber hinaus die Frage, welche Daten sich überhaupt auf eine identifizierte oder identifizierbare Person beziehen. Der Bezug von Daten auf Personen ist keineswegs immer schon in einer Weise gegeben, dass es nur um deren Identifizierbarkeit ginge. Er wird vielmehr in bestimmten Kontexten als Ergebnis einer sinngehaltszuschreibenden Leistung tatsächlich oder potenziell und gegebenenfalls erstmals hergestellt; auch gestaltet er sich vielfältig und von unterschiedlicher Dichte.[200] Dass Antworten darauf, wann sich Daten in datenschutzrechtlich relevanter Weise auf bestimmte Personen beziehen (können), nicht nur (akteurs-)relativ, sondern auch kontextabhängig sind und Wahrscheinlichkeitsannahmen, Prognosen und wertende Beurteilungen erfordern können, macht ein wesentliches **Abgrenzungs- und Anwendungsproblem des Datenschutzrechts** aus.

42 In Reaktion auf die Entwicklung der Kommunikation über das Internet und auf die global player mit ihren Gestaltungsmöglichkeiten reicht der **räumliche Anwendungsbereich** nach Art. 3 DSGVO über das gegenstandsbezogen zugeschnittene **Sitzlandprinzip** hinaus. Nach diesem Prinzip sind eine Niederlassung des Verantwortlichen oder Auftragsverarbeiters in der Union und eine Verarbeitung im Rahmen der Niederlassung maßgebend.[201] Ob die tatsächliche Verarbeitung der Daten dabei innerhalb der Union stattfindet, ist unerheblich.[202] Die Verordnung ist darüber hinaus im Falle nicht in der EU niedergelassener Verantwortlicher anwendbar, soweit die Datenverarbeitung im Zusammenhang damit steht, den betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten (unabhängig von deren Entgeltlichkeit) oder das in der Union erfolgende Verhalten der betroffenen Personen, etwa durch Tracking-Methoden, zu beobachten. Dieses **Marktortprinzip** ist einer der Mechanismen, mit denen die DSGVO unter den Bedingungen des Internets ihre Geltungskraft im Hinblick auf Adressaten außerhalb des unionalen Territoriums zu verstärken sucht.[203] Als Teil unionaler Datenschutzpolitik kommt ihm „strategische Bedeutung für die Behauptung europäischer Interessen in der globalen Arena"[204] zu.

---

[199] Zur Personenbezogenheit von IP-Adressen s. etwa *EuGH*, Urt. v. 24.11.2011, C-70/10, Rn. 88 – Scarlet Extended; Urt. v. 19.10.2016, C-582/14, Rn. 32ff. – dynamische IP-Adressen; zu Videoaufnahmen *EuGH*, Urt. v. 11.12.2014, C-212/13, Rn. 22f.; jeweils abrufbar unter http://curia.europa.eu.

[200] Zum Problem bereits oben → Rn. 16.

[201] Zur Beurteilung, wann eine Verarbeitung „im Rahmen" einer Niederlassung stattfindet, s. *EuGH*, Urt. v. 13.5.2014 – C-131/12, Google Spain; Urt. v. 5.6.2018 – C-210/16, Rn. 29ff. – Fanpage, beide unter http://curia.europa.eu.

[202] Zum etwas komplexeren Fall der räumlichen Reichweite des Rechts auf Auslistung aus den Ergebnislisten territorial differenzierter Suchmaschinenversionen *EuGH*, Urt. v. 24.9.2019, C-507/17, abrufbar unter http://curia.europa.eu, Rn. 54ff.

[203] Ausführlicher *Veit*, Safeguarding (Fn. 15), S. 464ff.

[204] *Cornils*, Entterritorialisierung (Fn. 15), S. 421.

c) Regelungssystematik und Regelungselemente

aa) Überblick

Normadressaten der DSGVO sind alle, denen sie in ihrem Anwendungsbereich Kompetenzen, Pflichten oder Rechte zuweist.[205] Angesichts der in erheblichem Umfang auf eine Prozeduralisierung setzenden Regelungskonzeption schließt dies Gesetzgebungsorgane, Aufsichtsbehörden und den Europäischen Datenschutzausschuss, regelsetzende Verbände, Verantwortliche, Auftragsverarbeiter und betroffene Personen ein. Ein prozeduralisiertes, reflexives Verständnis der Verordnung selbst spiegelt sich in der Verpflichtung zu ihrer regelmäßigen **Evaluation** wider (Art. 97 DSGVO).[206] 43

Allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten finden sich zunächst in Gestalt von **Grundsätzen**, die Art. 5 DSGVO in abstrakt-übergreifender Weise festhält. Die bündelnde Bezeichnung als „Grundsätze" hat einen entstehungsgeschichtlich-systematischen Hintergrund.[207] Im Näheren erweist sie sich als nur begrenzt treffend und kann zu einem erheblichen Einordnungs- und Interpretationsbedarf führen. Im Anschluss daran regeln Art. 6 bis 11 DSGVO weitere **Rechtmäßigkeitsvoraussetzungen.** Diese legen die Bedingungen der Zulässigkeit einer Verarbeitung fest, unterstellen besondere Kategorien personenbezogener Daten („sensible Daten") verschärften Anforderungen und enthalten dabei in unterschiedlichem Umfang Öffnungen zu Gunsten einer mitgliedstaatlichen Regelung.[208] Für **besondere Verarbeitungssituationen** sehen Art. 85 ff. DSGVO Rahmenvorgaben vor, deren Regelung mehr oder weniger weitreichend der mitgliedstaatlichen Kompetenz zugeordnet wird oder ist. Das betrifft etwa den Zugang der Öffentlichkeit zu amtlichen Dokumenten mitgliedstaatlicher Behörden, Beschäftigtendaten oder nationale Kennziffern. Während es diese in einigen Mitgliedstaaten bereits seit längerem gibt, soll in Deutschland im Zuge der Digitalisierung der Verwaltung die Steueridentifikationsnummer zu einem registerübergreifenden einheitlichen Identifikationsmerkmal umgebaut werden.[209] 44

Die Vorgaben zur Regulierung der Verarbeitung werden in Art. 12 bis 23 DSGVO um mehrstufig und vielfältig angelegte Vorgaben über die **Rechte der Betroffenen** ergänzt. Diese werden detaillierter geregelt als in der früheren Datenschutzrichtlinie, zum Beispiel im Hinblick auf automatisierte Entschei- 45

---

[205] S. als ersten Bericht die Mitteilung der *Europäischen Kommission* vom 24.6.2020, Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel –zwei Jahre Anwendung der Datenschutz-Grundverordnung, COM(2020) 264 final. Überblick bei *Alexander Roßnagel*, Evaluation der Datenschutz-Grundverordnung. Verfahren – Stellungnahmen – Vorschläge, DuD 2020, S. 287 (287 ff.).

[206] S. a. *Hornung/Spiecker gen. Döhmann* (Fn. 5), Art. 1 Rn. 10.

[207] Die EU-Datenschutz-Richtlinie hat sich hier an die Datenschutzkonvention angeschlossen, vgl. *Albers*, Selbstbestimmung (Fn. 31), S. 297 ff., 321 ff.

[208] Näher noch → Rn. 59.

[209] S. das Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG) v. 28.3.2021, BGBl. I S. 591, und hierzu näher den Gesetzentwurf der Bundesregierung zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz –RegMoG), BTDrucks. 19/24226, sowie die Beschlussempfehlung und den Bericht des Ausschusses für Inneres und Heimat, BT-Drucks. 19/26247.

dungen. Ergänzt sind etwa das sog. „Recht auf Vergessenwerden" oder das Recht auf Datenportabilität. In bestimmtem Umfang werden die Rechte bereits begrenzt. Art. 23 Abs. 1 DSGVO lässt unter bestimmten Voraussetzungen zusätzliche Beschränkungen sowohl durch Unionsrecht als auch durch mitgliedstaatliches Gesetzesrecht in bestimmten Feldern und zu Gunsten bestimmter Ziele zu.[210]

46 Im Anschluss an die Betroffenenrechte folgen in Art. 24 bis 43 DSGVO besondere Bestimmungen zur **Verantwortlichkeit** und damit einhergehenden spezifischen **Verantwortlichkeitspflichten.** Hier finden sich nicht nur Regelungen zur Auftragsdatenverarbeitung, sondern auch Pflichten im Hinblick auf den Datenschutz durch System- und Technikgestaltung **(„Privacy by Design")** und durch datenschutzfreundliche Voreinstellungen **(„Privacy by Default"),** das Verzeichnis der Verarbeitungstätigkeiten, die Gewährleistung der **Datensicherheit,** eine **Datenschutz-Folgeabschätzung** und behördliche oder betriebliche **Datenschutzbeauftragte.** Die Umsetzbarkeit dieses vielschichtigen und mannigfaltigen Bündels an Pflichten soll durch konkretisierte **Verhaltensregeln** und durch **datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen** erleichtert werden.

47 Nicht zuletzt im Anschluss an die einschlägige Rechtsprechung des EuGH[211] hat die DSGVO in den Art. 44ff. DSGVO die Vorgaben zur **Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen** erheblich ausgeweitet. Das gilt unter anderem im Hinblick auf die Verfahren zur Feststellung der Angemessenheit des gebotenen Schutzniveaus. Die Bindungen in Fällen der Übermittlung personenbezogener Daten in Drittländer sollen, ähnlich wie das Marktortprinzip, die Geltungskraft unionaler Standards in bestimmtem Umfang erhalten.[212] Im Gesamtzusammenhang der DSGVO ist dies konsequent. Im Ergebnis trägt sie so zur Internationalisierung datenschutzrechtlicher Standards bei.

48 Die unionalen datenschutzrechtlichen Vorgaben müssen nicht allein um- und durchgesetzt, sondern in erheblichem Umfang auch spezifiziert werden. Dabei wird den mitgliedstaatlich einzurichtenden unabhängigen **Aufsichtsbehörden** (Art. 51ff. DSGVO), den neu eingeführten **Zusammenarbeits- und Kohärenzverfahren** (Art. 60ff. und 63ff. DSGVO) und dem **Europäischen Datenschutzausschuss** (Art. 68ff. DSGVO) eine zentrale Rolle zugewiesen. Im Ergebnis wird ein auf den Datenschutz ausgerichteter **Europäischer Informations- und Verwaltungsverbund** hergestellt.[213]

49 Der effektiven Durchsetzung des Datenschutzrechts dienen zudem die ggf. mitgliedstaatlich zu etablierenden **Rechtsbehelfe der betroffenen Person** (Art. 77ff. DSGVO), die sich bei deren Wahrnehmung auch durch Datenschutzorganisationen vertreten lassen darf (Art. 80 DSGVO)[214], **Haftung** und **Schadensersatz** (Art. 82 DSGVO), die in Art. 83 DSGVO geregelten **Geldbußen** und

---

[210] Derartige Einschränkungen finden sich etwa in §§ 32–37 BDSG.

[211] *EuGH,* Urt. v. 6.10.2015 – C-362/14, Schrems I; Urt. v. 16.7.2020 – C-311/18, Schrems II, beide abrufbar unter http://curia.europa.eu.

[212] *Veit,* Einheit (Fn. 15), S. 469ff. Zu den Auswirkungen s. auch *Marc Rotenberg, Schrems II,* from Snowden to China: Toward a new alignment on transatlantic data protection, ELJ 26 (2020), S. 141ff.

[213] *Alexander Dix,* in: Kühling/Buchner (Fn. 107), Art. 61 Rn. 4.

[214] Vgl. hierzu auch den Vorlagebeschluss des *BGH* v. 28.5.2020, I ZR 186/17.

die den Mitgliedstaaten in Art. 84 DSGVO eingeräumte Kompetenz, **strafrechtliche Sanktionen**[215] festzulegen. Art. 83 DSGVO formuliert allgemeine Bedingungen für die Verhängung von Geldbußen, die nach Tatbeständen und Rechtsfolgen gegenüber der früheren Rechtslage ganz erheblich erweitert worden sind. Er eröffnet allerdings den Mitgliedstaaten die Möglichkeit, selbst Vorschriften dafür festzulegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen Geldbußen verhängt werden können. Diese Möglichkeit hat § 43 Abs. 3 BDSG in weitem, unionsrechtskonform zu reduzierendem Umfang genutzt.[216]

bb) Insbesondere: Grundsätze

In den **Grundsätzen des Art. 5 DSGVO** – Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht – werden in abstrakt-übergreifender Weise Strukturprinzipien aufgelistet. Man kann mehr oder weniger weitreichende Zweifel daran haben, ob diese Regelungstechnik sinnvoll ist, inwiefern die systematischen Zuordnungen, etwa zu den Grundsätzen statt zur Regelung der Rechtmäßigkeit der Verarbeitung in § 6 DSGVO, überzeugend sind und inwieweit die Ausgestaltung der jeweiligen Grundsätze gelungen ist. Die Grundsätze können im Rahmen aller datenschutzrechtlichen Bausteine Relevanz gewinnen. Je nach Bezugspunkt und je nach Inhalt des jeweiligen Grundsatzes sind sie entweder eindeutig oder graduell-komparativ zu erfüllen. In bestimmten Zusammenhängen der Datenverarbeitung stößt ihre Umsetzung auf prinzipielle Schwierigkeiten. Das betrifft etwa Einsatzfelder von Big Data oder der allgegenwärtigen Datenverarbeitung im Zusammenhang mit dem Internet der Dinge.[217] Die Verwaltung unterliegt allerdings rechtsstaatlichen Anforderungen, unter anderem hinsichtlich der Regelung sachlicher Kompetenzen, aufgrund derer Verarbeitungs- und Verwendungskontexte in sachbereichsabhängiger Weise vorstrukturiert sind, selbst wenn sich dies dann je nach Aufgabenfeld und Organisationsmustern differenziert darstellt.[218] Nicht nur, aber eben auch mit Blick auf die jeweiligen (typisierten) Verarbeitungskontexte werden die Grundsätze durch weitere allgemeine und sektorale Vorschriften der EU oder der Mitgliedstaaten, durch Rechtsprechung und durch sich herausbildende Dogmatiken konkretisiert und operationalisiert. 50

Der Grundsatz der **Rechtmäßigkeit** stellt eher programmatisch klar, dass die Verarbeitung personenbezogener Daten rechtlichen Anforderungen unterliegt; er bezieht sich insofern auf sämtliche Datenschutzregelungen.[219] Der Grundsatz einer Verarbeitung nach Treu und Glauben zielt über die Vorgaben rechtlicher Regelungen hinaus auf die **„Fairness"**[220] der Datenverarbeitung unter Berück- 51

[215] Dazu dann § 42 BDSG.

[216] Kritisch *Franziska Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 5), Art. 83 Rn. 55; zur Auslegung s. *Matthias Bergt*, in: Kühling/Buchner (Fn. 107), § 43 BDSG, Rn. 3 ff.

[217] S. bspw. die Ausführungen bei *Alexander Roßnagel*, Notwendige Schritte zu einem modernen Datenschutzrecht, in: ders./Michael Friedewald/Marit Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes, Zwischen Systemgestaltung und Selbstregulierung, 2018, S. 361 (367 ff.).

[218] → Rn. 60.

[219] *Alexander Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 5), Art. 5 Rn. 33.

[220] Das ist der treffendere Begriff der englischen Fassung.

sichtigung der berechtigten Interessen der Beteiligten in Verarbeitungssituationen. Dass personenbezogene Daten „in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden" müssen **(Transparenz)**, spiegelt sich unter anderem in den verschiedenen Informationsrechten der Betroffenen, aber auch in Pflichten der Verantwortlichen wie den Erläuterungs-, Dokumentations- oder Systemgestaltungspflichten oder in den Möglichkeiten der Zertifizierungsverfahren wider. Selbst wenn „die betroffene Person" in der Norm relativ objektiviert zu verstehen ist, greift der gewählte Fokus etwas kurz. Eine prinzipielle, im Einzelnen nach Komplexen und daran beteiligten Akteuren differenziert beurteilbare Nachvollziehbarkeit ist auch übergeordnet, etwa für den Verantwortlichen oder die Aufsichtsbehörden, von zentraler Bedeutung für Datenverarbeitungen, die rechtmäßig und fair verlaufen und eine tragfähige Basis für sachgerechte Entscheidungen darstellen sollen. Das gilt auch und insbesondere angesichts des zunehmenden Einsatzes (teil-)automatisierter, algorithmengesteuerter und ggf. selbstständig „lernender" Verarbeitungsmechanismen, hinsichtlich derer man passende Lösungen finden muss.

52 Der Grundsatz der **Zweckbindung,** den Art. 5 Abs. 1b DSGVO festhält, ist ein mehrere Komponenten bündelnder Begriff. Als ein datenschutzrechtliches Regelungselement meint er den Zweck oder die Zwecke, für die die personenbezogenen Daten im Ergebnis von Verarbeitungen, hier regelmäßig als Informationsgrundlagen, in einem bestimmten Kontext verwendet werden sollen. Als Komponenten zu unterscheiden sind die Zweckbestimmung oder Zweckfestlegung, die (in Art. 5 Abs. 1b DSGVO relativierte) Bindung an den ursprünglich festgelegten Zweck und die Zweckvereinbarkeit als Anforderung für die Weiterverarbeitung.[221] Komplementär tritt der Grundsatz der **Datenminimierung** (Art. 5 Abs. 1c DSGVO) hinzu. Dieses Konglomerat verschiedener Anforderungen umfasst neben der Angemessenheit und objektiven Relevanz personenbezogener Daten insbesondere deren Beschränkung auf das notwendige Maß. Dies ist nicht deckungsgleich mit der aus dem Übermaßverbot bekannten Anforderung des „mildesten Mittels", sondern ein datenschutzrechtliches Regelungselement.[222] Der Grundsatz der Datenminimierung wird in zeitlicher Hinsicht durch den Grundsatz der **Speicherbegrenzung** (Art. 5 Abs. 1e DSGVO) ergänzt. Beide Grundsätze setzen im Kontext des Art. 5 Abs. 1 DSGVO die Zwecke der Verarbeitung als vorgegeben (statt als ihrerseits zu überprüfen) voraus. Im Rahmen der Pflichten hinsichtlich der System- und Technikgestaltung werden sie allerdings ebenfalls in Bezug genommen mit der Folge, dass ihr Verständnis anforderungsreich wird.[223]

53 Der Grundsatz der **Richtigkeit** (Art. 5 Abs. 1d DSGVO) verweist mit der Vorgabe, dass die personenbezogenen Daten „sachlich richtig und erforderlichenfalls auf dem neuesten Stand" sind, ebenfalls auf eine Mehrheit näherer Anforderungen an die inhaltliche Richtigkeit, die Vollständigkeit oder die Aktualität. Diese Anforderungen sind im Hinblick auf die jeweiligen Verarbeitungszwecke zu beurteilen. Für das „richtige" Verständnis der Daten als Informationsgrundlagen, um das es bei der Aufgabenerledigung der Verwaltung geht, können kontextsichernde Begleit- oder Metadaten nötig sein. Ein jüngeres, allerdings

[221] Im Kontext der Phasenregulierung s. auch noch → Rn. 83 ff.
[222] Als Element der Phasenregulierung s. noch → Rn. 87 ff.
[223] S. Art. 25 Abs. 1 DSGVO und noch → Rn. 70 ff.

umfassenderes Stichwort vor dem Hintergrund der Digitalisierung ist das der „Datenqualität".[224] Der Grundsatz der Richtigkeit zeigt, dass Datenschutz und Aufgabenerfüllung keineswegs in jeder Hinsicht gegensätzlich sind. Löschung oder Berichtigung unrichtiger personenbezogener Daten müssen in der öffentlichen Verwaltung insbesondere mit Dokumentationspflichten, wie sie im überkommenen Prinzip der Aktenvollständigkeit und Aktenwahrheit zum Ausdruck kommen, und mit Rechtsschutzerfordernissen abgestimmt werden.

Art. 5 Abs. 1f DSGVO richtet sich mit dem Grundsatz der **Integrität und Vertraulichkeit** darauf, dass personenbezogene Daten nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Die normtextliche Formulierung bezieht sich nicht nur auf Datensicherungsmaßnahmen i.e.S., sondern auch auf den „Schutz vor unbefugter oder unrechtmäßiger Verarbeitung". Der Grundsatz, dessen textliche Fassung geglückter hätte sein können, zielt auf die Einhaltung der Anforderungen anderer Grundsätze und konkreterer Vorgaben mit Hilfe technischer oder organisatorischer Maßnahmen. 54

Der Grundsatz der **Rechenschaftspflicht** in Art. 5 Abs. 2 DSGVO hebt die Rolle des Verantwortlichen hervor, im Bereich der Verwaltung also der Stelle, der eine ausschließliche oder geteilte Entscheidungskompetenz über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zugewiesen ist.[225] Die verantwortliche Stelle ist zum einen für die Einhaltung der Anforderungen des Abs. 1 verantwortlich, damit eben auch insgesamt für die Rechtmäßigkeit der Verarbeitung, und zu dies gewährleistenden Maßnahmen verpflichtet. Zum anderen muss sie dessen Einhaltung nachweisen, also Dokumentations- und Nachweispflichten nachkommen. Die Verantwortlichkeitspflichten spiegeln sich in zahlreichen konkreten Vorschriften wider. 55

cc) Insbesondere: Rechtmäßigkeitsbedingungen

Im Sinne von **Rechtmäßigkeitsbedingungen** regeln Art. 6 ff. DSGVO in einer für allgemeine und „sensible" Daten differenzierten Weise, dass die Verarbeitung nur bei Vorliegen bestimmter Bedingungen rechtmäßig ist. Für die aufgezählten verschiedenartigen Konstellationen beschreiben sie in abschließender Regelung die Grundlagen, auf die sich Verarbeitungen stützen dürfen und müssen.[226] Bei dieser Regelungstechnik handelt es sich **nicht um ein „Verbot mit Erlaubnisvorbehalt"**.[227] Die aufgelisteten Tatbestände sind zwar abschließend, jedoch mehr oder weniger weit, unter Rückgriff auf unbestimmte Rechtsbegriffe und insofern rahmenartig gestaltet. Der Grund ihrer Gestaltung lässt sich als eine Reaktion auf das Problem begreifen, dass Daten, weil diesen Informationsgehalt und Verwendungsmöglichkeiten nicht anhaften[228], nicht von vornherein 56

[224] Dazu auch RfII – Rat für Informationsinfrastrukturen, Herausforderung Datenqualität – Empfehlungen zur Zukunftsfähigkeit von Forschung im digitalen Wandel, 2. Aufl. 2019.

[225] S. die Legaldefinition in Art. 4 Nr. 7 DSGVO und noch → Rn. 99 f.

[226] Vgl. auch *BVerwG*, Urt. v. 27.3.2019, 6 C 2.18, www.bverwg.de/270319U6C2.18.0, Rn. 44 ff.

[227] So aber eine häufig zu findende Bezeichnung, s. etwa *Benedikt Buchner*, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, S. 155 (157 f.). S. demgegenüber *Marion Albers/Raoul-Darius Veit* in: BeckOK (Fn. 181), DSGVO, Art. 6 Rn. 11; vgl. auch *Alexander Roßnagel*, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019, 1 (3).

[228] Oben → Rn. 5 und 6.

aus dem Schutz herausfallen dürfen. Soweit sie sich mitgliedstaatlichem Recht öffnen, tritt dieses hinzu.

57 Bei der **Informations- und Datenverarbeitung öffentlicher Stellen** hat die Einwilligung als Rechtsgrundlage (Art. 6 Abs. 1a DSGVO), die für die Datenverarbeitung Privater eine sehr große Rolle spielt und insbesondere mit Blick darauf rechtlich näher ausgestaltet wird[229], nur ergänzende Bedeutung. Zwar nicht ausschließlich, aber vor allem relevant sind **Art. 6 Abs. 1c DSGVO** und primär **Art. 6 Abs. 1e DSGVO**[230], dies i.V.m. **Art. 6 Abs. 2 und 3 DSGVO.** Art. 6 Abs. 1c DSGVO betrifft gesetzliche Pflichten, die sich unmittelbar auf Datenverarbeitungen beziehen.[231] Art. 6 Abs. 1e DSGVO knüpft die Rechtmäßigkeit der Verarbeitung daran, dass diese für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt[232] oder – dies deckt jedenfalls die hoheitlichen Kompetenzen ab – in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Art. 6 Abs. 2 DSGVO lässt es insoweit zu, dass die Mitgliedstaaten spezifischere Bestimmungen beibehalten oder einführen; Art. 6 Abs. 3 DSGVO enthält nähere Maßgaben für die Rechtsgrundlage, die durch Unionsrecht oder mitgliedstaatliches Recht festgelegt wird.[233] Demnach ergibt sich eine tragfähige Rechtsgrundlage immer erst aus der **Kombination der unionalen und mitgliedstaatlicher Vorschriften.**[234]

58 Für besondere Kategorien personenbezogener Daten **(„sensible Daten")** – Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person[235] – gelten strengere Rechtmäßigkeitsanforderungen. Schon mit Blick auf Datenbegriff und Informationsverständnis[236] ist wenig überraschend, dass die Antwort auf die Frage, ob und inwieweit man mit solchen Daten tun hat, insbesondere wann die

---

[229] S. etwa die Erfordernisse in Art. 7 DSGVO. S. auch *EuGH*, Urt. v. 1.10.2019, C-673/17 – Planet49 GmbH, Rn. 44ff., abrufbar unter http://curia.europa.eu; BGH, Urt. v. 28.5.2020 – I ZR 7/16 – Cookie-Einwilligung II, abrufbar unter www.bundesgerichtshof.de. Ausf. zur Einwilligung im Privatrecht etwa *Bunnenberg*, Datenschutzrecht (Fn. 36), S. 32ff.; *Michael Funke*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht, 2017.

[230] Art. 6 Abs. 1d DSGVO – Erforderlichkeit der Verarbeitung, um lebenswichtige Interessen der betroffenen Person oder einer anderen Person zu schützen – ist gegenüber anderen Rechtsgrundlagen subsidiär; nach EG 46 S. 2 sollten personenbezogene Daten nur dann auf seiner Basis verarbeitet werden, „wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann".

[231] Vgl. auch *Philipp Reimer*, Verwaltungsdatenschutzrecht, DöV 2018, S. 881 (887).

[232] Dies bestimmt nicht der Verantwortliche selbst; die Aufgabe muss ihm vielmehr als eine im öffentlichen Interesse liegende Aufgabe übertragen worden sein; so zutr. *Alexander Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 5), Art. 6 Rn. 70.

[233] Zur Abgrenzung und Kombination *Albers/Veit*, in: BeckOK (Fn. 181), Art. 6 Rn. 73ff.: Beide Öffnungsklauseln enthalten bestimmte Vorgaben bei zugleich weiten Gestaltungsspielräumen für die Mitgliedstaaten.

[234] *Albers/Veit*, in: BeckOK (Fn. 181), Art. 6 Rn. 73ff. Es greift jedoch zu kurz und wäre missverständlich, Art. 6 Abs. 1c und e DSGVO nur als „Scharniernormen" zu bezeichnen, so aber *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 5), Art. 6 Rn. 52, 71, 79.

[235] S. auch die Legaldefinitionen in Art. 4 Ziff. 13–15 DSGVO. Ansonsten näher *Albers/Veit*, in: BeckOK (Fn. 181), DSGVO Art. 9 Rn. 27ff.

[236] Oben → Rn. 5ff.

aufgezählten Gehalte aus Daten „hervorgehen", erhebliche Ab- und Eingrenzungsschwierigkeiten bereiten kann.[237] Das führt zu Differenzen bereits über den Anwendungsbereich der Norm und des strengeren Regimes für „sensible" Daten.[238] Jedenfalls partiell erfordern die Antworten einen Blick auf die hinter dem strengeren Regime stehenden Schutzgüter, -ziele und -gründe, die vielfältig sind.[239] Die Verarbeitung „sensibler" Daten wird in Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Davon nimmt Art. 9 Abs. 2 DSGVO – der die allgemeinen Rechtmäßigkeitsvoraussetzungen des Art. 6 Abs. 1 DSGVO nicht vollständig verdrängt, sondern überlagert – katalogartig aufgezählte, in den Voraussetzungen teilweise generalklauselartig gefasste Fallkonstellationen aus.[240] Für die öffentliche Verwaltung sind die meisten dieser Konstellationen relevant. Neben denjenigen, die etwa das Recht der sozialen Sicherheit oder die Gesundheitsversorgung ansprechen, spielt Art. 9 Abs. 2g DSGVO eine besondere Rolle: Diese Öffnungsklausel lässt eine Verarbeitung zu, wenn sie auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. In den Bereichen der Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten erlaubt Art. 9 Abs. 4 DSGVO den Mitgliedstaaten zudem zusätzliche Bedingungen, einschließlich Beschränkungen. Hier wie an vielen anderen Stellen stehen hinter den Öffnungen für mitgliedstaatliche Regelungen nicht allein politische Kompromisse, sondern auch gegenstandbedingte Gründe, also solche, die unter anderem aus dem Querschnittscharakter des Rechts des Umgangs mit personenbezogenen Daten und Informationen resultieren, Rücksichtnahmen auf die teilweise sehr diversen Sach- und Regelungsstrukturen in den Mitgliedstaaten und eine Reflektion der Kompetenzverteilung zwischen Union und Mitgliedstaaten.[241]

dd) Öffnungen für mitgliedstaatliche Regulierungen

Es kennzeichnet die Datenschutz-Grundverordnung, dass sie zahlreiche Bestimmungen in Form entweder expliziter **„Öffnungsklauseln"** oder **impliziter Öffnungen** enthält[242], an die sich eine mitgliedstaatliche Regulierung anschließen muss oder kann.[243] Sie sind nach Inhalt und Reichweite unter- 59

[237] Zu Grundsatzproblemen, auch hinsichtlich der Annahme erhöhter Diskriminierungsgefahren bei als „sensibel" eingestuften Daten, statt vieler *Tal Z. Zarsky*, Incompatible: The GDPR in the Age of Big Data, 47 Seton Hall LawReview (2016–2017), S. 995 (1012 ff.). S. auch *Albers/Veit*, in: BeckOK (Fn. 181), DSGVO Art. 9, Rn. 18 ff.

[238] Näher m. w. N. *Thomas Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 5), Art. 9 Rn. 12.

[239] *Albers/Veit*, in: BeckOK (Fn. 181), Art. 9 Rn. 23 ff.

[240] Die Streitfrage, ob neben Ausnahmeregelungen im Sinne des Art. 9 Abs. 2 DSGVO auch die Rechtmäßigkeitsvoraussetzungen des Art. 6 Abs. 1 DSGVO vorliegen müssen, hat das BAG mit Beschl. v. 26.8.2021 – 8 AZR 253/20 (A) – dem EuGH zur Entscheidung vorgelegt. Zu den Maßgaben und zur Abwägung im Falle des Begehrens einer Auslistung von Suchmaschinenlinks zu sensiblen Daten *EuGH*, Urt. v. 24.9.2019, C-136/17, Rn. 49 ff.

[241] Ausführliche Ausarbeitung dieser Sicht bei *Veit*, Einheit (Fn. 107).

[242] Die Terminologie ist heterogen und dahinter steht nicht selten ein bestimmtes Grundverständnis, näher dazu *Veit*, Einheit (Fn. 107), Teil 3 B. I.

[243] Ausf. hierzu *Veit*, Einheit (Fn. 107), Teil 3 B., hier auch mit näheren Ausführungen dazu, dass „Öffnungsklauseln" keine spezifische dogmatische Figur der DSGVO sind und dass man ex-

schiedlich gestaltet und lassen sich mit Hilfe verschiedener Ansätze und Kriterien **typologisieren,** etwa nach ihrer Art oder den jeweiligen Modi, hier zum Beispiel in Gestalt einer Konkretisierung, einer Anpassung, einer Ergänzung oder einer Abweichung im Sinne einer Einschränkung oder Schutzniveauverstärkung.[244] Zu aufschlussreicheren Ergebnissen und zu Analysemöglichkeiten auch hinsichtlich impliziter Öffnungen gelangt man, wenn man solche Typologisierungen um **funktionale Systematisierungen** ergänzt.[245] Diese können sich gegebenenfalls überlappen. Zahlreiche Öffnungsklauseln und implizite Öffnungen sind Bedingungen der Möglichkeit einer Abstimmung der weit und tief reichenden querschnittsartigen datenschutzrechtlichen Vorgaben mit der tatsächlichen und rechtlichen Lage in den Mitgliedstaaten. Das steht unter anderem hinter den im öffentlichen Sektor maßgeblichen Art. 6 Abs. 2 und Art. 6 Abs. 3 DSGVO und hinter einigen Ausnahmeklauseln des Art. 9 Abs. 2 DSGVO. Andere Öffnungen reflektieren die verfahrens- und organisationsrechtlichen Eigenheiten oder Gestaltungskompetenzen der Mitgliedstaaten. Nicht zuletzt kommt Öffnungen die Funktion zu, eine Abstimmung mit gegenläufigen Belangen oder eine Konkretisierung von Feldern zu ermöglichen, die im Kompetenzbereich der Mitgliedstaaten liegen. Dies betrifft wiederum Art. 6 Abs. 2 und 3 oder bestimmte Klauseln des Art. 9 Abs. 2 DSGVO. Besonders relevant sind hier aber auch die Beschränkungsmöglichkeiten des Art. 23 Abs. 1 DSGVO oder die Regelungsaufträge oder -optionen in Art. 85 ff. DSGVO hinsichtlich des Medienbereichs[246], des Zugangs der Öffentlichkeit zu amtlichen Dokumenten, der Verarbeitung einer nationalen Kennziffer, des Beschäftigtendatenschutzes oder des Wissenschaftsbereichs.

II. Einsatzfelder und Systembildung

1. Datenschutzrecht in der Differenz von Öffentlichem und privatem Recht

60 Es zählt zu den Charakteristika des Datenschutzrechts, dass es in seinem Grundkonzept **den öffentlichen und den privaten Bereich** gleichermaßen erfasst. Die DSGVO und auch das BDSG adressieren dementsprechend im Aus-

plizite Öffnungsklauseln und implizite Öffnungen differenzieren muss. Umfassend vor dem Hintergrund der Handlungsformenlehre auch *Marian Müller,* Die Öffnungsklauseln der Datenschutzgrundverordnung, 2018.

[244] Dazu *Jürgen Kühling/Mario Martini,* Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 9 ff.; *Müller,* Öffnungsklauseln (Fn. 243), S. 175 ff.; *Alexander Benecke/Julian Wagner,* Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG – Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl. 2016, S. 600 (600 ff.).

[245] Diese Überlegung und die oben im Folgenden genannten Systematisierungen finden sich bei *Veit,* Einheit (Fn. 107), Teil 3 B.

[246] Die Reichweite der Öffnungen des Art. 85 Abs. 1 und des Art. 85 Abs. 2 DSGVO ist umstritten, vgl. als Position zu Gunsten einer weitreichenden unionsrechtlichen Determination etwa *Jan Philipp Albrecht/Nils J. Janson,* Datenschutz und Meinungsfreiheit nach der Datenschutzgrundverordnung, CR 2016, S. 500 (502 ff.). Unabhängig davon, inwieweit hier unionale Vorgaben „durchgeführt" werden, kann es hier im Einzelnen erhebliche Abgrenzungsschwierigkeiten geben, sei es, weil Datenschutz und zivilrechtlicher Persönlichkeitsschutz unzureichend abgestimmt sind, sei es, weil die Anwendbarkeitsreichweite des allgemeinen Datenschutzrechts im Internet und die Abgrenzungen etwa im Medienrecht unklar sind.

gangspunkt öffentliche Stellen und Private gleichermaßen. Die Antwort auf die Frage, inwieweit ein solch übergreifender, viel diskutierter und kritisierter Regelungsansatz im Recht des Umgangs mit personenbezogenen Informationen und Daten sachgerecht ist, muss differenziert ausfallen. In den Rechtsordnungen der Mitgliedstaaten der EU sind die strukturierende Bedeutung und die Grenzlinien der Dichotomie von öffentlichem und privatem Recht unterschiedlich ausgeprägt. Diese ist allerdings nach wie vor mehr oder weniger bedeutsam, selbst wenn man sich die Vielfalt der Aufgaben und der Regelungsfelder[247], zunehmende Verflechtungen zwischen öffentlich-rechtlichen und privatrechtlichen Ordnungen und Verbund-Perspektiven[248], „private-public assemblages" im Überwachungs- und Sicherheitsbereich[249], Hybride im Bereich der Wissensgenerierung[250], Government-to-Business-Datennutzungen und projektbezogene Vernetzungen zwischen Verwaltung und gesellschaftlichen Akteuren[251] vergegenwärtigt. Die Schutzerfordernisse betroffener Personen werden zunächst durch die Eigenheiten der Informations- und Datenverarbeitungen und derer Folgen, weniger durch spezifisch hoheitliche Befugnisse und Instrumente bestimmt. Dennoch können sie sich im öffentlichen Bereich und im privaten Bereich manchmal schon im Ansatz und häufiger zumindest im Ergebnis des gesetzlichen Ausgleichs unterschiedlich gestalten. Ein übergreifender Regelungsansatz passt daher in bestimmtem, aber auch nur in begrenztem Umfang. Auf jeden Fall müssen **inhaltlich** der durch die Vielfalt der Schutzerfordernisse und der Regelungsfelder bedingte **Differenzierungsbedarf** und **dogmatisch** der **Koordinationsbedarf** mit den anderweitigen Normstrukturen des jeweiligen Sachgebiets unter Berücksichtigung von Verflechtungen in Rechnung gestellt werden.

Trotz des übergreifenden Ausgangspunktes sind in der **DSGVO** auch **zahlreiche Differenzierungen angelegt,** wie sie notwendig sind. Das zeigen insbesondere die differenzierten Rechtmäßigkeitstatbestände und die Öffnungen in Art. 6 DSGVO, die differenzierten Ausnahmeregelungen in Art. 9 Abs. 2 DSGVO oder explizite Ausnahmen für staatliche Behörden zum Beispiel im Hinblick auf die Datenschutzfolgenabschätzung oder die Verhaltensregeln[252]. Die in unterschiedlicher Weise sektorspezifische Gestaltung bereits der Vorschriften der DSGVO und die zudem den Mitgliedstaaten ermöglichte sektorspezifische Regulierung ist im Ergebnis beachtlich.[253] **61**

Im **deutschen Datenschutzrecht,** in dem die Differenz von öffentlichem und privatem Recht grundsätzlich nach wie vor prägend für die gesamte Rechtsord- **62**

[247] Die Muster staatlicher Aufgabenwahrnehmung reichen von traditionell hoheitlich geprägten Aufgaben, wie denen der Polizei, über die vielschichtigen Tätigkeiten der Umweltbehörden bis hin zu den persönlichkeitsnahen beratungsintensiven Aufgaben der Jugendhilfe oder der Drogenberatung. Der private Bereich schließt unterschiedlichste vertragliche und deliktsrechtliche Verhältnisse, die ehemals hoheitlichen Leistungen und Dienste in Telekommunikationsnetzen oder in der Arbeitsvermittlung, Rechtsbeziehungen mit monopol- oder oligopolartigen Intermediären oder auf Informationssammlungen und -auswertungen spezialisierte Dienstleistungen ein.

[248] → Bd. I *Burgi* § 18 Rn. 31 ff.; s. außerdem die Beiträge in *Hoffmann-Riem/Schmidt-Aßmann,* Auffangordnungen.

[249] *Albers,* Surveillance (Fn. 17), S. 75, 81, 105 ff.

[250] *Reiling,* Hybride (Fn. 53).

[251] → Bd. I *Britz/Eifert* § 26 Rn. 16 ff.

[252] Art. 35 Abs. 10, 41 Abs. 6 DSGVO.

[253] So *Veit,* Einheit (Fn. 107), Teil 3 B III 3d mit näheren Erläuterungen.

nung ist, weil das Grundgesetz den Staat anders konstituiert als es den privaten Bereich regelt[254], finden sich **noch deutlich ausgeprägtere Differenzierungen.** Das gilt bereits für das BDSG, aber auch mit Blick auf die im föderalen System relevanten Landesdatenschutzgesetze und auf die bereichsspezifischen Regelungskomplexe. § 1 BDSG adressiert zwar sowohl die öffentlichen Stellen des Bundes[255], dies mit einem gegenüber der DSGVO erweiterten sachlichen Anwendungsbereich[256], als auch nichtöffentliche Stellen[257]. Eine ganze Reihe von Vorschriften sind dann aber auf entweder jene oder diese Stellen zugeschnitten, etwa die Ermächtigung des § 3 BDSG, die Zweckänderungsvorschriften der §§ 23, 24 BDSG oder Ausnahmeklauseln bei der Information Betroffener in §§ 32, 33 BDSG.

2. Allgemeine und bereichsspezifische Regelungskomplexe

63 Das Recht des Umgangs mit personenbezogenen Informationen und Daten gliedert sich in eigenständiger Weise in **allgemeine** und **bereichsspezifische Regelungskomplexe.** Grundsätzlich gilt im Verhältnis zwischen jenen und diesen als Ausgangspunkt, dass die allgemeinen Datenschutzregelungen Standards setzen, die mit Rechtsbegriffen operieren müssen, die in allen Gebieten einsatzfähig und deswegen zwingend teilweise relativ unbestimmt sind.[258] Sie bestehen nicht allein aus einer Kodifikation, sondern auch aus anerkannten Instituten, Figuren, Grundsätzen und Rechtsbegriffen, die in bestimmtem Umfang für bereichsspezifische Regelungen systembildend wirken und sich darin widerspiegeln.[259] Der Sinn dieser Regelungen liegt darin, Regelungsprobleme, die sich bereichsspezifisch stellen, in Abstimmung mit den sachlichen Regelungsstrukturen sachgerecht, mit einem höheren Grad an Bestimmtheit oder auch durch auf das Regelungsfeld zugeschnittenen Mustern zu lösen. Allerdings wird die Dichotomie allgemeiner und bereichsspezifischer Regelungskomplexe aus mehreren Gründen relativiert.

64 Das gilt zum einen wegen des **komplexen Verhältnisses zwischen unionalem und mitgliedstaatlichem Recht.** Die Datenschutz-Grundverordnung formuliert allgemeine Vorgaben, die in bestimmtem Umfang auch das bereichsspezifische mitgliedstaatliche Recht beeinflussen bzw. dadurch umgesetzt werden, sofern

---

[254] Vgl. *Schmidt-Aßmann*, Ordnungsidee, 1. Kap. Rn. 26.

[255] Dazu § 2 Abs. 1 BDSG. Öffentliche Stellen der Länder sind mit der Auffangregelung des § 1 Abs. 1 Nr. 2 BDSG zwar ebenfalls zunächst eingeschlossen, unterliegen aber im Ergebnis, von Ausnahmen bei Einzelregelungen abgesehen, den in sämtlichen Ländern vorhandenen Landesdatenschutzgesetzen.

[256] → Rn. 37.

[257] Zu den nichtöffentlichen Stellen gehören natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, sofern sie nicht unter § 2 Abs. 1 bis 3 BDSG fallen und nicht, etwa als Beliehene, hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, s. § 2 Abs. 4 BDSG. Bereichsspezifische Vorschriften gehen vor, soweit sie den jeweiligen Sachverhalt abschließend und erschöpfend regeln.

[258] Bestes Beispiel ist die Zulässigkeit der Verarbeitung personenbezogener Daten, wenn dies „zur Erfüllung der Aufgaben" der verantwortlichen Stelle „erforderlich" ist, § 3 BDSG i.V.m. Art. 6 Abs. 1e DSGVO.

[259] Mit Blick auf das deutsche Allgemeine und Besondere Verwaltungsrecht allgemein dazu *Eberhard Schmidt-Aßmann*, Zur Funktion des Allgemeinen Verwaltungsrechts, DV, Bd. 27 (1994), S. 137 (137 ff); *Thomas Groß*, Die Beziehungen zwischen dem Allgemeinen und dem Besonderen Verwaltungsrecht, DV, Beiheft 2, 1999, S. 57 (57 ff., bes. 70 ff.). Trotz der inzwischen ausgeprägten Europäisierung des Datenschutzrechts sind diese Überlegungen in bestimmtem Umfang übertragbar.

sie nicht durch sektorale unionale Vorgaben verdrängt werden. Das sektorale europäische Datenschutzrecht hat sich allerdings in vielfältigen, partiell eigenständigen Linien entwickelt, in denen sich Regelungsmuster und Praktiken der Verarbeitung oder des Austauschs von Daten im Kontext der Sach-, Organisations- oder Kooperationsstrukturen im jeweiligen Handlungsfeld widerspiegeln.[260] Auch wenn das ehemals ausgeprägt heterogene Bild im Gesamtpaket der EU-Rechtsakte besser abgestimmt werden soll[261], bleibt das sektorale Datenschutzrecht wegen der engeren Bezüge zu den sektorspezifischen sachlichen Vorschriften vielfältig. In dieser Form beeinflusst es das bereichsspezifische mitgliedstaatliche Datenschutzrecht, soweit dieses daran angepasst sein muss.

Zum anderen muss das allgemeine Datenschutzrecht, soweit es die Verwaltung betrifft, wegen der Verflechtungen mit der Ebene sachlicher Aufgaben und Befugnisse, der Verwaltungsverfahren und der Verwaltungsorganisation[262] mit dem **Verwaltungsrecht** koordiniert werden. Dabei muss es zunächst mit den Kategorien des Allgemeinen Verwaltungsrechts abgestimmt werden und sie ergänzen. Zugleich dient es im Verhältnis zum Besonderen Verwaltungsrecht als Allgemeiner Teil in informationeller Hinsicht. Darüber hinaus sollte es, soweit möglich, gegenüber dem bereichsspezifischen Datenschutzrecht Transformations-, Bündelungs-, Entlastungs-, Harmonisierungs- und sonstige Systembildungsfunktionen erfüllen. Im bereichsspezifischen Datenschutzrecht wiederum besteht ein besonderer Koordinationsbedarf mit den sachlichen Strukturen. Die Schwierigkeiten macht das – nicht in jeder Hinsicht geglückte – Bemühen anschaulich, die Datenschutzrichtlinie für Polizei und Strafjustiz in Teil 1 und Teil 3 des BDSG umzusetzen; dies wird ergänzt durch die bereichsspezifischen Regelungen des Sicherheitsrechts.[263] 65

Eigenheiten und Abstimmungserfordernisse hinsichtlich des bereichsspezifischen Datenschutzrechts werden mit Blick auf einige besonders markante **Referenzgebiete** deutlich.[264] Das **Telekommunikations- und Telemediendatenschutzrecht** reagiert auf das Internet und beeinflusst den Baustein der System- oder der Technikgestaltung ebenso wie differenzierte Formen der Verantwortlichkeit[265] oder die Fortentwicklung der Rechte betroffener Personen. Anschaulich ist der Anspruch auf eine anonyme oder unter Pseudonym erfolgende Nut- 66

[260] *Albers*, Umgang (Fn. 163), Rn. 40 f. m.N.

[261] Oben → Rn. 3.

[262] → Rn. 1, 8 ff., 14.

[263] Zu §§ 48 und 49 BDSG *Albers/Schimke*, in: BeckOK (Fn. 181), BDSG; zu den bereichsspezifischen Bestimmungen ausf. *Albers*, Datenschutzbestimmungen, in: BeckOK (Fn. 181), Syst. L.

[264] Grundsätzlich sind Referenzgebiete diejenigen besonderen Gebiete, die fachübergreifende Problemlagen und -lösungen aufweisen und in deren Fallmaterial sich die allgemeinen Aussagen wiederfinden oder auch neu herauskristallisieren. Zum Verständnis des Begriffs der Referenzgebiete *Schmidt-Aßmann*, Funktion (Fn. 259), S. 148 ff.; → Bd. I *Voßkuhle* § 1 Rn. 43 ff., *Möllers* § 2 Rn. 56, *Burgi* § 18 Rn. 115 ff. Gerade im Datenschutzrecht sind Referenzgebiete relativ zu bestimmen und Zwischenschichten herauszuarbeiten, in denen Regelungen oder Bausteine des Datenschutzrechts bereichsspezifisch ausgeformt werden, ohne dass ihre Entlastungs- und Systembildungsfunktionen dadurch ganz verloren gingen. S. auch *Nikolaus Marsch/Timo Rademacher*, Generalklauseln im Datenschutzrecht, Die Verwaltung 54 (2021), S. 1 (25 f.) dazu, dass allgemeine Datenschutznormen „ein Forum für den institutionellen Austausch aller beteiligten Akteure eines umfassend verstandenen Steuerungsverbundes" bieten und so „*Recht als Prozess*" ermöglichen können.

[265] Vgl. etwa *BGH*, Urt. v. 27.2.2018, VI ZR 489/16, abrufbar unter juris.bundesgerichtshof.de.

zung von Telemedien.[266] Im **Sozialrecht** als einem Recht staatlicher Leistungen und einem Kooperationsrecht zwischen Behörden geht es um passende Vorschriften für den ausgeprägten behördlichen Informations- und Wissensbedarf bei oftmals „sensiblen" Daten.[267] Charakteristisch für das **Polizeirecht** sind zum einen die Vorfeldaufgaben, die gerade mittels Informations- und Datenverarbeitungen und mittels Wissensproduktion erfüllt und durch Datenschutzregelungen erst begrenzt und präzisiert werden. Zum anderen stehen diesen Sicherheitsbehörden eingriffsintensive heimliche Ermittlungsmethoden zu, die Regelungserfordernisse nicht nur für Datenerhebungen, sondern für sämtliche weiteren Verarbeitungsphasen und für die sicherheitsbehördliche Zusammenarbeit auslösen.[268] Darüber hinaus gehört die informationelle Vernetzung in der modernen Sicherheitsarchitektur zu den zentralen Themen.[269] Anschauliche Beispiele sind der Umbau des Bundeskriminalamtes[270] und die gemeinsamen Dateien von Polizei und Nachrichtendiensten, etwa die Anti-Terrordatei.[271] Sachbedingt werden nicht zuletzt die Inhalte und vor allem die Grenzen der Informationsrechte betroffener Personen besonders, wenn auch teilweise wiederum in einer Mischung abstrahierter und spezifischer Bestimmungen, geregelt.[272] Gerade das Sicherheitsrecht zeigt auf, dass sich datenschutzrechtliche Vorgaben selten isoliert erschließen, sondern ein **Denken in Verarbeitungs- und Regelungskontexten** erfordern.

3. Datenschutzrecht im Verwaltungsrecht

67 Das Datenschutzrecht ist, soweit es die Verwaltung betrifft, mehr oder weniger eng mit den Vorschriften zu den sachlichen Kompetenzen der jeweiligen Behörden, zum Verwaltungsverfahren oder zur Verwaltungsorganisation verbunden. Unter anderem bieten die **rechtlich verankerten sachlichen Aufgaben und Befugnisse** regelmäßig in bestimmten Hinsichten ein Gerüst für das Verständnis und die Ausgestaltung der Datenschutzregelungen. Anschaulich ist dies beispielsweise, wenn die Rechtmäßigkeit von Datenverarbeitungen daran geknüpft wird, dass diese „zur Erfüllung der Aufgabe erforderlich" sind. Das Datenschutzrecht und das sachbezogene Verwaltungsrecht müssen also auf Gesetzes- und auf Anwendungsebene aufeinander bezogen und miteinander abgestimmt werden. Enge Wechselbeziehungen und Abstimmungserfordernisse bestehen außerdem zwischen dem Datenschutz- und dem **Verwaltungsverfahrensrecht.** Da Verwaltungsverfahren immer auch Informations- und Datenverarbeitungen sind[273], regelt dieses Recht – unter der Perspektive einer sach-

[266] S. §§ 9, 13, 19 TTDSG.

[267] Zur Verletzung des Sozialgeheimnisses durch Offenbarung des Bezugs von ALG II *BSG*, ZD 2012, S. 573 (573 ff.).

[268] Dazu näher *Marion Albers*, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, 2001, bes. S. 97 ff.; *Matthias Bäcker*, Kriminalpräventionsrecht, 2015, bes. S. 410 ff., 473 ff.

[269] Näher *Marion Albers*, Sicherheitsbehördliche Netzwerke und Datenschutz, in: Seckelmann (Fn. 65), S. 509 ff.

[270] S. etwa zum neu gestalteten Verbundsystem §§ 29 ff. BKAG.

[271] Dazu §§ 1 ff. ATDG.

[272] S. übergreifend *Albers*, Datenschutzbestimmungen, in: BeckOK (Fn. 181), Syst. L Rn. 109 ff.

[273] Für Verwaltungsverfahren i. S. d. § 9 VwVfG s. auch Bd. II 2. Aufl. *Gusy* § 23 Rn. 33: Das auf eine rechtsverbindliche (Abschluss)Entscheidung gerichtete (Verwaltungs)Verfahren liefert den maßgebli-

gerechten Aufgabenwahrnehmung[274] – seinerseits einige Fragen der Beschaffung von Informationen und Daten, etwa mit dem Amtsermittlungsgrundsatz in § 24 VwVfG oder mit der Anhörung in § 28 VwVfG. § 1 Abs. 3 BDSG klärt bestimmte Überschneidungen mittels einer Vorrangklausel zu Gunsten des Datenschutzrechts, das die Regelungen des allgemeinen Verwaltungsverfahrensrechts entsprechend modifiziert. Die engen Bezüge zwischen Datenschutz- und **Verwaltungsorganisationsrecht** werden deutlich, wenn es etwa um Portallösungen und eine einheitliche Identifikationsnummer[275], um rechtmäßige Gestaltungen eines Cloud-Computing oder um eine (relative) informationelle Abschottung unterschiedlicher Behörden gegeneinander[276] geht. Abgestimmt werden muss das Recht des Umgangs mit personenbezogenen Informationen und Daten nicht zuletzt auch mit der behördlichen Öffentlichkeitsarbeit, Medienauskunftsansprüchen, den Informationsfreiheits- oder Transparenzgesetzen sowie mit Open Data-Konzepten und Weiterverwendungsmöglichkeiten von Daten des öffentlichen Sektors, vor allem wenn künftig auch die Weiterverwendung besonders geschützter Daten unter bestimmten Bedingungen möglich werden soll[277].

4. Bausteine des Datenschutzrechts

Das Verständnis des Datenschutzrechts können systembildende **Bausteine** anleiten und erleichtern. Ausgangs- und Ansatzpunkt ist dabei im Wesentlichen ein funktionaler Zugriff mit Blick auf den Umgang mit personenbezogenen Informationen und Daten als Gegenstand, die Schutzgüter und die Bezugspunkte rechtlicher Steuerung. Herausstellen lassen sich, ohne dass dies abschließend und erschöpfend wäre, die **Phasenregulierung,** die **Systemgestaltung,** die **Technikgestaltung,** die Zuweisung einer in bestimmter Weise ausgestalteten **Verantwortlichkeit** und **Verantwortlichkeitspflichten, Selbstregulierungsmechanismen,** die **Informations-, Partizipations- oder Einflussmöglichkeiten Betroffener,** die Einrichtung spezialisierter **Datenschutzinstitutionen** sowie die Gewährleistung von **Rechtsbehelfs-, Haftungs-** und **Sanktionsformen.** 68

Nimmt man eine rechtsetzungsorientierte Perspektive ein, ist die **Ausgestaltung** der einzelnen Bausteine mit dem Vorbehalt, dass die datenschutzrechtlich notwendigen Funktionen in der Gesamtschau sichergestellt werden, **relativ kontingent.** Es ist zudem ohne Weiteres möglich, dass man, wie in der DSGVO realisiert, Bausteine teilweise nach dem „One size fits all"-Ansatz, teilweise nach 69

chen Fokus zur Selektion von Informations- und Datenverarbeitungen (ohne dass dies bedeutet, dass eine Entscheidung nicht auch aus einer übergreifenden Perspektive selbst als Information beschrieben werden könnte oder dass der Umgang mit Informationen und Daten immer im Rahmen eines Verwaltungsverfahrens zu betrachten wäre).

[274] Im Vergleich zum Recht des Umgangs mit personenbezogenen Informationen und Daten hat das Recht des Verwaltungsverfahrens einen ausgeprägteren Sachbezug, während jenes Recht spezifische Erfordernisse individuellen Schutzes realisiert und insofern nicht von vornherein funktional auf die sachlichen Aufgaben bezogen ist, sondern diese Bezüge erst aufgrund der faktischen und rechtlichen Eingliederung der Verarbeitungsvorgänge in den jeweiligen sachlichen Kontext erhält.

[275] → Rn. 44 und 81; außerdem → Bd. I *Britz/Eifert*, § 26 Rn. 62 f.

[276] S. etwa *BVerfG*, Beschl. v. 10.11.2020 – 1 BvR 3214/15 – Antiterrordatei II, www.bverfg.de, Rn. 101 ff.

[277] Vgl. oben → Rn. 3.

dem risikobasierten Ansatz gestaltet. Zwischen den einzelnen Bausteinen bestehen zahlreiche **Wechselwirkungen,** aus denen ein **Koordinationsbedarf** resultiert. Die Gestaltung einer Komponente kann zum einen einen Folgeregelungs- oder Folgeentscheidungsbedarf an anderen Stellen auslösen. Werden beispielsweise an bestimmten Stellen der Verarbeitungsabläufe individuelle Einflussmöglichkeiten garantiert, setzt dies eine damit abgestimmte Gewährleistung der individuellen Kenntnischancen voraus. Zum anderen kann die Gestaltung einer Komponente im Sinne von Substitutions- oder Kompensationswirkungen dazu führen, dass der Regelungs- oder Entscheidungsbedarf an anderen Stellen entfällt, weil sie das dort vorhandene Problem bereits löst. So könnte eine relativ breite und vage Zwecksetzung, die in dieser Form dem Regelungsgebiet oder den Möglichkeiten der Zweckfestlegung zu einem bestimmten Verarbeitungszeitpunkt Rechnung trägt, durch Informations-, Partizipations- und Einflussrechte der Betroffenen im weiteren Verarbeitungsverlauf kompensiert werden.[278] Der Verwendungszweck könnte dann zu Beginn abstrakt-umgreifend benannt, aber unter Beteiligung der betroffenen Personen an angemessenen Stellen im Entscheidungsprozess spezifiziert werden. Durch solche Ausgestaltungsmöglichkeiten gewinnt das Recht des Umgangs mit personenbezogenen Informationen und Daten Flexibilität.

III. Ausgestaltung und Koordination zentraler Bausteine

1. Systemdatenschutz als Kontextgestaltung

a) Funktionen und Anknüpfungspunkte

70 Die **Systemgestaltung** ist ein erster zentraler Baustein des Datenschutzrechts. Auch wenn dieser Baustein mittlerweile etabliert ist, bleibt oft dunkel, was dabei mit dem zu gestaltenden „System" gemeint ist. Oft werden „technische Systeme" der Datenverarbeitung als Bezugspunkt gewählt: „Unter Systemdatenschutz versteht man Datenschutzfunktionalität eingebaut in Systeme und Verfahren"[279]. Ein solcher Bezugspunkt ist jedoch zu reduziert. Der Blick weitet sich über eine Ausarbeitung der **Funktionen,** die eine Systemgestaltung erfüllen soll. Hinter ihr steht die treffende Überlegung, dass die Regulierung allein der Verarbeitungsvorgänge zu kurz greift. Denn indem die Gestaltung der Aufgaben, die Organisation, die Kommunikations- oder Entscheidungsverfahren und die eingesetzten Techniken den Kontext und die Bedingungen der Informations- und Datenverarbeitungen mitkonstituieren, prägen sie zugleich, welche personenbezogenen Daten erforderlich sind, in welcher Form und Menge sie gespeichert werden, wie viele Personen darauf Zugriff haben müssen oder wie transparent Verarbeitungen ablaufen können. Unter Umständen können alternative Aufgaben-, Organisations- oder Verfahrensgestaltungen die Daten oder deren Verarbeitungsumfang deutlicher begrenzen oder mit mehr Trans-

[278] Vgl. auch *Maximilian von Grafenstein*, The Principle of Purpose Limitation in Data Protection Laws, 2018, S. 325 ff., der für bestimmte Felder im Privatsektor die Zweckbestimmung als Risikoentdeckungsverfahren konzipiert und entsprechend prozeduralisiert.

[279] So – mit Bezug auf IT-Systeme – *Marit Köhntopp*, Datenschutz technisch sichern, in: Alexander Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik?, 2001, S. 55 (56).

parenz verbunden sein. Vor diesem Hintergrund klärt sich das Verhältnis zur Technik: Da technische Datenverarbeitungssysteme eine Teilkomponente des übergreifenden Kommunikationssystems sind, umfasst eine Systemgestaltung Aspekte der Technikgestaltung[280], erschöpft sich darin jedoch nicht.[281] Sie bezieht sich auf abgrenzbare soziale Systeme oder Teilsysteme, in deren Rahmen in Kommunikations-, Entscheidungs-, Informations- und Datenverarbeitungsverfahren unter Einsatz von Kommunikations- und Datenverarbeitungstechniken Aufgaben erledigt oder bestimmte Ziele verfolgt werden und in denen sich die Verarbeitungsvorgänge bewegen.[282] Datenschutz durch Systemgestaltung hat die Funktion der **sachlichen, organisatorischen und technischen Ausgestaltung** der in Bezug genommenen **Kommunikationssysteme** auf einer der Regulierung der Verarbeitungsphasen (analytisch) vorgelagerten Ebene.

Versteht man den „Systemdatenschutz" als **Kontextgestaltung,** ist er breit an- 71
gelegt: Er reicht von der Gestaltung der sachlichen Kompetenzen, auf die Verarbeitungsvorgänge ausgerichtet werden, über die Verwaltungsorganisation und die Entscheidungsverfahren, die dann beispielsweise die getrennte Verarbeitung von Daten mit unterschiedlicher Zweckbindung oder Zugangsbeschränkungen gewährleisten, bis hin zu konkreten Maßnahmen, die etwa Authentizität, Revisionsfähigkeit und Transparenz sicherstellen. Abstrakt betrachtet gibt es kaum Faktoren, die nicht unter dem Aspekt der „Systemgestaltung" variiert werden könnten. Schon deswegen, aber auch aus weiteren Gründen ist die Systemgestaltung mehr oder weniger **anforderungsreich.** Denn sie setzt in unter Umständen außerordentlich komplexen Zusammenhängen nicht nur eine Analyse voraus, welche Informationen und welche Daten benötigt werden, sondern erfordert zudem alternative Entwürfe der Gestaltung des übergeordneten Systems und einen Vergleich der mit ihnen jeweils verbundenen Verarbeitung personenbezogener Daten. Deswegen lassen sich zwar **Anknüpfungspunkte, Verfahren oder Instrumentarien** in bestimmtem Umfang **allgemein-abstrakt** beschreiben. Die konkreten Gestaltungserfordernisse und -möglichkeiten erschließen sich jedoch erst im jeweiligen Sachbereich. Im Konzept der Systemgestaltung steckt somit das Erfordernis **bereichsspezifischer Realisierung.**

b) Komponenten der Systemgestaltung

Anforderungen an die Systemgestaltung finden sich in einer **Reihe der Be-** 72
stimmungen der DSGVO und sind insofern in deren Vorschriften eingewebt. Zu den Beispielen gehört die allgemeine Verpflichtung des Verantwortlichen

[280] Sie erfasst keineswegs alle Aspekte der Technikentwicklung und -gestaltung, die sich als Baustein ihrerseits relativ eigenständig darstellt, s. noch → Rn. 77 ff.

[281] Vgl. auch die Beschreibung von *Ann Cavoukian*, Privacy by design: the definitive workshop, Identity in the Information Society Vol. 3 (2010), S. 247 ff., https://doi.org/10.1007/s12394-010-0062-y: „*Privacy by Design* prescribes that we build privacy directly into the design and operation, not only of technology, but also of operational systems, work processes, management structures, physical spaces and networked infrastructure. [...] it allows us to consider technology, business processes, management functions and other organizational issues in a comprehensive manner and to embed privacy at every layer."

[282] Insofern lässt sich die datenschutzbezogene Systemgestaltung unter Berücksichtigung der auf beiden Seiten nötigen Perspektivenerweiterungen mit dem Topos des Wissens-, Informations- und Datenmanagements verknüpfen. S. insgesamt zu Verwaltungsinformationsbeziehungen auch → Bd. I *Wischmeyer* § 24 m. w. N.

aus Art. 24 DSGVO, die deren Anforderungen, hier unter anderem aus den Grundsätzen des Art. 5 DSGVO, mit dem Erfordernis der Umsetzung geeigneter technischer und organisatorischer Maßnahmen verknüpft. Ausdrücklich auch auf das Verarbeitungsvorfeld richten sich Artt. 25 DSGVO, 32 oder 35 DSGVO. Es kennzeichnet die Verordnungsvorgaben, dass sie **abstrakt, prozedural** oder **funktional** angelegt sind und die Maßnahmen selbst zwar gelegentlich exemplifizieren, aber nicht im Einzelnen vorschreiben. Immerhin müssen auf ihrer Ebene **Abstimmungserfordernisse** hinsichtlich sowohl mitgliedstaatlicher Kompetenzen als auch bereichsspezifischer Eigenheiten ebenso in Rechnung gestellt werden wie der absehbare **dynamische Wandel** etwa bei Organisationsmustern oder Techniken.

73 Bei näherer Analyse zielen die Vorgaben des Art. 25 Abs. 1 DSGVO nicht lediglich auf eine Technikgestaltung, sondern umfassend auf einen **Datenschutz durch Gestaltung** („data protection by design")[283]. Bereits sein Normtext macht die in der Vorgabe steckende **Komplexität** klar: Er bezieht sich auf die Gewährleistung sämtlicher Datenschutzgrundsätze und auf sämtliche einschlägigen Anforderungen der Verordnung. Er verlangt eine Herausarbeitung der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten betroffener Personen, einschließlich des Gewichts und der Eintrittswahrscheinlichkeit von Beeinträchtigungen. Bereits dafür, aber auch wegen der im Ergebnis nötigen Abwägung sind Verarbeitung und Verarbeitungskontexte selbst in hinreichendem Umfang herauszuarbeiten. Bei der Abwägung spielen darüber hinaus beispielsweise Implementierungskosten eine Rolle. In der Zeitdimension bezieht sich die Vorgabe sowohl auf den Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch auf den Zeitpunkt der eigentlichen Verarbeitung. Die zu treffenden Maßnahmen bleiben, nicht überraschend, abstrakt; exemplarisch wird auf die Möglichkeiten einer Pseudonymisierung hingewiesen. Für bestimmte Konstellationen wird Art. 25 Abs. 2 DSGVO präziser, indem er das Erfordernis datenschutzfreundlicher Voreinstellungen („data protection by default") hervorhebt.[284] Mehr Präzision weist auch Art. 32 DSGVO auf, der über eine enger verstandene **Datensicherheit** hinaus reicht, in seinem Regelungsbereich aber funktionale Konkretisierungen treffen kann. Die in Art. 32 Abs. 1 DSGVO gewählte Begrifflichkeit schließt zum Teil an die Sprache und die Methoden der IT-Sicherheitstechnik an.[285]

74 Die Idee einer **Datenschutzfolgenabschätzung** als Komponente der Systemgestaltung, wie sie Art. 35 DSGVO aufgreift, kann an die inzwischen lange Tradition der Technikfolgenabschätzung anknüpfen. Deren Ausarbeitungen und die auf den Datenschutz fokussierten „Privacy Impact Assessment"-Studien zeigen wiederum die mehr oder weniger ausgeprägte Kom-

---

[283] Ausf. und zutr. dazu *Marit Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 5), Art. 25 Rn. 16 ff.

[284] S. näher *Felix Bieker/Marit Hansen*, Datenschutz „by Design" und „by Default" nach der neuen europäischen Datenschutz-Grundverordnung, RDV 2017, S. 165 (165 ff.); *Ulrich Baumgartner/Tina Gausling*, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, ZD 2017, S. 308 (309 ff.).

[285] Vgl. dazu etwa *Martin Rost/Andreas Pfitzmann*, Datenschutz-Schutzziele – revisited, DuD 2009, S. 353 (353 ff.); weiterführend *Martin Rost/Kirsten Bock*, Privacy by Design und die neuen Schutzziele – Grundsätze, Ziele und Anforderungen, DuD 2011, S. 30 (31 ff.).

plexität auf, die mit solchen Folgenabschätzungen verbunden sind. Aus Art. 35 Abs. 7 DSGVO ergeben sich Mindestvorgaben hinsichtlich der zu berücksichtigenden Aspekte und in bestimmtem Umfang auch Verfahrensstufen und -schritte.[286] Art. 35 Abs. 3 DSGVO präzisiert in einem die Datenschutzfolgenabschätzung insgesamt prägenden risikobasierten Zugriff Regelfälle, in denen eine Folgenabschätzung durchzuführen ist.[287] Soweit es um den öffentlichen Sektor geht, kann eine Folgenabschätzung im Rechtsetzungsverfahren unter der Voraussetzung, dass sowohl die auf die Verarbeitung bezogenen Rechtsnormen als auch die durchgeführte Folgenabschätzung hinreichend konkret sind, die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung ersetzen.[288] Diese bleibt aber möglich und mitgliedstaatlichem Ermessen überlassen.

Die im deutschen Recht ehemals als „Prototyp innovativen Rechts"[289] bezeichneten und als Element der Systemgestaltung eingeordneten **Prinzipien der Datenvermeidung** und der **Datensparsamkeit** finden sich – angesichts der bereits in der unionalen Grundverordnung enthaltenen allgemeinen Vorgaben – nicht mehr in den gemeinsamen Bestimmungen des BDSG, aber noch in **§ 71 BDSG**, der von der Datenschutzrichtlinie für Polizei und Strafjustiz erfasste Sicherheitsbehörden betrifft. Entsprechend § 3a BDSG a.F. gilt danach sowohl für die Verarbeitung personenbezogener Daten als auch für die Gestaltung und Auswahl von Datenverarbeitungssystemen die Zielvorgabe, dass keine personenbezogenen Daten oder so wenig personenbezogene Daten wie möglich verarbeitet werden. Ergänzt wird dies um die Pflicht, zum frühestmöglichen Zeitpunkt von den **Möglichkeiten der Anonymisierung** und **Pseudonymisierung** Gebrauch zu machen, soweit dies nach dem Verarbeitungszweck möglich ist, das mit der Verarbeitung konkret verfolgte Ziel also auch ohne Identifizierung der betroffenen Person erreicht werden kann. Die Vorgaben sind prominent platziert. Die Möglichkeitsvorbehalte verweisen jedoch bereits auf deren Leistungsgrenzen in der Praxis, und zwar erst recht im Sicherheitssektor. Statt solcher Vorgaben, die als spezifiziertes Teilelement brauchbar sein können, als generalisiertes Konzept jedoch nicht überzeugen[290], bedarf es der **Entwicklung treffenderer Systemgestaltungsmaßgaben** in Umsetzung der Richtlinie. 75

Bei einer **bereichsspezifischen Analyse** erschließt sich die Systemgestaltung unter zahlreichen Gesichtspunkten. Im Recht der Nachrichtendienste hat die Integration von Verarbeitungsregelungen dazu geführt, dass die sachlichen **Aufgaben**, auf die der Umgang mit personenbezogenen Informationen und Daten bezogen ist und von denen er mitbestimmt wird, **gesetzlich verankert, präzisiert** oder **differenziert** wurden. Im Rahmen spezifizierter sachlicher Kompetenzen können Verarbeitungszusammenhänge zugeordnet und gegeneinander **abgeschottet** werden, **Anonymisierungs-** oder **Pseudonymisierungsmöglichkeiten** genutzt oder weitere **Organisations-** oder **Verfahrensmaßnahmen** getroffen 76

[286] S. dazu *Michael Friedewald u. a.*, Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz. White Paper, Karlsruhe, 3. Aufl. 2017, S. 18 ff.

[287] Zu den aufgezählten Regelbeispielen gehört, dass eine umfangreiche Verarbeitung von personenbezogenen Daten i.S.d. Art. 9 Abs. 1 oder Art. 10 DSGVO vorliegt oder eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche erfolgt.

[288] Art. 35 Abs. 10 DSGVO. Eine pauschale Einschätzung der Gesetzesfolgen genügt nicht.

[289] *Johann Bizer*, in: Spiros Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 3a Rn. 27.

[290] Ausf. *Albers*, Umgang (Fn. 163), Rn. 107 f., 110 f.

werden. Eine Abschottung dient dem Schutz der betroffenen Personen vor der unerwünschten Zusammenführung von Wissen. Oft dient sie zugleich der Funktionsfähigkeit der Aufgabenerfüllung selbst. Klassisches Beispiel ist die Statistikerarbeitung.[291] Im Transplantationsrecht soll die abschottende Gestaltung der Verarbeitungsbefugnisse der Vermittlungsstelle, der Koordinierungsstelle und des Transplantationszentrums unter anderem sicherstellen, dass die Identität des Spenders dem Transplantationszentrum in der Regel nicht bekannt wird, und zugleich als Missbrauchsvorkehrung die gerechte Organverteilung gewährleisten.[292] Anonymisierungen oder Pseudonymisierungen sind schutzbedarfs- und aufgabengerecht im Rahmen von Teledienstleistungen, bei der Gestaltung von Chipkarten oder elektronischen Patientenakten im Gesundheitsbereich oder für die Sammlung genetischer Proben und Daten in Biobanken.[293]

2. Entwicklung und Gestaltung der Verarbeitungsinfrastrukturen und -techniken

a) Funktionen, Schichten und Instrumentarien

77 Hinter dem Baustein der **Technikgestaltung**, der mit Blick auf (technische) Datenverarbeitungssysteme und entsprechende Infrastrukturen mehr oder weniger eng mit der Systemgestaltung verknüpft ist, stehen mehrere miteinander verknüpfte Überlegungen. Verarbeitungsinfrastrukturen und Verarbeitungstechniken ermöglichen Informations- und Datenverarbeitungen, setzen ihren Formen und Optionen allerdings zugleich naturwissenschaftlich-verarbeitungstechnische Grenzen. Aus rechtlicher Sicht ist das technisch eröffnete Spektrum nur dann einsatzfähig, wenn es mit den normativen Vorgaben vereinbar ist.[294] Umgekehrt kann die Installation verarbeitungstechnischer Grenzen dafür sorgen, dass es den Nutzern von Datenverarbeitungssystemen gar nicht möglich ist, rechtliche Vorgaben zu unterlaufen. Insofern kann Datenschutz weitaus effektiver durch Technik realisiert werden als durch Verhaltenspflichten.[295]

78 Vor diesem Hintergrund lassen sich mehrere Schichten differenzieren. Auf einer ersten Stufe zielt die Steuerung von **Technikentwicklungen** darauf, dass überhaupt Kommunikations- und Datenverarbeitungstechniken zur Verfügung stehen, mit denen sich die normativen Anforderungen an den Umgang mit personenbezogenen Informationen und Daten realisieren lassen. Auf dieser Stufe ist man im Wesentlichen auf indirekte Anreize und Einflussmechanismen, also auf Formen eines „soft law",[296] angewie-

[291] §§ 10 ff. BStatG.

[292] Siehe insbes. §§ 13 ff. TPG; näher *Stephan Rixen*, Datenschutz im Transplantationsgesetz, DuD 1998, S. 75 (77 ff.).

[293] Zum Anspruch auf eine anonyme oder unter Pseudonym erfolgende Nutzung von Telemedien s. § 19 Abs. 2 TTDSG. Zur elektronischen Gesundheitskarte *Gerrit Hornung*, Die digitale Identität, 2005, S. 367; BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R, NZS 2021, 923.

[294] *Heiner Fuhrmann*, Technikgestaltung als Mittel zur rechtlichen Steuerung im Internet, ZfRSoz 2002, S. 115 (117).

[295] Statt vieler *Alexander Roßnagel*, Allianz von Medienrecht und Informationstechnik: Hoffnungen und Herausforderungen, in: ders. (Hrsg.), Allianz (Fn. 279), S. 17 (23 f.).

[296] Dazu *Meinolf Dierkes/Weert Canzler*, Innovationsforschung als Gegenstand der Technikgeneseforschung, in: Wolfgang Hoffmann-Riem/Jens-Peter Schneider (Hrsg.), Rechtswissenschaftliche Innovationsforschung, 1998, S. 63 (76 ff.).

sen.[297] In Betracht kommen die Institutionalisierung von Gremien oder Verfahren zur Entwicklung datenschutzgerechter Techniken, die Unterstützung und Begleitung der Standardbildung, die Stimulation von Leitbild- oder Metapherentwicklungen in den Bereichen der Kommunikationstechniken, staatliche Fördermaßnahmen oder die Vergabe von Gütesiegeln. Auf der zweiten Stufe bewegt sich die Steuerung von **Technikgestaltungen** in einem der Regulierung der Verarbeitungsprozesse **vorgelagerten Vorfeld.** Hier werden Anforderungen an die Auswahl, den Einsatz und die Konfiguration von Datenverarbeitungsnetzwerken, -anlagen, -programmen oder Speichermedien gestellt, die sicherstellen sollen, dass normative Vorgaben technisch bereits verankert oder jedenfalls erfüllbar sind. Die dritte Stufe bezeichnet den überkommenen Komplex der Anforderungen an die **Technikgestaltung,** die die Regulierung der Verarbeitungsphasen begleiten und absichern, dieser also **nachgeschaltet** sind. Dabei werden „technische Anforderungen in die normative Ausformung der Anforderungen an die Verarbeitung personenbezogener Daten integriert".[298]

Sowohl die Steuerung der Technikentwicklung als auch vorgelagerte An- 79
forderungen an Auswahl, Einsatz oder Konfiguration von Techniken setzen eine **Analyse** voraus, **welche Leistungsmerkmale** Anlagen oder Programme überhaupt erfüllen müssen.[299] Das ist nicht leicht auszuarbeiten. Schwierigkeiten kann bereits die angemessene Beschreibung der Schutzerfordernisse und deren Abstimmung mit anderweitig geltenden Anforderungen bereiten. Darüber hinaus besteht das gleiche Problem wie bei der Realisierung eines Datenschutzmanagements: Trotz der unterschiedlichen Kulturen und Denkmuster des Verwaltungspersonals und der Techniker müssen mit Blick auf regelmäßig komplexe Systeme der Verwaltungskommunikation rechtliche, aufbau- und ablauforganisatorische sowie technische Gesichtspunkte in ein stimmiges Gesamtkonzept zusammengeführt werden. Aus Sicht des Rechts ist die Technikentwicklung und -gestaltung zwar grundsätzlich auf (anderweitige) normative Vorgaben bezogen, die auf unterschiedlichen Ebenen und in verschiedenen Hinsichten den Umgang mit personenbezogenen Informationen und Daten steuern. Technische und ökonomische Bedingungen können aber nicht ausgeblendet werden. Soweit Techniken aus ökonomischen Gründen in vielfältigen Anwendungsfeldern einsatzfähig sein müssen, kommt es auf abstrakter Ebene vor allem darauf an, dass sie **Gestaltungsoptionen** bieten, die es ihren Anwendern ermöglichen, technische Anlagen oder Programme so zu **konfigurieren,** dass sie den für sie geltenden Vorgaben für den Umgang mit personenbezogenen Informationen und Daten in einer technisch abgesicherten Weise nachkommen können. Spezifische Anforderungen sind dann im Wege der konkreten Gestaltung technisch umzusetzen. Diese hängt wiederum von den jeweiligen Systemen, Techniken oder Medien

[297] Zu den Problemen, dass die Steuerung zu einem sehr frühen Zeitpunkt in den Entwicklungsprozessen ansetzen muss und dass ihre Adressaten private, international verteilte oder handelnde Akteure sind, *Fuhrmann*, Technikgestaltung (Fn. 294), S. 121.

[298] So *Alexander Roßnagel/Andreas Pfitzmann/Hansjürgen Garstka*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des BMI, 2001, S. 36.

[299] In technischen Diskussionsforen finden sich nähere Überlegungen unter dem Stichwort der „Schutzziele in IT-Systemen", die mit den normativen Vorgaben aber oft nur begrenzt abgestimmt sind, s. *Hannes Federath/Andreas Pfitzmann*, Gliederung und Systematisierung von Schutzzielen in IT-Systemen, DuD 2000, S. 704 (704 ff.).

ab, also davon, ob man mit vernetzten Systemen, mit Chipkarten oder mit Videoüberwachungsanlagen zu tun hat.

b) Rechtliche Standards datenschutzgerechter Gestaltung

80 Für die Technikgestaltung ergeben sich **allgemeine Vorgaben** aus einer Reihe von Bestimmungen der DSGVO, dies entweder übergreifend wie in Art. 24 oder Art. 28 DSGVO, in engem Zusammenhang mit der Systemgestaltung wie in Art. 25 oder 32 DSGVO oder im Zusammenhang mit bestimmten Normen, die wie Art. 6 oder Art. 9 DSGVO etwa „geeignete Garantien" als Rechtmäßigkeitsvoraussetzungen nennen. Wegen der **Abstraktionshöhe** und wegen der **Technikneutralität der DSGVO** sind sie regelmäßig abstrakt gefasst. Gegebenenfalls sind sie, wie die Datensicherheitsregelung des Art. 32 DSGVO, (auch) darauf ausgerichtet, dass bestimmte Funktionen gewährleistet sind. Spezifische technische Risiken werden in der DSGVO damit aber nur begrenzt thematisiert.[300] Die Stufe der Technikentwicklung und darauf bezogene Anreize und Vorgaben werden bestenfalls indirekt über die Förderung der Einführung datenschutzspezifischer Zertifizierungsverfahren oder von Datenschutzsiegeln oder -prüfzeichen[301] erfasst, sofern dies einen Wettbewerb hinsichtlich des Einsatzes und dann auch der Entwicklung datenschutzgerechter Techniken auszulösen vermag. Wenn beispielsweise Art. 25 DSGVO dem Verantwortlichen Pflichten aufgibt, kommt zu kurz, dass das Produkt- oder Diensteangebot der Hersteller Bedingung der Möglichkeit der Umsetzung datenschutzgerechter technischer Maßnahmen ist.[302]

81 Im deutschen Verwaltungsrecht sind **bereichsspezifische Anforderungen** an die Technikgestaltung gelegentlich präziser verankert. Das Registermodernisierungsgesetz, das die Einführung und Verwendung einer übergreifenden Identifikationsnummer regelt, enthält eine Reihe von Anforderungen etwa im Hinblick auf Verschlüsselungen, Authentifizierungen oder Protokollierungen.[303] Im Bereich der gesetzlichen Krankenversicherung stellt § 291a SGB V für die elektronische Gesundheitskarte technische Anforderungen an die Datenverarbeitungs-, Authentifizierungs-, oder Verschlüsselungsmöglichkeiten und erfordert damit eine Telematik-Architektur. Das Passgesetz formuliert datenschutzbedingte Anforderungen an die maschinenlesbare Zone und an die Verschlüsselungs- und Sicherungsverfahren bei biometrischen Merkmalen.[304] Deutlich weiter reichende Vorkehrungen enthalten die Bestimmungen der §§ 5, 10 ff. PAuswG, vor allem weil der Personalausweis angesichts von E-Government und E-Commerce zugleich Funktionen eines elektronischen Identitätsnachweises erfüllen soll. Im Zusammenhang mit dem automatisierten Kontenzugriff durch die Finanzämter werden den in Dienst genommenen privaten Kreditinstituten Maßnahmen zur Sicherstellung des Datenschutzes und der Da-

[300] Grds. Kritik dazu bei *Roßnagel*, Schritte (Fn. 217), S. 374 ff.
[301] Art. 42 DSGVO.
[302] S. die begrenzte Thematisierung der Hersteller in EG 78 S. 4. Kritisch zur unzureichenden Adressierung *Alexander Roßnagel/Christian Geminn*, Datenschutz-Grundverordnung verbessern, 2020, S. 91 ff.
[303] Zum Gesetz s. den N. in Fn. 209.
[304] §§ 4, 16a PassG; näher *Hornung*, Identität (Fn. 293), S. 47 ff., 165 ff., 246 ff., 346 ff.

tensicherheit entsprechend dem jeweiligen Stand der Technik auferlegt.[305] Auch bei weiteren bereichsspezifischen Informations- und Datenverarbeitungen könnten elaborierte Techniken Problemlösungen bieten. So wäre es technisch möglich, die bei einer Videoüberwachung öffentlicher Räume erfassten Gesichter automatisch zu verschleiern und diese Verschleierung nur im Falle eines gefahrenabwehr- oder strafverfolgungsrechtlich relevanten Ereignisses aufzuheben. Das Problem der Streubreite dieser Maßnahme ließe sich dadurch reduzieren, das Übermaßverbot einhalten. Das **Potenzial der Technik** wird in solchen Zusammenhängen in der Praxis **bislang nicht ausgeschöpft.**

3. Regulierung und Gestaltung der Verarbeitungsphasen

Art. 4 Nr. 2 DSGVO stellt den Begriff der „Verarbeitung" in den Mittelpunkt 82
und einzelne Phasen in diesen Rahmen. Die Phasenregulierung ist nicht als rechtliche Nachzeichnung faktischer Abläufe, sondern als **problemorientierte Steuerung von Verarbeitungsphasen** zu begreifen, die einerseits als solche, andererseits im jeweiligen Verarbeitungszusammenhang und -prozess zu betrachten sind. **Phasenübergreifende Elemente** beziehen sich auf alle Phasen und haben insbesondere die unions- und verfassungsrechtlich relevante Funktion, begrenzte und strukturierte Verarbeitungszusammenhänge herzustellen.[306] **Phasenbezogene Elemente** reagieren zusätzlich auf bestimmte Regelungserfordernisse im Zusammenhang mit einem Verarbeitungsschritt.

a) Phasenübergreifende Elemente

aa) Zweckbindung und Flexibilitäten

Die **Zweckbindung** ist ein zentrales **datenschutzrechtliches Regelungsele-** 83
ment. In Gestalt des Art. 5 Abs. 1b DSGVO ist sie ein mehrere Komponenten bündelnder Begriff.[307] Eingeschlossen ist zunächst das – durch Art. 8 Abs. 2 S. 1 GRCh in bestimmtem Umfang vorgegebene – Erfordernis der Festlegung eines eindeutigen[308] und legitimen Zweckes vor oder bei der Datenerhebung oder spätestens bei der Speicherung.[309] Als datenschutzrechtliches Element bezieht sich der Begriff auf den Zweck oder die Zwecke[310], für die die personenbezogenen Daten im Ergebnis einer Verarbeitung, hier regelmäßig als Informationsgrundlagen, in einem bestimmten Kontext verwendet werden sollen. Diese (Verwendungs-)Zwecke sind nicht deckungsgleich mit den sachlichen Verwaltungsaufgaben. Vielmehr hat ihre Festlegung gerade die Funktion, die Verarbeitung personenbezogener Daten, die für sich genommen vielfältig nutzbar wären, mit den sachlichen Kompetenzen, die im Verwaltungsrecht somit als Anknüpfungspunkt und als Gerüst dienen, rechtlich zu verklammern. Diese

[305] § 24c Abs. 6 KWG.

[306] Dazu → Rn. 26, 33.

[307] Im deutschen Recht hat sich der Begriff ursprünglich allein in engerem Sinne auf die Bindung an den vor oder bei Erhebung oder Speicherung festgelegten Verwendungszweck im Verarbeitungsablauf bezogen.

[308] Vgl. *Article 29 Data Protection Working Party*, WP 203 – 00569/13/EN, Opinion 03/2013 on purpose limitation v. 2.4.2013, S. 11 ff.; *Peter Schantz*, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841 (1843 f.): Die geforderte Eindeutigkeit und Erfordernisse des Transparenzgebots führen zu Präzisionsanforderungen.

[309] Die letzte Variante greift nur, falls der Verantwortliche die Daten nicht erhoben hat.

[310] Eine Bündelung mehrerer eindeutiger Zwecke ist prinzipiell möglich.

Verklammerung verknüpft die Informations- und die Sachebene und damit – an einem ersten zentralen Punkt – das Datenschutzrecht mit dem materiellen Verwaltungsrecht. Sie führt zu einer Begrenzung und Strukturierung der Informations- und Datenverarbeitung sowie zur Eingrenzung des jeweils relevanten Wissens- und Handlungskontexts. Mit der Zweckfestlegung entsteht zugleich ein Bezugspunkt oder ein Band, das die einzelnen Verarbeitungsvorgänge zu einheitlichen oder auch zu sich differenzierenden Verarbeitungszusammenhängen verbindet. Verwendungszwecke und Verarbeitungszusammenhänge ermöglichen zudem eine nähere Regulierung einzelner Phasen, wie sie etwa mittels des Tatbestandselements der „Erforderlichkeit" und dessen Anwendung erfolgt. Im Näheren wird es möglich zu präzisieren, welche Informationen für die Entscheidungen im Rahmen der Aufgabenerfüllung benötigt werden, welche Daten als Informationsgrundlage erforderlich und zu erheben sind, wie Daten unter Umständen verändert werden müssen und wie lange man sie braucht. Mit den festgelegten Zwecken erhält der Kontext bestimmte Konturen, in dem sich erst beschreiben lässt, welche Informationen und welches Wissen über eine Person entstehen und mit welchen ggf. beeinträchtigenden Folgen überhaupt zu rechnen ist. Nicht zuletzt soll die Kenntnis des Verwendungszwecks der betroffenen Person eine gewisse Einschätzung dessen ermöglichen, was mit den sie betreffenden Daten passiert und welche Informationen über sie in welchen Kontexten gewonnen werden. Mit all dem erfüllt die Zweckfestlegung Funktionen der Begrenzung, der Strukturierung und der Transparenz in Fällen einer Verarbeitung personenbezogener Daten.[311] Im Rahmen der Rechtsgrundlagen obliegt es der verantwortlichen Stelle die konkreten Zwecke, für die die Daten verarbeitet werden sollen, präzise und eindeutig festzulegen.

84 Allerdings liefe die Zweckfestlegung leer, wenn nicht auch in der Zeitdimension eine den Prozess der Verarbeitung übergreifende Bindung an die vor oder bei Erhebung festgelegten Zwecke rechtlich gewährleistet wäre. Das Erfordernis der Zweckfestlegung wird deshalb in Art. 5 Abs. 1b DSGVO ergänzt um die Vorgabe, dass die gesamte Verarbeitung an die festgelegten Zwecke insoweit gebunden ist, als die personenbezogenen Daten nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Darin liegt eine gewisse, aber keine „strikte", sondern eine **relativierte Bindung an den ursprünglich festgelegten Zweck**[312]. Vielmehr schließt der Zweckbindungsgrundsatz in Gestalt des Art. 5 Abs. 1b DSGVO die **Möglichkeit von Zweckänderungen** ein, soweit die neuen Zwecke nach Maßgabe der Kriterien des Art. 6 Abs. 4 Hs. 2 DSGVO mit den ursprünglichen Verwendungszwecken ver-

[311] Vgl. zur Grundidee auch *Merel Elize Koning*, The purpose and limitations of purpose limitation, 2020, S. 58: „The purposes determine a chain of processing actions within one processing operation that starts at the moment of collecting the data and ends at the moment the purposes are fulfilled. The purposes specification, therefore, categorizes the data processing into viable processes with a start and end point: a processing operation." Sofern man die Funktionen in Kombination mit anderweitigen Schutzvorkehrungen sicherstellt, lassen sich auch im Bereich der Verwaltung prozeduralisierende Konzepte entwickeln. S. vor allem mit Blick auf Startups *von Grafenstein*, Principle (Fn. 278), S. 325ff.; *ders.*, Die Auswirkungen des Zweckbindungsprinzips auf Innovationsprozesse in Startups, in: Jürgen Taeger (Hrsg.), Smart World – Smart Law?, 2016, S. 233 (233ff.).

[312] Unzutreffenderweise wird oft behauptet, die DSGVO habe den Zweckbindungsgrundsatz in gleicher Gestalt verankert, wie er zuvor im deutschen Recht festgehalten war. S. zum Vergleich der (unterschiedlichen) Konzeptionen näher *Albers*, Selbstbestimmung (Fn. 31), S. 324f., 507ff.

einbar sind („**Zweckvereinbarkeit**"). Auch diese flexibilisierte Bindung kann jedoch – jedenfalls bei teleologisch treffender Auslegung und bei ergänzenden Vorkehrungen insbesondere zur Gewährleistung der Kenntnis der betroffenen Person[313] – im Verbund mit Zweckfestlegungen zur Begrenzung, Strukturierung und Transparenz von Datenverarbeitungen beitragen. Im dogmatischen Gesamtzusammenhang werfen Art. 5 Abs. 1b und Art. 6 Abs. 4 DSGVO allerdings eine Reihe von Auslegungsschwierigkeiten auf, die zu Kontroversen und zu unterschiedlichen Lösungen führen. Im Ergebnis muss sich eine Weiterverarbeitung zu einem kompatiblen geänderten Zweck ihrerseits im Rechtsrahmen des Art. 6 Abs. 1 DSGVO halten.[314] Art. 6 Abs. 4 Hs. 1 i.V.m. Art. 23 Abs. 1 DSGVO lässt weitere Zweckänderungen zu, die die Kriterien einer Zweckvereinbarkeit nicht erfüllen. Eine solche zweckändernde Weiterverarbeitung muss nicht nur die Voraussetzungen des Art. 6 Abs. 4 Hs. 1 i.V.m. Art. 23 Abs. 1 DSGVO einhalten, sondern auch von einem der Rechtmäßigkeitstatbestände des Art. 6 Abs. 1, ggf. i.V.m. Abs. 2 und 3, DSGVO getragen werden.[315] Im Bereich der öffentlichen Verwaltung relativieren sich beide Probleme allerdings im systematischen Zusammenhang mit anderen Normen.

Eine (Weiter-)Verarbeitung personenbezogener Daten für andere Zwecke als die ursprünglich festgelegten Zwecke ist im Bereich der Verwaltung nicht nur nach Maßgabe der **Zweckkompatibilitätsregelungen** des Art. 5 Abs. 1b i.V.m. Art. 6 Abs. 4 Hs. 2, Abs. 1, 2 und 3 DSGVO, sondern zudem nach Maßgabe der **Beschränkungsmöglichkeiten** der Artt. 6 Abs. 4 Hs. 1, 23 Abs. 1, 6 Abs. 1, 2 und 3 DSGVO und dann der **auf beide Varianten gestützten Zweckänderungsregelung** des § 23 BDSG möglich.[316] Dieser erlaubt Zweckänderungen in sechs katalogartig, wenn auch partiell generalklauselartig aufgelisteten Konstellationen. Dahinter stehen verschiedenartige Gründe, etwa die vermuteten Interessen der betroffenen Person, überwiegende Allgemeinwohlbelange oder überwiegende Rechte anderer Personen[317]. Die jeweiligen Tatbestände knüpfen die (Weiter-)Verarbeitung, von Ausnahmen abgesehen, dabei wiederum an die Erforderlichkeit für die Erfüllung der aufgelisteten Aufgaben und an den jeweils geänderten Zweck. Bei sensiblen Daten i.S.d. Art. 9 Abs. 1 DSGVO gestalten sich die Zweckänderungsmöglichkeiten enger (§ 23 Abs. 2 BDSG).[318] 85

[313] S. dazu Art. 13 Abs. 3, 14 Abs. 4 DSGVO. Vgl. außerdem *Peter Schantz*, in: BeckOK (Fn. 181), Art. 5 Rn. 19 ff. mit einem Fokus auf den Erwartungen der betroffenen Person.

[314] Ob die Weiterverarbeitung die Rechtmäßigkeitsanforderungen (auch) des Art. 6 Abs. 1 DSGVO erfüllen muss oder ob es ausreicht, wenn die ursprüngliche Erhebung durch einen der Tatbestände abgedeckt war und dann die Kriterien des Art. 6 Abs. 4 Hs. 2 DSGVO erfüllt sind, ist umstritten. Richtigerweise muss sich die Weiterverarbeitung – trotz der missverständlichen Formulierung in EG 50 – ihrerseits im Rahmen der Rechtmäßigkeitstatbestände des Art. 6 Abs. 1 DSGVO bewegen. Vgl. zur Debatte ausf. *Albers/Veit*, in: BeckOK (Fn. 181), DSGVO, Art. 6 Rn. 102 ff.; i. Erg. wie hier *BVerwG*, Urt. v. 27.9.2018 – 7 C 5/17, https://www.bverwg.de/270918U7C5.17.0, Rn. 27; s.a. *Tobias Herbst*, in: Kühling/Buchner (Fn. 107), Art. 5 Rn. 28 f., 49 f.; *Philipp Reimer*, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 5 Rn. 24; a.A. *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 5), Art. 6 Abs. 4 Rn. 12.

[315] Dazu *Albers/Veit*, in: BeckOK (Fn. 181), DSGVO Art. 6 Rn. 110 ff. m.w.N.; offen lassend BGH, Beschl.v. 24.9.2019 – VI ZB 39/18, https://juris.bundesgerichtshof.de, Rn. 44.

[316] § 23 BDSG deckt in bestimmtem Umfang auch Konstellationen ab, die die Voraussetzungen einer Zweckvereinbarkeit i.S.d. Art. 5 Abs. 1b i.V.m. Art. 6 Abs. 4 Hs. 2 DSGVO erfüllen.

[317] Näher *Albers/Veit*, in: BeckOK (Fn. 181), BDSG § 23 Rn. 19 ff.

[318] Dazu *Albers/Veit*, in: BeckOK (Fn. 181), BDSG § 22 Rn. 15 ff.; § 23 Rn. 40 ff.

86 Im **bereichsspezifischen Verwaltungsrecht** findet sich ein Spektrum von fallorientierten bis hin zu übergreifenden gesetzlichen Zweckfestlegungen, die allerdings nicht immer angemessen mit den Regelungs- und Schutzerfordernissen abgestimmt sind. Enge Zweckvorgaben sind sinnvoll, wenn ein besonderes Schutzniveau verankert werden muss oder soll. So sind die Zweckfestlegungen im Sozialrecht meistens auf konkrete Aufgaben bezogen,[319] und das Telekommunikations- und Telemediendatenschutzrecht sieht in §§ 9 und 19 TTDSG eine restriktive Zweckbestimmung und Möglichkeiten einer anonymen Nutzung vor, weil im Bereich des Internets zahlreiche, partiell sensible Nutzungsdaten anfallen, die leicht für personenbezogene Nutzungsprofile verwendet werden könnten. Abstrakte Zweckvorgaben oder Zweckbündelungen sind möglich, wenn sie aufgrund präzise gefasster sachlicher Aufgaben Gehalt gewinnen, die eingeschlossenen konkreten Zwecke und die dafür geltenden Vorgaben nicht miteinander unvereinbar sind und die sich im Kontext ergebenden Schutzerfordernisse betroffener Personen gewährleistet sind. Je nach Gesetzesfassung obliegt es in mehr oder weniger weit reichendem Umfang der Exekutive, die Zweckvorgaben aufgaben- und schutzbedarfsgerecht im Regelungs- und Entscheidungskontext zu konkretisieren.

bb) Erforderlichkeit als Regelungselement

87 Die Zweckbindung wird durch die in Art. 5 Abs. 1c DSGVO verankerte Anforderung der Angemessenheit, Erheblichkeit und Notwendigkeit ergänzt. Im Baustein der Phasenregulierung spiegelt sich dies im Regelungselement der **Erforderlichkeit** wider, das zu den gesetzlichen Komponenten der Regulierung des Umgangs mit personenbezogenen Informationen und Daten zählt.[320] Seinen Funktionen nach beschreibt es „eine **Relation** zwischen einem **Informationsverarbeitungsvorgang** und einer **Aufgabenerfüllung**"[321]. Es stellt eine Abhängigkeitsbeziehung zwischen der Verarbeitung personenbezogener Daten und den festgelegten Zwecken her und formuliert den Abhängigkeitsgrad, mit dem die jeweilige Stelle auf den jeweiligen Verarbeitungsvorgang angewiesen ist. Diese Relationierung ergänzt die Zweckbindung. Zugleich bewirkt sie, dass die einzelnen Phasen inhaltlich noch näher eingegrenzt werden können. Sie betrifft grundsätzlich sämtliche Phasen im Prozess der Gewinnung und Umsetzung von Informationen und der Verarbeitung von Daten.[322] Erforderlich sein muss erstens gerade der jeweilige Verarbeitungsschritt mit den ihm zukommenden Funktionen. Zweitens muss die Verarbeitung gerade der personenbezogenen Informationen und Daten erforderlich sein, auf die sich die Verarbeitung bezieht. Drittens kann man weiter differenzieren, ob die Verarbeitung gerade personenbezogener Informationen und Daten erforderlich ist oder ob nicht anonymisierte oder pseudonymisierte Daten genügen.

---

[319] Vgl. *BSGE* 90, 162 (166 f.), zur Frage, ob Krankenkassen im Rahmen des § 284 SGB V zur Mitgliederwerbung Daten erheben dürfen.

[320] S. a. oben → Rn. 52, dass dies nicht mit der Erforderlichkeitskomponente des Übermaßverbots gleichgesetzt werden darf.

[321] *Adalbert Podlech*, Individualdatenschutz – Systemdatenschutz, in: Klaus Brückner/Gerhard Dalichau (Hrsg.), Beiträge zum Sozialrecht. Festgabe für Grüner, 1982, S. 451 (455).

[322] Anonymisierung und Pseudonymisierung, Löschung und Einschränkung sind dabei wegen ihrer eigenständigen Bedeutung ausgenommen.

Im Rahmen der **gesetzlichen Ausgestaltung** beschränkt sich § 3 BDSG darauf festzuhalten, dass die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig ist, wenn sie **zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe** oder **in Ausübung öffentlicher Gewalt,** die dem Verantwortlichen übertragen wurde, **erforderlich** ist. Mehr als dies kann in einem allgemeinen Standard und Auffangtatbestand nicht geregelt werden. Trotz ihrer allgemeinen Formulierung ist die Regelung keine nichtssagende Floskel. Vielmehr **verknüpft** sie die Datenverarbeitung zum einen über die Zweckbindung („zur Erfüllung der Aufgabe") **mit dem materiellen Verwaltungsrecht** sowie den dort geregelten sachlichen Kompetenzen, zum anderen über den Bezug auf gerade den zuständigen Verantwortlichen **mit dem Organisationsrecht** und der **Zuständigkeitsverteilung.** Demnach darf eine öffentliche Stelle personenbezogene Daten nur verarbeiten, soweit sie selbst eben diese Daten zur Erfüllung einer ihr zugewiesenen konkreten Aufgabe nach Maßgabe ihrer Befugnisse benötigt. Der Gesetzgeber hat zudem – dies verweist auf den Baustein der Systemgestaltung – die Möglichkeit, datenschutzrechtliche Ziele durch einen höheren Präzisionsgrad auf der sachlichen Ebene sicherzustellen. Die Voraussetzung der „Erforderlichkeit zur Aufgabenerfüllung" bedeutet zugleich, dass in den Fällen, in denen § 3 BDSG die Ermächtigungsgrundlage hergibt, immer auch der Blick in den sachlichen Regelungskomplex notwendig ist, über den sich erst ergibt, ob die in Rede stehenden Daten für eine bestimmte rechtlich gedeckte Aufgabenerfüllung gebraucht werden.[323] 88

Im Rahmen der Erforderlichkeit muss man bestimmen, **welche Informationen** und **welche Daten als Informationsgrundlage** die staatliche Stelle benötigt, damit sie die Aufgabe oder Befugnis in einem konkreten Fall vollständig und in rechtmäßiger Weise wahrnehmen kann. Was dies bedeutet, wird in datenschutzrechtlichen Debatten oft kaum gesehen. Dabei ist die Auslegung der in Bezug genommenen sachlichen Normen und ihrer Tatbestandsmerkmale und die semantische Beschreibung der in den Normanwendungssituationen benötigten Informationen schon für sich genommen mehr oder weniger **anspruchsvoll.** Erschwerend kommt hinzu, dass vor allem zu Beginn eines Verarbeitungsprozesses noch der Prozess selbst antizipiert werden muss, der sich komplex gestalten und relativ unberechenbar verlaufen kann. Ob bestimmte personenbezogene Daten später tatsächlich noch benötigt werden, kann eine **hochgradig ungewisse Prognose** sein. Insofern kann die Erforderlichkeit gegebenenfalls nur prozedural angelegt und muss im Verarbeitungsablauf spezifiziert werden. 89

Bereichsspezifisch lässt sich die Komponente der Erforderlichkeit auf der Ebene der gesetzlichen Ausgestaltung in verschiedener Weise näher gestalten und präzisieren. Sie kann in **phasenbezogene Tatbestandsvoraussetzungen** eingehen. Auch kann der geforderte **Abhängigkeitsgrad** in unterschiedlicher Schärfe bestimmt werden.[324] Fehlt es an einer gesetzlichen Spezifikation, werden Einschreitschwellen oder tatbestandliche Einschränkungen im sachlichen Ge- 90

[323] Siehe z. B. die Konkretisierungen der jeweils fallrelevanten Normen mit Blick auf Kompetenzen und Zweckfestlegungen in BVerwGE 120, 188 (191 ff.); BSGE 90, 162 (166 ff.); HessVGH NJW 2005, S. 2727 (2730 ff.).

[324] Zum Polizeirecht *Albers*, Determination (Fn. 268), S. 281.

samtzusammenhang teilweise durch Verwaltungsvorschriften,[325] teilweise im Wege der Interpretation der Erforderlichkeitskomponente herauskristallisiert.[326]

b) Phasenbezogene Elemente

91 Zu den phasenübergreifenden Elementen der Zwecksetzungen und der Erforderlichkeit kommen **phasenbezogene Elemente** hinzu. Diese reagieren unter Berücksichtigung der Funktionen verschiedener Verarbeitungsphasen in den Verarbeitungsprozessen auf die **normativen Probleme**, die sie einerseits für sich, andererseits mit Blick auf Verarbeitungsabläufe und -kontexte aufwerfen. Die **allgemeinen Vorgaben** der DSGVO und des BDSG adressieren lediglich einige **Grundsatzfragen.** Hier finden sich Regelungen etwa zur **Offenheit der Datenerhebung**[327], für **Datenübermittlungen** von öffentlichen Stellen an andere öffentliche oder an nicht-öffentliche Stellen[328] oder zur **Löschung**[329]. So gibt § 25 Abs. 1 BDSG für Datenübermittlungen einer öffentlichen Stelle an eine andere im Verhältnis zum Betroffenen eine Ermächtigungsgrundlage in allen Fällen her, für die eine bereichsspezifische Vorschrift weder vorhanden ist noch wegen der Eingriffsintensität notwendig wäre.[330] Phasenbezogene Elemente betreffen die Zulässigkeit einer mit der Übermittlung ggf. verbundenen Zweckänderung[331] und die relativierte Bindung der Verarbeitung auf Seiten der empfangenden Stelle an den Zweck, zu dessen Erfüllung ihr die Daten übermittelt wurden[332]. Der Richtigkeit der Informationen und der Gewährleistung bestimmter Rechtmäßigkeitsbedingungen, die die empfangende Stelle beachten muss, dienen im Anwendungsbereich des § 45 BDSG die in §§ 74 und 75 BDSG verankerten Überprüfungs-, Beifügungs-, Hinweis- und Nachberichtspflichten. Hinsichtlich der Löschung der personenbezogenen Daten finden sich spezifischere Vorgaben

---

[325] Vgl. z. B. zum Abruf von Kontostammdaten durch die Finanzbehörde i. V. m. dem einschlägigen Anwendungserlass des BMF zur AO und zur Frage, ob dies als Einschreitschwelle genügt, *BVerfGE* 118, 168 (191 ff.).

[326] Für die Videoüberwachung öffentlicher Räume etwa *VGH BW*, MMR 2004, S. 198 (201): „[…] die zu überwachenden Orte (werden) durch das in § 21 Abs. 3 PolG enthaltene [.] Erforderlichkeitskriterium weiter eingegrenzt. […] Dieses Merkmal bedeutet […], dass die Örtlichkeit eine besondere Kriminalitätsbelastung aufweisen, es sich bei ihr um einen sog. Kriminalitätsbrennpunkt handeln muss".

[327] S. dazu die Unterrichtungspflichten in Art. 13, 14 DSGVO.

[328] Für nicht-öffentliche Stellen s. § 25 Abs. 2 BDSG. Zum bayerischen Recht und zur Abstimmung mit Auskunftsansprüchen der Presse BVerwG, Urt. v. 27.9.2018 – 7 C 5/17, https://www.bverwg.de/270918U7C5.17.0. Den privaten Dritten vermittelt § 25 Abs. 2 BDSG – ebenso wie der betroffenen Person – ein subjektives öffentliches Recht. Privaten stehen auch Informationszugangsansprüche nach dem Informationsfreiheitsgesetz zu, das nach § 1 Abs. 2 BDSG vorgeht und seinerseits in § 1 Abs. 1 und 2, § 5, § 7 Abs. 1 S. 3 und Abs. 4 oder § 8 IFG einschlägige Vorschriften enthält. Soweit sich der Informationserhalt nach diesen Vorschriften richtet und einfacher ist, wird die praktische Bedeutung des § 25 Abs. 2 BDSG relativiert.

[329] Zum Löschen, hier auch zu den Fragen der Anforderungen an den Löschvorgang und zur Durchsetzbarkeit, vgl. *Sven Hunzinger*, Das Löschen im Datenschutzrecht, 2018.

[330] Der empfangenden Stelle vermittelt die Norm keinen Anspruch darauf, dass die in Rede stehenden Daten übermittelt werden. Zum „Doppeltürmodell", das Mitteilungs- oder Übermittlungsbefugnisse auf Seiten der weiterleitenden Stelle und Empfangs- und Verwendungsbefugnisse auf Seiten der empfangenden Stelle erfordert, vgl. auch *BVerfGE* 130, 151 (184); *BayVGH*, Beschl. v. 20.8.2019, 12 ZB 19.333, BeckRS 2019, 18701; *BVerfG*, Beschl. v. 27.5.2020 – 1 BvR 1873/13 u. 2618/13 – Bestandsdatenauskunft II, www.bverfg.de, Rn. 93, 95.

[331] § 25 Abs. 1 S. 1 i. V. m. § 23 BDSG .

[332] § 25 Abs. 1 S. 2 und 3 BDSG.

in den ausdrücklich verankerten Rechten betroffener Personen und korrespondierenden Pflichten Verantwortlicher.[333] Allerdings sind in der öffentlichen Verwaltung auch Dokumentationsfunktionen zu beachten, die einer Löschung entgegenstehen können, dann aber mit einer Einschränkung der Verarbeitung[334] verbunden sein müssen.[335] Die praktische Umsetzung kann hier sehr anforderungsreich sein. Im **bereichsspezifischen Recht** können für bestimmte Verarbeitungsphasen mehr oder weniger detailliertere Vorgaben gelten. Illustrativ sind die ausführlichen Regelungen zur Informations- und Datenverarbeitung des Bundeskriminalamts oder auch Offenlegungsregelungen, die die Einsicht und Nutzung von Archivdaten ermöglichen[336].

c) Rechtmäßigkeitsanforderungen und Rechtswidrigkeitsfolgen

Mit den Rechtmäßigkeitsanforderungen an den Umgang mit personenbezogenen Informationen und Daten wird die „rechtmäßige Handhabung der informationellen Ressourcen [...] zu einem Bezugspunkt, an dem sich das Verfahren ebenso zu orientieren hat wie an der Sachentscheidung, die bisher im Vordergrund stand".[337] Da sich die einzelnen Verarbeitungsphasen dabei nicht nur faktisch, sondern auch rechtlich in Verarbeitungs- und Regelungszusammenhänge eingliedern, sind sie nicht isoliert, sondern mit Blick auf ihre Chronologie zu beurteilen. Informationen haben eine **„Informationsgeschichte"**.[338] Deshalb müssen im Verwaltungsrecht nunmehr in breitem Umfang Fragen beantwortet werden, die im Strafprozessrecht in Gestalt der „Beweisverbote und deren „Fernwirkung" zu den besonders schwierigen Problemen gehören. Man darf weder davon ausgehen, dass es gar keine Rechtswidrigkeitszusammenhänge, sondern lediglich isoliert zu beurteilende Vorgänge gibt, noch darf man ohne Weiteres zugrunde legen, dass die Rechtswidrigkeit eines bestimmten Verarbeitungsschrittes bedeutet, dass auch alle nachfolgenden Schritte rechtswidrig sind („Rechtswidrigkeitskette"). Vielmehr sind die in Rede stehenden Verarbeitungsvorgänge anhand eines jeweils **eigenständigen und dabei zugleich die Verarbeitungszusammenhänge berücksichtigenden Rechtmäßigkeitsurteils** zu beurteilen. 92

Soweit es um die Rechtswidrigkeitszusammenhänge zwischen einzelnen Verarbeitungsvorgängen geht, lassen sich unterschiedliche Aspekte abschichten. Das Problem der Rechtswidrigkeitsfolgen im Verarbeitungsprozess stellt sich nicht, sofern bestimmte gesetzliche Maßgaben **durchgängig**, also für jede Phase, greifen und (auch) in der zu beurteilenden Phase fehlen. Erfüllt die Verarbeitung diese Voraussetzungen nicht, ist sie aus sich heraus rechtswidrig und löst 93

[333] Etwa Art. 17 Abs. 2 DSGVO.

[334] Zur Einschränkung s. die Legaldefinition in Art. 4 Nr. 3 DSGVO: Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Zumal wegen der Probleme einer bloßen Markierung – dazu *Alexander Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 5), Artikel 4 Nr. 3 Rn. 3 ff. – ist diese Definition unvollständig und man muss weitere Maßnahmen, etwa die Auslagerung der Daten auf ein anderes Datenverarbeitungssystem oder Maßnahmen im Rahmen des Zugriffsmanagements, einschließen.

[335] S. dazu Art. 17 Abs. 3b und d DSGVO, § 35 Abs. 2 BDSG.

[336] Dazu *BVerwG*, NJW 2019, 2186 Rn. 26 ff.: Archivrechtlicher Anspruch auf Nutzung von Unterlagen des BND.

[337] *Carl-Eugen Eberle*, Zum Verwertungsverbot für rechtswidrig erlangte Informationen im Verwaltungsverfahren, in: GS Wolfgang Martens, 1987, S. 351 (358).

[338] *Friedhelm Hufen*, Fehler im Verwaltungsverfahren, 4. Aufl. 2002, Rn. 147.

Unterlassensansprüche aus. Wenn Maßgaben dagegen nicht durchgängig gelten oder zwar im ersten Verarbeitungsschritt fehlen, dann aber vorliegen,[339] kommt es primär darauf an, inwieweit **Rechtswidrigkeitsfolgen** in unionsrechts- und verfassungsmäßiger Weise **im Gesetz** selbst verankert sind. Ergeben sich aus dem Gesetz keine ausdrücklichen Vorgaben, müssen Exekutive und Judikative mit Blick auf den jeweils relevanten Regelungszusammenhang **interpretatorische Antworten** entwickeln[340]. Mit Hilfe des Kriteriums des Rechtswidrigkeitszusammenhanges lassen sich zunächst Verstöße gegen Regelungselemente ausgrenzen, die ausschließlich eine bestimmte Phase betreffen und gar nicht auf den Verarbeitungsverlauf durchgreifen. Das hilft allerdings nur begrenzt weiter, weil die phasenbezogenen Regelungen mit vielen ihrer Elemente ein sich ergänzendes Schutzkonzept bilden. Soweit Rechtmäßigkeitsverstöße Relevanz haben, kann im Verwaltungsverfahren der in § 45 VwVfG verankerte Grundgedanke der Heilung herangezogen werden: Bestimmte Rechtmäßigkeitsanforderungen, etwa die Unterrichtungspflichten im Falle der Erhebung beim Betroffenen, können mit der Folge einer Korrektur der Rechtsfehler nachgeholt oder zumindest kompensiert werden.[341] Ausgeweitet wird der Heilungsgedanke in der Konstruktion des hypothetischen Ersatz- oder Wiederholungseingriffs, nach der nachfolgende Verarbeitungsschritte keinem Rechtswidrigkeitsverdikt unterliegen, wenn die Behörde die Daten auch rechtmäßig erlangen könnte oder hätte erlangen können.[342] Die Überzeugungskraft dieser Konstruktion muss konstellationsabhängig und gegebenenfalls in den bereichsspezifischen Regelungszusammenhängen beurteilt werden.[343] Soweit eine Heilung nicht möglich ist, muss man mit einer normgeleiteten Abwägung operieren.[344] Dafür kann man allgemein geltende, allerdings gegebenenfalls bereichsspezifisch auszufüllende Kriterien anführen. Auf der einen Seite spielen das überindividuelle Interesse an der grundsätzlichen Rechtmäßigkeit exekutiven Handelns (Aspekt rechtsstaatlicher „Disziplinierung"[345]), die Schutzfunktionen des Tatbestandselements, gegen das verstoßen worden ist[346], die Schwere der Rechtsverletzung und die Schutzwürdigkeit der betroffenen Person eine Rolle. Auf der anderen Seite stehen

[339] Dies sind die eigentlich problematischen Konstellationen. Beispiel: Eine Behörde erhebt personenbezogene Daten, ohne dass die Voraussetzungen der Erhebungsermächtigung erfüllt wären, und gewinnt durch die rechtswidrige Erhebung Erkenntnisse, aufgrund derer nunmehr die Voraussetzungen einer Verarbeitung der Daten erfüllt sind.

[340] Knapp dazu, dass das Regime der DSGVO nichts an der Verwertbarkeit rechtswidrig von Privaten erlangter Beweismittel im Strafverfahren geändert habe, BGH, Beschl. v. 18.8.2021, 5 StR 217/21, Rn. 7. Zum Problem und zu Lösungen vgl. mit Blick auf das Strafverfahren *BVerfGE* 130, 1 (Rn. 95 ff.); für parlamentarische Untersuchungsausschüsse s. *BVerfGE* 124, 78 (127 f.). S. außerdem *BSG*, NZS 2006, 43 (45 ff.); *OVG Hamburg*, NJW 2008, 96 (98 ff.) mit differenziert ausgearbeiteter Sicht.

[341] Das Verwaltungsverfahren unterscheidet sich an dieser Stelle grundlegend vom Strafprozess, in dem eine Nachholung oder Kompensation der Rechtmäßigkeitsanforderungen an die vorangegangene Informations- und Datenverarbeitung der Polizei oder der Staatsanwaltschaft in der Regel nicht möglich ist.

[342] Dazu in allgemeinem Kontext *Klaus Macht*, Verwertungsverbote bei rechtswidriger Informationserlangung im Verwaltungsverfahren, 1999, S. 57 f., 252 ff.

[343] Zum Polizeirecht *Albers*, Determination (Fn. 268), S. 320 ff., 325 ff.

[344] S. auch m. w. N. *OVG Lüneburg*, Urt. v. 20.11.2014, 11 LC 232/13 (juris), Rn. 33.

[345] *Albers*, Determination (Fn. 268), S. 331 f.

[346] Vgl. dazu *BGHSt* 38, 214 (220); 38, 372 (373 f.); 42, 15 (21); *BGH*, NStZ 1995, S. 410 (410 f.); zum Richtervorbehalt einerseits *BVerfG (Kammer)*, NJW 2015, S. 1005 (1006 f.), andererseits OVG Sachsen-Anhalt, Beschl. v. 15.6.2017, 3 M 100/17 (juris), Rn. 10 ff.

Inhalt, Umfang und Gewicht der Rechtsgüter oder der öffentlichen Belange, die im Falle einer Rechtswidrigkeit der weiteren Verarbeitung der Daten nicht geschützt oder realisiert werden könnten. Die Abwägung erfolgt demnach nicht in völlig neuer Weise, sondern ist auch an das (verletzte) Tatbestandselement in der Regelung des vorangegangenen Verarbeitungsschrittes rückgebunden. Die Folgen der Rechtswidrigkeit können jedoch, ohne dass die entsprechenden normativen Vorgaben und ihre Verletzung ganz bedeutungslos wären, in bestimmtem Umfang relativiert werden.

Sofern der Zusammenhang zwischen Informationsverwendung und Sachentscheidung zu beurteilen ist, kann die Rechtswidrigkeit jener prinzipiell nach § 46 VwVfG **unbeachtlich** sein.[347] Im Vergleich zum Verhältnis zwischen Verwaltungsverfahren und Abschlussentscheidung resultieren jedoch Einschränkungen daraus, dass der Umgang mit personenbezogenen Informationen und Daten mehr noch als das Verwaltungsverfahren eigenständige Schutzinteressen realisiert. Die Rechtswidrigkeit einer Informationsverwendung wirkt sich jedenfalls dann nicht aus, wenn die Entscheidung bereits von anderweitigen Informationen getragen wird, die in sie eingeflossen sind.[348] Für die Frage, inwiefern die Rechtswidrigkeit eines Verarbeitungsschrittes nicht nur die Verwertung gewonnener Informationen in weiteren Verarbeitungsschritten des jeweiligen Verfahrens verbietet, sondern es im Sinne einer „Fernwirkung" darüber hinaus ausschließt, dass die gewonnenen Informationen als Anlass neuer Ermittlungen genutzt werden, sind ebenfalls zunächst die Aussagen des Gesetzes und die sich daraus ergebende Reichweite des Verwertungsverbots relevant. Im Übrigen ist auch insoweit eine normgeleitete Abwägung unter Berücksichtigung der oben genannten Kriterien vorzunehmen.[349] 94

4. Verantwortlichkeit und Verantwortlichkeitspflichten

Im Mittelpunkt vielschichtiger konkreter Pflichten hinsichtlich der Verarbeitung personenbezogener Daten steht der „Verantwortliche". Ihrer Funktion nach soll die Figur der **Verantwortlichkeit** – angesichts dessen, dass sich der Umgang mit personenbezogenen Informationen und Daten außerhalb der Sphäre der geschützten Personen vollzieht – für diese Personen und auch für die Datenschutzaufsicht einen **Zurechnungsendpunkt hinsichtlich datenschutzrechtlicher Pflichten** liefern. Maßgeblich für die Verantwortlichkeit ist, dass eine Stelle allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[350] In Fällen der Auftragsverarbeitung oder der Verarbeitung durch Dritte, wie sie je nach Ausgestaltung beispielsweise in Konstellationen des Cloud Computing gegeben sind[351], bleibt der Verantwortliche grundsätzlich selbst für die Einhaltung der Datenschutz- 95

[347] Ausführlicher *Macht*, Verwertungsverbote (Fn. 342), S. 275 ff., sowie weiter zur „Fernwirkung" S. 294 ff. Dazu, dass § 46 VwVfG einen allgemeinen Rechtsgedanken festhält, *BVerwGE* 110, 173 (180).

[348] S. auch *Macht*, Verwertungsverbote (Fn. 342), S. 284 ff.

[349] Vgl. dazu grdsl., wenn auch im Detail etwas verkürzt *BVerwG*, DVBl 2018, S. 658 (660 f.).

[350] Art. 4 Nr. 7 DSGVO.

[351] Zu den Legaldefinitionen Art. 4 Nr. 8 und Nr. 10 DSGVO. Zum Cloud Computing *Thomas Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 5), Art. 28 Rn. 18 ff.: Die große Bandbreite der in diesem Rahmen angebotenen Dienstleistungen verbietet eine pauschale datenschutzrechtliche Einordnung.

vorgaben verantwortlich.[352] Ansonsten liefert der Begriff der „Entscheidung" und auch derjenige der „Zwecke und Mittel der Verarbeitung" allerdings nicht unbedingt hinreichende Kriterien. Etwa hat man im Bereich von Social Media-Plattformen, in dem im Falle von nutzergenerierten Inhalten unterschiedliche Akteure jeweils bestimmte Entscheidungen treffen, mit einem **Geflecht an Verantwortlichkeiten** zu tun.[353] Da die gemeinsame Verantwortlichkeit in solchen Fällen keine gleichwertige Verantwortlichkeit sein kann[354], steht man vor dem Erfordernis nicht nur der Bewertung einzelner Beiträge, sondern vor allem auch der Aufschlüsselung der Konstellation. Im Bereich der Verwaltung stellt sich dieses Problem allerdings nicht flächendeckend. Gerade hier können Verantwortliche oder nähere Kriterien auch durch ggf. mitgliedstaatliche Rechtsnormen vorgegeben werden. Zu besonderen Herausforderungen führen bei einer zunehmend digitalisierten Verwaltung allerdings **vernetzte soziotechnische Systeme** unter Mitwirkung privater Unternehmen und/oder unter Einsatz Künstlicher Intelligenz, bei denen man absehen kann, dass **Entscheidungsmacht als Ansatz** der Zuschreibung von Verantwortlichkeit **verkürzt** ist.[355]

96 Zu den zentralen **Pflichten**, die aus der Verantwortlichkeit resultieren, gehört nach Maßgabe eines **grundsätzlich risikobasierten Ansatzes** die allgemeine Verpflichtung, geeignete technische und organisatorische Maßnahmen umzusetzen, damit die Einhaltung sämtlicher einschlägiger Anforderungen an die Verarbeitung personenbezogener Daten sichergestellt und nachgewiesen werden kann.[356] Die sich bereits in diesem Rahmen ergebenden allgemeinen Dokumentationspflichten und -obliegenheiten[357] werden durch die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten[358] und durch spezielle Pflichten wie etwa die zur Dokumentation von Verletzungen des Schutzes personenbezogener Daten[359] konkretisiert und ergänzt. Solche Verletzungen muss der Verantwortliche unter bestimmten Voraussetzungen der Aufsichtsbehörde oder auch der betroffenen Person melden.[360] Schon aufgrund dieser Anforderungen wird im Ergebnis ein mehr oder weniger ausgeprägtes und aufwändiges **Datenschutzmanagement** entstehen. In besonders risikobehafteten Fällen muss auch eine Datenschutzfolgenabschätzung als Vorab-Evaluation durchgeführt

---

[352] Vgl. auch die näheren Regelungen in Art. 28, 29 DSGVO.

[353] Dazu *EuGH*, Urt. v. 5.6.2018 – C-210/16, http://curia.europa.eu, Rn. 29 ff. – Fanpage; *EuGH*, Urt. v. 24.9.2019 – C-136/17, http://curia.europa.eu, Rn. 34 ff. – GC u. a.

[354] *EuGH*, Urt, v. 5.6.2018 – C-210/16, http://curia.europa.eu, Rn. 43: Die Akteure können „in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist."

[355] Vgl. auch zur Entwicklung einer neuen Verantwortlichkeitsfigur für Plattformen *Florian Wittner*, Die datenschutzrechtliche Verantwortlichkeit im Kontext der verteilten Verarbeitungsrealität, Manuskript 2021 (i. E.), S. 382 ff.

[356] Allgemein Art. 5 Abs. 2, 24 DSGVO. Die Pflichten sind Grundlage der Haftung des Verantwortlichen. S. auch Art. 82 DSGVO.

[357] Überblick bei *Niels Lepperhoff*, Dokumentationspflichten in der DSGVO, RDV 2016, S. 197 ff.

[358] Art. 30 Abs. 1 und Abs. 2 DSGVO geben dessen Inhalte (z. B. die Beschreibung der Zwecke der Verarbeitung oder der Kategorien betroffener Personen, personenbezogener Daten und von Empfängern) detailliert vor.

[359] Art. 33 Abs. 5 DSGVO; zur Legaldefinition der „Verletzung des Schutzes personenbezogener Daten" Art. 4 Nr. 12 DSGVO.

[360] S. die im einzelnen differenzierten Regelungen der Art. 33, 34 DSGVO.

werden.[361] Die öffentliche Verwaltung ist davon befreit, wenn Rechtsnormen die Verarbeitungsvorgänge hinreichend konkret regeln und es im Normsetzungsverfahren bereits eine spezifizierte Datenschutzfolgenabschätzung gegeben hat.

5. Rechte der betroffenen Personen

a) Informationsrechte

Informationsrechte der betroffenen Personen erfüllen unterschiedliche **Funktionen**: Sie sollen der Person die Informationen über das Wissen öffentlicher Stellen oder anderer Privater vermitteln, die – im Sinne einer „Wissensfacette" des Persönlichkeitsschutzes – für die freies Verhalten erst ermöglichenden Orientierungen und die relative Erwartungssicherheit sowie für das Selbstwertgefühl und eine Selbstbehauptung notwendig sind.[362] Sie liefern das Zwischenglied zwischen den Verarbeitungsregulierungen und Verantwortlichkeitspflichten einerseits und den Einflussnahmechancen andererseits, die die betroffenen Personen nur im Falle eigener Informationen wahrnehmen können. Insofern sollen sie eine zuverlässige Grundlage für die von den Betroffenen selbst zu treffende Entscheidung darüber hergeben, welche Relevanz den jeweiligen Verarbeitungen beigemessen und inwieweit auf deren Inhalte oder deren Verlauf Einfluss genommen wird. Sie ermöglichen des Weiteren den individuellen Rechtsschutz.[363] Im Hinblick auf die Verwaltung tragen sie nicht zuletzt zu deren Legitimation bei. Ihre Funktionen verweisen darauf, dass die reguläre informierende, beratende und unterstützende Kommunikation zwischen Verwaltung und Bürgern über die rechtlich geregelten Formen hinausgehen kann und wird. Ebenso wie verwaltungsverfahrensrechtliche Positionen wie die Anhörung oder Akteneinsichtsrechte bieten die **datenschutzrechtlichen Informationsansprüche** den Betroffenen rechtsförmige Minimalpositionen in Gestalt einer **Reserveordnung.**[364] Ihre Ziele der Orientierungs- und Erwartungssicherheit der betroffenen Personen und der Legitimation der Verwaltung erreichen sie gerade auch dann, wenn sie lediglich vorhanden sind, aber nicht permanent in Anspruch genommen werden (müssen).[365] 97

Bei der Gewährleistung von Informationsrechten ist auf einer ersten Stufe das Problem zu lösen, wie die betroffenen Personen erfahren können, in welchen Zusammenhängen und bei welcher Stelle überhaupt sie betreffende Informationen und Daten verarbeitet werden. Die notwendigen **übergreifenden Orientierungschancen** werden partiell dadurch gewährleistet, dass der exekutive Umgang mit personenbezogenen Informationen und Daten durch **normenklare Regelungen** begrenzt, strukturiert und transparent gestaltet wird.[366] Diese Regelungen erfül- 98

[361] Dazu → Rn. 74.

[362] Ausf. zu dieser Überlegung *Albers*, Selbstbestimmung (Fn. 31), S. 469 ff.; s. a. *BVerfG* (Kammer), NJW 2006, 1116 (1117 ff.); *BVerfGE* 120, 351 (362 f.).

[363] Zum grundrechtlichen Hintergrund → Rn. 26, 33. Übergreifender zu gerichtlichen Verwaltungskontrollen → Bd. II *Möllers/Buchheim* § 46.

[364] Zu den Informationsfunktionen der verwaltungsverfahrensrechtlichen Beteiligungsrechte vgl. auch *Gusy*, Informationsbeziehungen (Fn. 273), Rn. 43.

[365] Deswegen bedeutet ihre nur gelegentliche Inanspruchnahme in der Praxis nicht, dass sie wegen Desinteresses überflüssig wären. Im Gegenteil sorgt ihre Verankerung für das Vertrauen in ordnungsmäßige Verwaltungsabläufe, auf das die Verwaltung angewiesen ist.

[366] S. auch *BVerfGE* 112, 33 (53 ff.).

len also **nicht lediglich Steuerungs-, sondern auch die Informationsfunktionen,** die Rechtsnormen im Rechtsstaat zukommen. Unterhalb der Normebene könnten **Informations- und Kommunikationspläne** die Strukturen und Prozesse exekutiver Informations- und Datenverarbeitungen in den jeweiligen Kommunikations- und Entscheidungszusammenhängen veranschaulichen.[367]

99 Auf einer zweiten Stufe garantieren zunächst Pflichten und Rechte hinsichtlich einer **Unterrichtung auf Initiative der Verwaltung** die individuellen Kenntnismöglichkeiten. Art. 12 bis 14 DSGVO geben den Verantwortlichen umfangreiche Informationspflichten mit näheren Maßgaben zu deren Inhalten oder zur Art und Weise der Informationsvermittlung auf. Den Pflichten entsprechen Rechte der betroffenen Personen. Dabei soll die Unterrichtung über die Identität der verantwortlichen Stelle sicherstellen, dass die betroffene Person weiß, mit wem sie es zu tun hat und gegenüber wem sie ihre Rechte geltend machen kann. Die Mitteilung der Zweckbestimmungen, zu denen die personenbezogenen Daten verarbeitet werden, soll der betroffenen Person vermitteln, wofür die Daten benötigt und verwendet werden, welche Informationen in einem bestimmten Kontext daraus entstehen und mit welchen Folgen dies unter Umständen verbunden sein wird. Auch angesichts der Regelungen zur Zweckvereinbarkeit ist in diesem Zusammenhang von besonderer Bedeutung, dass der Verantwortliche der betroffenen Person vor einer beabsichtigten Zweckänderung alle relevanten Informationen darüber zu Verfügung zu stellen hat.[368] In **bereichsspezifischen Regelungskomplexen** finden sich insbesondere im Sicherheitsrecht **Benachrichtigungspflichten** zur Kompensation der Heimlichkeit der jeweiligen Datenerhebungen und -verarbeitungen.

100 Bereits in den Regelungen der DSGVO finden sich **Eingrenzungen und Einschränkungen** der in ihr geregelten Informationspflichten und -rechte. Dazu gehören die Fälle, dass die betroffene Person bereits über die Informationen verfügt[369] oder dass diese hinreichend präzisen unionalen oder mitgliedstaatlichen Rechtsvorschriften entnommen werden können[370]. Hinzu kommen die sich mitgliedstaatlichem Recht öffnenden Beschränkungsmöglichkeiten des Art. 23 DSGVO. Einschränkungen, wie sie dann in § 32 und 33 BDSG etwa aus den Gründen der Gefährdung ordnungsmäßiger Aufgabenerfüllung, der Gefährdung der öffentlichen Sicherheit oder Ordnung oder sonstiger Nachteile zu Lasten des Wohls des Bundes oder eines Landes vorgesehen werden, sind nur nach Maßgabe einer Abwägung mit den Interessen der betroffenen Person tragfähig. Diese Abwägung muss in inhaltlicher, zeitlicher und personeller Hinsicht differenziert erfolgen, also sorgfältig unterscheiden, welche Angaben ab bzw. bis wann und wem mitzuteilen oder nicht mitzuteilen sind.[371] Auch im bereichsspezifischen Sicherheitsrecht sind Abwägungen nötig, selbst wenn hier weiter spezifizierte Einschränkungen tragfähig sein können.

101 An die Initiative der betroffenen Person knüpfen **Ansprüche auf Auskunft** an, wie sie Art. 15 Abs. 1 DSGVO der betroffenen Person verbürgt. Geschützt ist das **reine Informationsinteresse der betroffenen Person,** ohne dass es auf eine poten-

[367] S. dazu im Informationsfreiheitsrecht § 11 IFG.
[368] Art. 13 Abs. 3, 14 Abs. 4 DSGVO.
[369] Art. 13 Abs. 4, 14 Abs. 5a DSGVO.
[370] Art. 14 Abs. 5c DSGVO mit weiteren Voraussetzungen.
[371] Vgl. insoweit *BVerwGE* 89, 15 (20 ff.); 118, 10 (13 f.), 119, 11 (13 ff.).

zielle Verletzung anderweitiger Rechte ankäme.[372] Der Schutz dieser Interessen wird durch das begleitende Recht verstärkt, dass der Verantwortliche der betroffenen Person eine Kopie oder ein gängiges elektronisches Format zur Verfügung stellt.[373] Die zu erteilende Auskunft kann sich u.a. auf die Verarbeitungszwecke, die Kategorien personenbezogener Daten, auf die Empfänger oder Kategorien von Empfängern, auf die geplante Speicherdauer, auf die Datenherkunft oder auf die Bedingungen der Möglichkeit der Wahrnehmung bestimmter Betroffenenrechte erstrecken. Entscheidend ist, dass die Person den Prozess der sie betreffenden Informations- und Datenverarbeitung nachvollziehen und ihre Rechte einschätzen kann. Der Auskunftsanspruch unterliegt hinsichtlich des Rechts auf Erhalt einer Kopie den **Grenzen** des Art. 15 Abs. 4 DSGVO und den **Beschränkungsmöglichkeiten** aufgrund des Art. 23 DSGVO. Für Einschränkungen aus Gründen der Gefährdung ordnungsmäßiger Aufgabenerfüllung oder der Gefährdung der öffentlichen Sicherheit oder Ordnung (vgl. § 34 Abs. 1 Nr. 1 i.V.m. § 33 Abs. 1 Nr. 1, Nr. 2b und Abs. 3 BDSG) gilt wiederum das Erfordernis einer Abwägung mit den Interessen des Betroffenen. Eingrenzungen, die die betroffene Person zur Bezeichnung der Art der Daten verpflichten oder auf den Aufwand des Auffindens von Daten in Akten abstellen (§ 34 Abs. 4 BDSG), sind restriktiv auszulegen. Einschränkungen sind zudem in besonderen Verarbeitungssituationen vorgesehen.[374] Auch im **bereichsspezifischen Recht** gibt es zahlreiche Anspruchsgrundlagen, die vor allem im Sicherheitsrecht wiederum anspruchsausschließenden oder -einschränkenden Grenzen unterliegen.[375] Sofern bestimmte Grenzen der gesetzlichen Anspruchsgrundlagen greifen, erkennt das Bundesverwaltungsgericht neben diesen einen Anspruch auf ermessensfehlerfreie Entscheidung an, den es unmittelbar aus dem Recht auf informationelle Selbstbestimmung herleitet.[376]

Lehnt die Verwaltung einen Antrag auf Auskunft ab, muss sie nach § 34 Abs. 2 BDSG die Gründe der Auskunftsverweigerung dokumentieren und die Ablehnung der Auskunftserteilung gegenüber der betroffenen Person **begründen**, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.[377] Im Vorfeld von Gerichtsverfahren soll die **Möglichkeit der Einschaltung des Datenschutzbeauftragten** auf Initiative des Betroffenen die Einschränkungen der Reichweite der Mitteilung kompensieren.[378] Im **Gerichtsverfahren** verlangt Art. 19 Abs. 4 GG, dass die Dokumente über die maßgeblichen Verwaltungsvorgänge dem Gericht zur Verfügung stehen, soweit sie für die Beurteilung der Rechtmäßigkeit der behördlichen Entscheidung und der gel- 102

[372] Vgl. auch *BVerwGE* 89, 15 (17 f.).

[373] Dazu *VG Gelsenkirchen*, Urt. v. 27.4.2020, 20 K 6392/18 – Einsicht in Prüfungsakte, Rn. 126 ff.

[374] Vgl. §§ 27 Abs. 2, 28 Abs. 2, 29 Abs. 1 S. 2 BDSG.

[375] Aus der Rechtsprechung vgl. *BVerwG*, Urt. v. 15.6.2016 – 6 A 7.14 –, https://www.bverwg.de/150616U6A7.14.0; Urt. v. 24.1.2018 – 6 A 8.16 –, https://www.bverwg.de/240118U6A8.16.0; OVG NW, Urt. v. 31.7.2019 – 16 A 1009/14, BeckRS 2019, 24608.

[376] S. *BVerwG*, Urt. v. 15.6.2016 – 6 A 7.14 –, https://www.bverwg.de/150616U6A7.14.0, Rn. 21 ff.; Urt. v. 24.1.2018 – 6 A 8.16 –, https://www.bverwg.de/240118U6A8.16.0, Rn. 29 ff.

[377] Ein rigoroser Ausschluss der Begründung, wie ihn Art. 23 Abs. 3 S. 1 BayVSG vorsieht, ist auch im Bereich der Nachrichtendienste verfassungswidrig. Anders: *BayVerfGH*, NVwZ-RR 1998, 273 (279); *BayVGH*, Urt. v. 9.4.2003, 24 B 00.1240 (juris); Urt. v. 29.4.2004, 24 B 00.1446 (juris).

[378] § 34 Abs. 3 BDSG.

tend gemachten Rechtsverletzung von Bedeutung sein können.[379] § 99 Abs. 2 VwGO sieht mittlerweile ein Zwischenverfahren vor, das in allen Fällen abgelehnter Informationsansprüche relevant werden kann.[380] Die Einführung von **In-Camera-Verfahren** wäre verfassungsrechtlich möglich.[381]

b) Einfluss- und Partizipationsrechte

103 **Einfluss- und Partizipationsformen** sollen den betroffenen Personen die Gelegenheit bieten, die Informationen, das Wissen oder das „Bild" zu beeinflussen, das die Verwaltung über sie gewinnt und das deren Entscheidungen und Verhalten ihnen gegenüber prägt. Sie richten sich zum einen auf die Daten, die der staatlichen Stelle im Verarbeitungsverlauf zur Verfügung stehen. Dabei können sie die vollständige Ausklammerung bestimmter Daten, aber auch die Nutzung der Daten zu einem bestimmten Zweck oder die Richtigkeit der Daten betreffen. Zum anderen richten sie sich auf die Informationen und übergreifender auf das Wissen, das aus Daten oder anderen Informationsgrundlagen über die Person erzeugt wird.[382] Sie tragen zur Legitimation der Verwaltung und zum Grundrechtsschutz bei. Die **gesonderten datenschutzrechtlichen Einflussrechte** sind ebenso wie die Informationsrechte **rechtsförmige Minimalpositionen,** die die Verwaltung um weitere sachgerechte Formen der Beteiligung ergänzen kann. Zusätzlich haben sie die Funktion strukturierender Aufmerksamkeitsregeln: Über die Partizipation betroffener Personen soll die Verwaltung die Vollständigkeit oder Aktualität der Informationsgrundlagen und damit zugleich die Sachgerechtigkeit der Entscheidungen absichern.

104 Einflussmöglichkeiten in den erforderlichen vielfältigen Formen werden bereits geschaffen, indem geschützte Personen vor dem Hintergrund des Art. 8 GRCh oder des Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG und/oder sonst einschlägiger Grundrechte die Beachtung insoweit in Betracht kommender Datenschutznormen verlangen und dann etwa **Unterlassungsansprüche** geltend machen können.[383] Darüber hinaus listet die DSGVO **bestimmte Einflussrechte** ausdrücklich auf: das Recht auf Berichtigung oder Vervollständigung, das Recht auf Löschung oder das Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit, das Widerspruchsrecht und das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden.[384] Hat der Verantwortliche die personenbezogenen Daten

---

[379] *BVerfGE* 101, 106 (122 ff.).

[380] Dazu *BVerwGE* 117, 8 (9 ff.). Vgl. auch zur Konstellation der Überprüfung der Unrichtigkeit gespeicherter Daten *BVerwG*, NJW 2007, 789 (790 ff.).

[381] Zum In-camera-Verfahren als Option *BVerfGE* 101, 106 (128 ff.); 115, 205 (234 ff.); und als verfassungsrechtliches Gebot Sondervotum *Reinhard Gaier*, *BVerfGE* 115, 205 (250 ff.).

[382] Deutlich in den Ausführungen zum Berichtigungsanspruch in *BVerwGE* 120, 188 (190): „Unrichtig [...] sind Daten, wenn die Information, welche die einzelnen Angaben über die persönlichen oder sachlichen Verhältnisse des Betroffenen vermitteln, nicht mit der Realität übereinstimmt. [...] Unrichtig in diesem Sinne können Daten auch dann sein, wenn die durch sie vermittelte Information unvollständig, lückenhaft und dadurch missverständlich ist."

[383] Vgl. dazu auch (dies vor dem Hintergrund der deutschen Schutznormtheorie) *BVerwGE* 120, 188 (189, 191). S. außerdem zur Herleitung eines subjektiv-rechtlichen Anspruchs aus der Pflicht des § 13 Abs. 1 BVerfSchG *OVG NW*, NVwZ 2005, S. 969 (969); *BVerwG*, NJW 2007, S. 789 (790), und aus der Pflicht des § 6 HambMG *BVerwG*, NJW 2006, 3367 (3367 f.).

[384] Art. 16 bis 22 DSGVO.

öffentlich gemacht und ist er zu deren Löschung verpflichtet, wird ihm noch eine spezielle Mitteilungspflicht auferlegt, die über die Mitteilungspflicht des Art. 19 DSGVO hinausgeht: Er muss unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel angemessene Maßnahmen treffen, um die (anderen) Verantwortlichen, die diese personenbezogenen Daten verarbeiten, über den Antrag der betroffenen Person zu informieren, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen. Hierin spiegelt sich ein **„Recht auf Vergessenwerden"**, dessen breite Diskussion in den DSGVO-Entwürfen einen ihrer Anlässe hatte, nur noch rudimentär wider. Was und wie unter den heutigen gesellschaftlichen Bedingungen erinnert und vergessen werden und inwieweit es „Rechte auf Vergessenwerden" geben soll, bleibt allerdings ein in zahlreichen Feldern zentrales und in komplexer Weise ausarbeitungsbedürftiges Thema.

Bei einem Blick auf die **Grenzen der Rechte** hat das Widerspruchsrecht bereits **105** Grenzen in Art. 21 Abs. 1 S. 2 DSGVO und § 36 BDSG schränkt dieses Recht – in im Detail kritikwürdiger Form[385] – gegenüber einer öffentlichen Stelle noch einmal ein, soweit ein zwingendes öffentliches Interesse an der Verarbeitung besteht, das die Interessen der betroffenen Person überwiegt, oder soweit eine Rechtsvorschrift zur Verarbeitung verpflichtet. Für die Ansprüche auf Löschung und Mitteilung sieht Art. 17 Abs. 3 DSGVO unter Rückgriff auf teilweise sehr vage und konkretisierungsbedürftige Rechtsbegriffe Ausnahmen vor. Für nicht automatisierte Datenverarbeitungen enthält § 35 BDSG weitere Einschränkungen.

c) Insbesondere: Rechte bei automatisierten Entscheidungen

Art. 22 Abs. 1 DSGVO gehört, obwohl er Vorläufer hat[386], zu den jüngeren **106** Normen in Reaktion auf die Digitalisierung, die individuelle **Rechtspositionen** und daraus resultierende **Rechtmäßigkeitsbedingungen** für **automatisierte Einzelfallentscheidungen** formulieren. Danach hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Als automatisierte Verarbeitung erfasst ist unter anderem ein Profiling, bei dem nach Maßgabe der etwas vagen Definition des Art. 4 Nr. 4 DSGVO (auch) personenbezogene Daten automatisiert verarbeitet und zur Bewertung bestimmter persönlicher Aspekte wie der Arbeitsleistung, der Interessen oder des Verhaltens verwendet werden.[387] Art. 22 Abs. 2 DSGVO sieht zum einen vertrags- und einwilligungsbezogene Ausnahmen vor, die ihrerseits an die Gewährleistung akzessorischer Einflussrechte der betroffenen Person geknüpft sind. Zum anderen lässt er Ausnahmen auf der Basis unionaler und mitgliedstaatlicher Rechtsvorschriften zu, sofern diese angemessene Maßnahmen zur Wahrung der Rechte, Freiheiten und berechtigten Interessen der betroffenen Person enthalten. Für Entscheidungen auf der Grundlage besonderer Kategorien personenbezogener Daten werden die Ausnahmen wiederum eingeschränkt. Sofern es eine automatisierte Entscheidungsfindung im Rahmen der Norm gibt, müssen betroffene

[385] Vgl. etwa *Herbst*, in: Kühling/Buchner (Fn. 107), § 36 BDSG, Rn. 2, 5 ff.
[386] Art. 15 DSRL, umgesetzt in § 6a BDSG a.F.
[387] Zum Profiling s.a. die N. in → Fn. 81 und Fn. 82.

Personen darüber informiert werden. Der Verantwortliche muss ihnen außerdem, damit eine faire und transparente Verarbeitung gewährleistet ist, zumindest in bestimmten Fällen aussagekräftige Informationen „über die involvierte Logik" und über Auswirkungen der Verarbeitung zur Verfügung stellen.[388] Mit zusätzlichen Tatbestandsmerkmalen sind von Art. 22 DSGVO erfasste Entscheidungsverfahren eines der Regelbeispiele für das Erfordernis, eine Datenschutzfolgenabschätzung durchzuführen, und Gegenstand einer ausdrücklichen Aufgabenzuweisung an den Europäischen Datenschutzausschuss, Leitlinien, Empfehlungen und bewährte Verfahren bereitzustellen.[389]

107 Die Normen sind **in erheblichem Umfang interpretations- und konkretisierungsbedürftig.** Ohne dass man ins Detail gehen müsste, wird erkennbar, dass Art. 22 Abs. 1 DSGVO über den traditionellen datenschutzrechtlichen Fokus – den Umgang mit personenbezogenen Informationen und Daten – hinausreicht.[390] Im Mittelpunkt steht die Verbindung zwischen Person und beeinträchtigender Entscheidung, welche auf einer automatisierten Verarbeitung nicht näher spezifizierter Daten beruht[391], die im Entscheidungsfindungsvorgang mit der Person verknüpft werden. Indem Menschen nicht ausschließlich maschinenproduzierten rechtsbeeinträchtigenden Entscheidungen ausgesetzt werden sollen, ohne dass auf das Entscheidungsergebnis Einfluss genommen werden kann, zielt die Regelung auf das **Vertrauen** in die Angemessenheit der Entscheidungsabläufe und -ergebnisse, mittelbar auch auf **die aus Sicht des Individuums notwendigen Bedingungen der Möglichkeit der Akzeptanz** solcher Entscheidungen. Ein weiterer Grund liegt in der Gewährleistung der **Entscheidungsqualität:** angesichts der mannigfaltig denkbaren Fehlerquellen, der Opazität komplexer und gegebenenfalls selbstständig lernender Algorithmen oder deren Diskriminierungspotenzials sollen automatisierte Entscheidungen durch Menschen in gewissem Umfang überprüf- und beeinflussbar sein.

108 Mit Blick auf die Schutzziele müssen **Anwendungsbereiche, Rechtsfolgen, Ausnahmetatbestände** und **Rechtspositionen** in zahlreichen Hinsichten geklärt werden. Eine Entscheidung auf der Grundlage einer ausschließlich automatisierten Verarbeitung liegt nicht vor, wenn Menschen in einer im Hinblick auf das Entscheidungsergebnis relevanten Weise in den Prozess eingebunden sind, aber wie gering oder stichprobenartig das Maß an Mitwirkung und Überprüfung im jeweiligen Feld sein darf, kann schwer zu beantworten sein.[392] Die in den Blick genommenen Entscheidungsfolgen erfassen nicht jede, sondern nur erhebliche und insofern konkretisierungsbedürftige Beeinträchtigungen. Näherer Ausarbeitungen bedarf es auch im Hinblick auf die Fragen, welche Maßnahmen und Schutzvorkehrungen im Falle von Ausnahmen getroffen werden müssen und welche Rechte der betroffenen Person in solchen Fällen an welcher Stelle zustehen. Sie hat Informationsrechte, aber bereits das Erfordernis, sie über die Existenz einer automatisierten Entscheidungsfindung zu informieren, hängt

[388] Art. 13 Abs. 2 lit. f; 14 Abs. 2 lit. g DSGVO.

[389] Art. 35 Abs. 3 lit. a, Art. 70 Abs. 1 S. 2 lit. f DSGVO.

[390] S. a. zu den Erfordernissen übergreifenderer Perspektiven → Rn. 8 ff., 17 f., 60 ff.

[391] Dabei braucht es sich nicht um personenbezogene Daten zu handeln. Rechtmäßigkeitsvoraussetzungen für deren Verarbeitung liefern andere Normen der DSGVO, vgl. EG 72 für das Profiling.

[392] Einen jedenfalls unter gegenwärtigen Bedingungen engen Anwendungsbereich bescheinigt der Norm *Martini*, Black Box (Fn. 67), S. 172 ff.

von Antworten auf die Fragen zum Anwendungsbereich des Art. 22 Abs. 1 DSGVO ab. Ein breitgefächerter Streit besteht darüber, von welcher Art, Qualität und Tiefe Erläuterungen sein müssen, damit der betroffenen Person aussagekräftige Informationen über die involvierte Logik und die Tragweite oder Auswirkungen der Verarbeitung zur Verfügung gestellt worden sind, wie man dies mit Geheimnisschutzerfordernissen abstimmt[393], inwieweit die verantwortliche Stelle dies angesichts des Einkaufs und der Komplexität eingesetzter Programme überhaupt leisten kann und ob man nicht zumindest auch spezialisierte professionelle Gremien braucht. Insgesamt kann Art. 22 DSGVO nur ein **Einstieg in die** erforderlichen und notwendigerweise übergreifenden **Debatten** sein.

6. Institutionelle Gewährleistungs- und Kontrollmechanismen

Die DSGVO legt einen Schwerpunkt auf **prozedurale Mechanismen der Normkonkretisierung, -umsetzung und -durchsetzung.**[394] Wesentliche Bedeutung haben hierbei die **Aufsichtsbehörden** und der **Europäische Datenschutzausschuss** mit ihren jeweiligen Kompetenzen und die insoweit institutionalisierten Verfahren der Zusammenarbeit und Abstimmung. Auch **behördliche und betriebliche Datenschutzbeauftragte** sind in begrenzter, die Eigenständigkeit ihrer Rolle wahrende Weise in Zusammenarbeits- und Abstimmungsmechanismen eingebunden. Der Bedeutung der Aufsichtsbehörden und des Europäischen Datenschutzausschusses entsprechen die ausführlich geregelten Aufgaben und Befugnisse, die weit über eine Beratung[395] und Kontrolle hinaus etwa auch die systematische Beobachtung und Analyse relevanter Entwicklungen, den systematischen Wissensaustausch, Öffentlichkeitsarbeit sowie die Standardsetzung oder eine Beteiligung daran einschließen. Zu den institutionellen Gewährleistungsmechanismen könnten künftig auch – auf einer anderen Ebene und mit eigenständigen Aufgaben – **Datenmittler, Datentreuhänder** und **datenaltruistische Organisationen** gehören.[396] 109

a) Aufsichtsbehörden und deren Zusammenarbeit

Art. 51 DSGVO gibt jedem Mitgliedstaat die **Einrichtung unabhängiger Behörden** auf, die für die Überwachung der Anwendung der DSGVO zuständig sind, einen Beitrag zu deren einheitlicher Anwendung in der gesamten Union leisten sollen und zu diesem Zweck untereinander sowie mit der Kommission zusammenarbeiten. In den Folgebestimmungen finden sich recht detaillierte Anforderungen an die Institutionalisierung, u.a. im Hinblick auf die „völlige Unabhängigkeit" der Aufsichtsbehörden[397] oder zu den Verschwiegenheits- 110

[393] S. für Betriebs- und Geschäftsgeheimnisse §§ 1 ff. GeschGehG; vgl. auch *BGH* Urt. v. 28.1.2014, VI ZR 156/13, www.juris.bundesgerichtshof.de, Rn. 27 ff. – Scoreformel der Schufa. Im staatlichen Sektor gibt es es eigenständige Geheimhaltungsgründe; Betriebs- und Geschäftsgeheimnisse können aber unter mehreren Aspekten ebenfalls relevant werden, sofern Programme von privaten Unternehmen eingekauft werden.

[394] Zum reflexiven Selbstverständnis → Rn. 43.

[395] S. auch zu den Beratungsfunktionen des Europäischen Datenschutzbeauftragten *EuGH*, C-318/04, Slg. 2005, I-2467 (Rn. 18).

[396] Dazu → Rn. 3.

[397] Zum Merkmal der Unabhängigkeit nach Art. 28 Abs. 1 RL 95/46/EG s. *EuGH*, C-518/07, Slg. 2010, I-01885 (Rn. 31 ff.); und Urt. v. 16.10.2012, C-614/10, ZD 2012, 563. Ausf. Analyse bei *Malte Kröger*, Unabhängigkeitsregime im europäischen Verwaltungsverbund. Eine europa- und verfas-

pflichten. Nach Maßgabe dieser Vorgaben obliegt die Errichtung der Aufsichtsbehörden den Mitgliedstaaten selbst, die in diesem Rahmen etwaige weitere Vorgaben nationalen (Verfassungs-)Rechts beachten müssen. Das BDSG sowie die jeweiligen Landesdatenschutzgesetze sehen Bundes- bzw. Landesdatenschutzbeauftragte vor[398], die regelmäßig zugleich Beauftragte für die Informationsfreiheit sind. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wird auf Vorschlag der Bundesregierung vom Deutschen Bundestag für fünf Jahre gewählt (§ 11 BDSG).

111 Der Katalog der **Aufgaben** in Art. 57 Abs. 1 DSGVO nennt an erster Stelle, dass die Aufsichtsbehörde die Anwendung der DSGVO überwachen und durchsetzen muss. Weit über den bisherigen Aufgabenbereich der Datenschutzaufsichtsbehörden hinaus[399] werden dann noch zahlreiche andere Aufgaben aufgezählt, die sich u.a. auf Aufklärung, Beratung, Unterstützung, systematische Beobachtung von Entwicklungen, Koordination und Standardisierung richten. Geht man davon aus, dass die Kontrollmaßstäbe, die die Datenschutzbestimmungen für die Aufgabe derer Überwachung und Durchsetzung liefern, nicht selten noch konkretisierungsbedürftig sind, ist eine solch weite Aufgabenbeschreibung durchaus stimmig. Sie macht zugleich deutlich, welch zentrale Rolle die Aufsichtsbehörden spielen sollen. Der Aufgabenbereich der Datenschutzbeauftragten hat sich dementsprechend, wie § 14 BDSG exemplarisch zeigt[400], signifikant erweitert. Der weitgehend abschließende, also regelmäßig keinen Regelungsspielraum belassende, abgestufte Maßnahmenkatalog[401] aufsichtsbehördlicher **Befugnisse** in Art. 58 DSGVO ist unterteilt in Untersuchungsbefugnisse[402], Abhilfebefugnisse[403] sowie Genehmigungsbefugnisse und beratende Befugnisse[404]. § 16 BDSG weist der oder dem Bundesbeauftragten für den Datenschutz diese Befugnisse im Wege der Verweisung zu. Zugleich sieht er im Falle festgestellter Datenschutzverstöße- oder -mängel eine Mitteilung an die zuständige Rechts- oder Fachaufsichtsbehörde und vor Ausübung der meisten Befugnisse eine Abstimmung mit dieser Behörde vor, die divergierende Entscheidungen vermeiden oder zumindest reduzieren soll.[405]

---

sungsrechtliche Untersuchung unionsrechtlicher Organisationsregelungen für Mitgliedstaaten anhand von Regulierungsagenturen, Datenschutzbehörden sowie statistischen Ämtern, 2020.

[398] Vgl. §§ 8 ff. BDSG.

[399] Vgl. auch *Franziska Boehm*, in: Kühling/Buchner (Fn. 107), Art. 57 Rn. 2 und 8.

[400] § 14 BDSG wiederholt teilweise Aufgabenbeschreibungen, die sich bereits in Art. 57 Abs. 1 DSGVO finden, dies vor dem Hintergrund, dass er zugleich Art. 46 der Datenschutzrichtlinie für Polizei und Strafjustiz umsetzt.

[401] *BVerwG*, Urt. v. 27.3.2019, 6 C 2.18, www.bverwg.de/270319U6C2.18.0, Rn. 38 f.

[402] Z.B.: Anweisungen an den Verantwortlichen zur Bereitstellung von Informationen, Zugang zu allen personenbezogenen Daten und Informationen, die für die Aufgabenerfüllung erforderlich sind, Zugang zu den Räumlichkeiten und Datenverarbeitungsanlagen.

[403] Z.B.: Anweisungen an den Verantwortlichen, Verarbeitungsvorgänge an die DSGVO-Vorgaben anzupassen oder Anträgen der betroffenen Person zu entsprechen, Beschränkung der Verarbeitung personenbezogener Daten, Verhängung einer Geldbuße. Vgl. auch *BVerwG*, Urt. v. 27.3.2019, 6 C 2.18, www.bverwg.de/270319U6C2.18.0, Rn. 42: „Diese Befugnis soll als Auffangtatbestand grundsätzlich jeden Verstoß gegen die Datenschutz-Grundverordnung, d.h. jede unionsrechtswidrige Verarbeitung von personenbezogenen Daten erfassen".

[404] Z.B.: Erteilung von Zertifizierungen, Genehmigung von Vertragsklauseln, Beratung des Verantwortlichen, Erarbeitung von Stellungnahmen.

[405] Für Rechtsstreitigkeiten ist der Verwaltungsrechtsweg gegeben, § 20 BDSG.

Umfangreiche Regelungen zur **Informations- und Amtshilfe** (Art. 61 DSGVO) sollen die Zusammenarbeit zwischen den Aufsichtsbehörden der Mitgliedstaaten fördern.[406] Das Konzept der federführenden Aufsichtsbehörde in Fällen grenzüberschreitender Datenverarbeitung und die insoweit näher geregelten Zusammenarbeitsverfahren (Art. 56, 60 DSGVO[407]) greifen nicht, wenn die Verarbeitung durch Behörden oder private Stellen auf der Grundlage von Art. 6 Abs. 1c oder e DSGVO erfolgt. Nach Art. 55 Abs. 2 DSGVO ist hier die Aufsichtsbehörde des jeweils betroffenen Mitgliedstaats allein zuständig. Art. 61 DSGVO zählt zu den Normen, die – wie dann vor allem auch die Regelungen zum Europäischen Datenschutzausschuss – einen **Europäischen Informations- und Verwaltungsverbund** hinsichtlich der auf den Datenschutz ausgerichteten Institutionen und deren Verfahren herstellen.[408] Art. 61 Abs. 1 DSGVO enthält hierzu eine etwas übergreifendere Regelung; im Übrigen steht die einzelfallbezogene Amtshilfe im Vordergrund der Norm. Der Austausch personenbezogener Daten kann nicht auf diese Amtshilferegelung gestützt werden, sondern bedarf gesonderter Befugnisse. 112

b) Europäischer Datenschutzausschuss

Der **Europäische Datenschutzausschuss** ist eine Einrichtung der Union mit eigener Rechtspersönlichkeit, die in ihrer Aufgaben- und Befugniswahrnehmung unabhängig ist.[409] Der Ausschuss setzt sich aus den Leitern jeweils einer Aufsichtsbehörde jedes Mitgliedstaats[410] und dem für die Organe und Institutionen der EU zuständigen Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern zusammen; die Kommission ist berechtigt, ohne Stimmrecht an den Tätigkeiten und Sitzungen des Ausschusses teilzunehmen.[411] Im Vergleich zur Datenschutzgruppe nach Art. 29 DSRL werden dem Ausschuss erheblich erweiterte Kompetenzen zugewiesen; er ist die „entscheidende Einrichtung zur Sicherstellung einer einheitlichen Anwendung des neuen Rechtsrahmens"[412]. Neben Stellungnahmen oder verbindlichen Beschlüssen im Kohärenzverfahren[413] berät der Ausschuss die Kommission in allen Fragen des Datenschutzes. Hinsichtlich zahlreicher konkretisierungsbedürftiger Punkte der DSGVO stellt er Leitlinien, Empfehlungen oder bewährte Verfahren (best practices) bereit, die als „soft law" Wirkung entfalten. Nicht zuletzt fördert er die Zusammenarbeit zwischen den mitgliedstaatlichen Aufsichtsbehörden und den 113

[406] Kritisch im Vorfeld *Johannes Caspar*, Das aufsichtsbehördliche Verfahren nach der EU-Datenschutz-Grundverordnung, Defizite und Alternativregelungen, ZD 2012, S. 555 (556 ff.).

[407] Dazu die knappen Anm. in *EuGH*, Urt. v. 24.9.2019, C-507/17, abrufbar unter http://curia.europa.eu, Rn. 68 f. Zu den Zuständigkeiten einer mitgliedstaatlichen und der federführenden Aufsichtsbehörde s. weiter *EuGH*, Urt. v. 15.6.2021, C-645/19, http://curia.europa.eu, Rn. 43 ff.

[408] *Alexander Dix*, in: Kühling/Buchner (Fn. 107), Art. 61 Rn. 4.

[409] Art. 68 Abs. 1, 69 Abs. 1 DSGVO Ausf. zu den Fragen einer verwaltungsorganisationsrechtlichen Einordnung und zu Legitimationsfragen *Bettina Schöndorf-Haubold*, in: Sydow (Fn. 314), Art. 68 Rn. 2 ff., Art. 69 Rn. 11 ff.

[410] Mitgliedstaaten mit mehreren Aufsichtsbehörden bestimmen eine Behörde als Vertreterin im Ausschuss und führen ein Verfahren ein, mit dem sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren einhalten (Art. 68 Abs. 4, Art. 51 Abs. 3 DSGVO).

[411] Art. 68 Abs. 3 und 5 DSGVO.

[412] *Dix*, in: Kühling/Buchner (Fn. 107), Art. 70 Rn. 1.

[413] Art. 64 Abs. 8 i. V. m. Art. 65 Abs. 1 DSGVO.

Wissensaustausch mit Datenschutzaufsichtsbehörden in aller Welt.[414] Wechselwirkungen zwischen Praxisproblemen und -anforderungen sowie Kontroll- und Beratungsleistungen der Datenschutzinstitutionen können zu einem „lernenden" Datenschutzrecht beitragen.

Leitentscheidungen

EuGH, Urt. v. 13.5.2014 – C-131/12, http://curia.europa.eu – Google Spain.
EuGH, Urt. v. 5.6.2018 – C-210/16, http://curia.europa.eu – Fanpage.
EuGH, Urt. v. 24.9.2019 – C-136/17, http://curia.europa.eu – GC u. a.
EuGH, Urt. v. 16.7.2020 – C-311/18, http://curia.europa.eu – Schrems II.
EuGH, Urt. v. 6.10.2020, C-511, 512 u. 520/18, http://curia.europa.eu – Quadrature du Net u. a.
EuGH, Urt. v. 6.10.2020, C-623/17, http://curia.europa.eu – Privacy International.
BVerfGE 65, 1 – Volkszählung.
BVerfGE 120, 351 – Auskunftsanspruch.
BVerfGE 141, 220 – BKA-Gesetz.
BVerfG, Beschl. v. 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, www.bverfg.de.
BVerfG, Beschl. v. 6.11.2019, 1 BvR 276/17 – Recht auf Vergessen II, www.bverfg.de.
BVerfG, Urt. v. 19.5.2020, 1 BvR 2835/17 – Auslandsüberwachungsbefugnisse des BND, www.bverfg.de.
BVerfG, Beschl. v. 27.5.2020 – 1 BvR 1873/13 u. 2618/13 – Bestandsdatenauskunft II, www.bverfg.de.
BVerfG, Beschl. v. 10.11.2020 – 1 BvR 3214/15 – Antiterrordatei II, www.bverfg.de.
BVerwG, Urt. v. 15.6.2016, 6 A 7.14, https://www.bverwg.de/150616U6A7.14.0 – Auskunftsanspruch gegenüber dem BND.
BVerwG, Urt. v. 27.3.2019, 6 C 2.18, www.bverwg.de/270319U6C2.18.0 – Videoüberwachung durch Private.

Ausgewählte Literatur

Albers, Marion, Informationelle Selbstbestimmung, Baden-Baden 2005.
– */Ingo Sarlet* (eds.), Personality and Data Protection Rights on the Internet, 2022.
Colonna, Liane, Legal Implications of Data Mining, Stockholm, 2016.
Fuster González, Gloria, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Cham u. a. 2014.
Grafenstein, Maximilian von, The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation, Baden-Baden 2018.
Gratton, Éloise, Understanding Personal Information: Managing Privacy Risks, LexisNexis, 2013.
Hornung, Gerrit, Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden 2005.
Lynskey, Orla, The foundations of EU data protection law, Oxford 2015.
Marsch, Nicolaus, Das europäische Datenschutzgrundrecht, Tübingen 2018.
Masing, Johannes, Einheit und Vielfalt des Europäischen Grundrechtsschutzes, JZ 2015, S. 477–487.
Munkler, Laura (Hrsg.), Dimensionen des Wissens im Recht, Tübingen 2019.
Nissenbaum, Helen, Privacy in Context. Technology, Policy, and the Integrity of Social Life, Stanford 2010.
Oostveen, Manon, Protecting Individuals Against the Negative Impact of Big Data, 2018.
Ruffert, Jörn, Konturen des europäischen Datenschutzgrundrechts, AöR, Bd. 142 (2017), S. 528–565.
Schimke, Anna, Das Medienprivileg als Koordinationsmechanismus. Zum Verhältnis von Datenschutz- und Äußerungsrecht im Internet, in: Albers, Marion/Katsivelas, Ioannis (Hrsg.), Recht & Netz, Baden-Baden 2018, S. 155–186.
Trute, Hans-Heinrich, Wissen – Einleitende Bemerkungen, in: Hans C. Röhl (Hrsg.), Wissen – Zur kognitiven Dimension des Rechts, DV, Beiheft 9, 2010, S. 11–38.
Tzanou, Maria, The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance, Oxford 2017.
Veit, Raoul-Darius, Einheit und Vielfalt im europäischen Datenschutzrecht, Dissertation Hamburg, Manuskript 2021 (i. E.).

[414] Näher insgesamt Art. 70 Abs. 1 DSGVO.