Kompendien

für Studium, Praxis und Fortbildung

Eßer | Franck

Datenschutzrecht

Fälle und Lösungen

Nomos

Kompendien

für Studium, Praxis und Fortbildung

Dr. Martin Eßer, Maître en Droit
Prof. Dr. Lorenz Franck

Datenschutzrecht

Fälle und Lösungen

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8487-7678-8 (Print)

ISBN 978-3-7489-1053-4 (ePDF)

1. Auflage 2022

Inhaltsverzeichnis

Vorwort

Das vorliegende Studienbuch richtet sich gleichermaßen an Studierende, Rechtsanwendende und angehende Datenschutzbeauftragte oder -verantwortliche in Unternehmen und Behörden, die vor der Herausforderung stehen, das abstrakte Datenschutzrecht auf praktische Fälle anzuwenden. Bei der Auswahl der Fälle haben wir einen Fokus auf das Systemverständnis des Datenschutzes gelegt und unterschiedliche Aufgaben- und Klausurtypen abgebildet. Die ausgewählten Fragestellungen sind der Praxis entnommen und den Fällen wurde eine Einführung u.a. zur Methodik der Fallbearbeitung und zu den Textquellen datenschutzrechtlicher Auseinandersetzung vorangestellt.

Hinweise und Kritik nehmen wir gerne entgegen unter esser.franck@datenschutzkommentar.eu

Bonn und Sankt Augustin, im Juli 2021

Dr. Martin Eßer, Maître en droit (Paris IX)
Prof. Dr. Lorenz Franck

Einführung – Das juristische Gutachten im Datenschutz

Oft ist es nur ein Satz
Der alle anderen nach sich zieht
Ein Beginn und ein Ende
Das Ende der Stille; So wie dieser hier […]
Sie schmücken aus; Sie engen ein
Sie biegen ab; Sie verweisen auf einander
Sie verwirren und ergänzen sich
Wörter Sinnen über Wörter

(Kid Kopphausen, Nur ein Satz)

Datenschutzrechtliche Falllösungen begegnen nicht nur Studierenden der Rechtswissenschaften im entsprechenden Schwerpunktbereich[1] als Prüfungsform. In den juristischen Staatsexamina sind sie nicht unmittelbar vorgesehen, gleichwohl nicht ausgeschlossen.[2] Der Schutz personenbezogener Daten kann zudem als Nebenfach in technischen Studiengängen, als Vertiefungsveranstaltung an verwaltungsinternen Hochschulen oder bei Qualifizierungsleistungen privater Schulungsanbieter vorkommen. **1**

Die Rechtsanwendung im Datenschutz bewegt sich dabei an der Schnittstelle von Recht und Technik und zugleich im Grenzdickicht vielfältiger Rechtsquellen, aufsichtsbehördlicher Zuständigkeiten sowie einer blühenden Kommentarlandschaft. Im Rahmen dieser Einführung sollen daher die Besonderheiten des Datenschutzrechts gegenüber anderen Rechtsmaterien beleuchtet und zugleich die Bedeutung und Grundregeln des juristischen Gutachtenstils aufgefrischt werden. **2**

I. Datenschutzrecht

1. Aufgabe und Grundrechtsrelevanz des Datenschutzrechts

Das Datenschutzrecht schützt – vereinfacht ausgedrückt – natürliche Personen vor unrechtmäßiger, unrichtiger und missbräuchlicher Verarbeitung ihrer personenbezogenen Daten. Aus der grundlegenden Beschränkung auf natürliche Personen ergibt sich die **Menschzentriertheit** des Datenschutzrechts (klarstellend Erwägungsgrund 14 Satz 1 DS-GVO). Juristische Personen werden nur dann in den Schutzbereich des Datenschutzrechts einbezogen, wenn sich dies unmittelbar kraft gesetzlichen Verweises ergibt, etwa im Telekommunikations-,[3] Steuer-[4] oder Sozialdatenschutz.[5] **3**

1 Schwerpunktbereichsklausur zur Anfechtungsklage gegenüber der Datenschutzaufsicht bei Golla, Jura 2020, 472 ff.
2 Vgl. etwa § 11 Abs. 1 Satz 2 JAG NRW. Eine Examensklausur zum Recht auf Vergessenwerden findet sich bei Ludyga/Scholer, JA 2019, 255 ff.
3 Siehe § 91 Abs. 1 Satz 2 TKG.
4 Siehe § 2a Abs. 5 Nr. 2 AO.
5 Siehe § 35 Abs. 4 SGB I.

4 Vergleicht man die Formulierungen von Art. 1 Abs. 2 DS-GVO („Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen […]“) und etwa § 1 Abs. 1 BDSG a.F. („Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“), wird die **freiheitsermöglichende Dimension** des Datenschutzes schon im Gesetzeswortlaut deutlich.

5 Ein frühes Zeugnis[6] dieses Gedankens findet sich bereits 1890 in der Harvard Law Review.[7] Warren und Brandeis postulierten das Recht auf Privatheit als Abwehrrecht, namentlich als das Recht, in Ruhe gelassen zu werden (**right to be let alone**): *„Dass ein solcher Schutz zu wünschen – oder besser nötig – ist, kann, so glauben wir, nicht bezweifelt werden. Die Presse überschreitet in allen Richtungen die offensichtlichen Grenzen von Anstand und Benehmen. Klatsch ist nicht mehr der Quell für Müßiggänger oder Böswillige; Klatsch ist vielmehr zur Handelssache geworden, der mit Eifer und Unverfrorenheit nachgegangen wird. Um Lüsternheit zu befriedigen, werden Details über sexuelle Beziehungen in den Kolumnen der Tageszeitungen verbreitet. Um träge Menschen zu unterhalten, werden Kolumnen über Kolumnen mit müßigem Klatsch gefüllt, der nur über das Eindringen in das häusliche Umfeld erlangt werden kann.“*[8]

6 In aller Deutlichkeit stellte das BVerfG im richtungsweisenden **Volkszählungsurteil** fast einhundert Jahre später (1983) ebenfalls fest: *„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“*[9] Das Grundrecht auf informationelle Selbstbestimmung wurde hier aus einer Zusammenschau von Art. 1 Abs. 1 GG (Menschenwürde) und Art. 2 Abs. 1 GG (Persönlichkeitsentfaltung) konstruiert.

7 Der Schutz personenbezogener Daten im Sinne der Vertraulichkeit gegenüber Dritten sowie der Transparenz gegenüber der betroffenen Person selbst ist insoweit der Schlüssel für die effektive Wahrnehmung weiterer verbriefter Grundrechte, angefangen bei der Versammlungs- und Vereinigungsfreiheit, über die Unterrichtung aus frei verfügbaren Quellen, die Religionsausübung bis hin zur sexuellen Entfaltung. Dabei stehen nicht nur die individuellen Entfaltungschancen des Einzelnen im Fokus, sondern auch das Gemeinwohl insgesamt, da die Selbstbestimmung als elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens verstanden wird.[10]

---

6 Zur Rechtsgeschichte des Datenschutzes von Lewinski, Zufall und Notwendigkeit bei der Geschichte des Datenschutzrechts, in: Pohle/Knaut, Fundationes I, 2014, S. 9 ff.; von Lewinski, Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive, in: Schmidt/Weichert, Datenschutz, 2012, S. 23 ff.; von Lewinski, Die Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt et al., Freiheit -Sicherheit -Öffentlichkeit, 2009, S. 196 ff.; von Lewinski, DuD 2003, 61 ff.; Kilian, CR 2021, 9 ff.

7 Warren/Brandeis, The Right to Privacy, Harvard Law Review Bd. 4 Nr. 5 (1890), S. 193 ff. (online unter https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf).

8 Übersetzung Hansen/Weichert, DuD 2012, 755 (756).

9 BVerfGE 65, 1 (43).

10 BVerfGE 65, 1 43.

Inzwischen ist der Datenschutz fester Bestandteil des Grundrechtekanons und wird außerdem flankiert durch das Brief-, Post- und Fernmeldegeheimnis gem. Art. 10 GG, das Recht auf Unverletzlichkeit der Wohnung gem. Art. 13 GG (im Falle des Lauschangriffs[11]) und das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme[12] (sog. Computergrundrecht) gem. Artt. 1 Abs. 1, 2 Abs. 1 GG. **8**

Auch einige Landesverfassungen enthalten einschlägige Datenschutz-Gewährleistungen: NRW war das erste Bundesland, welches den Schutz personenbezogener Daten bereits 1978 ausdrücklich zum Grundrecht erklärte.[13] Die Verfassungen von Berlin,[14] Brandenburg,[15] Bremen,[16] Mecklenburg-Vorpommern,[17] Rheinland-Pfalz,[18] Saarland,[19] Sachsen,[20] Sachsen-Anhalt,[21] Schleswig-Holstein[22] und Thüringen[23] verfügen über vergleichbare Regelungen. **9**

Auf europäischer Ebene ist der Datenschutz in den Artt. 7 und 8 der Europäischen Grundrechte-Charta (GRCh) sowie Art. 8 der Europäischen Menschenrechtekonvention (MRK) verankert. Er ist zudem Gegenstand internationaler Übereinkommen wie der Konvention 108 des Europarates (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten) oder Art. 17 des Internationalen Paktes über bürgerliche und politische Freiheiten (IPbpR). **10**

2. Schutzgegenstand des Datenschutzrechts

Nach dem oben Gesagten dürfte klar sein, dass der Schutzgegenstand des Datenschutzrechts nicht das Datum an sich ist, wie etwa in anderen Materien des Informationssicherheitsrechts.[24] Stattdessen geht es stets um den Menschen, also die lebende natürliche Person. Sie ist die **betroffene Person** im Sinne des Art. 4 Nr. 1 DS-GVO. **11**

„Identifiziert" ist diese Person, wenn sich ihre Identität unmittelbar aus den jeweiligen Daten ergibt. „Identifizierbar" ist sie, wenn sich ihre Identität aus den Daten zumindest ableiten lässt, ggf. unter Zuhilfenahme von verfügbarem Zusatzwissen. **12**

Werden die Daten „anonymisiert" (vgl. Erwägungsgrund 26 Satz 5 DS-GVO), werden sie derart verändert, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer identifizierten oder bestimmbaren natürlichen Person zugeordnet werden können. Fehlt der Personenbezug, unterliegen die Daten keinen datenschutzrechtlichen Einschränkungen. **13**

---

11 BVerfGE 109, 279.
12 BVerfGE 120, 274.
13 Siehe Art. 4 Abs. 2 LVerf NRW.
14 Siehe Art. 33 LVerf BN.
15 Siehe Art. 11 LVerf BB.
16 Siehe Art. 12 LVerf BR.
17 Siehe Art. 6 LVerf M-V.
18 Siehe Art. 4a LVerf RP.
19 Siehe Art. 2 LVerf SL.
20 Siehe Art. 33 LVerf SN.
21 Siehe Art. 6 LVerf ST.
22 Siehe Art. 15 LVerf SH.
23 Siehe Art. 6 LVerf TH.
24 Überblick bei Franck in: Wollinger/Schulze, Handbuch Cybersecurity für die öffentliche Verwaltung, 2020, S. 261 ff.

14 Mit der Anonymisierung nicht zu verwechseln ist die „Pseudonymisierung" im Sinne von Art. 4 Nr. 5 DS-GVO. Hierbei handelt es sich lediglich um das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein anderes Kennzeichen. Da weiterhin eine Ersetzungs- bzw. „Klarliste" existiert, handelt es sich bei Pseudonymen weiterhin um personenbezogene Daten.

3. Unionsrechtsbezug

15 Rechtsanwender sind seit der Europäischen Datenschutzreform mit drei (sich gegenseitig ausschließenden) Rechtssphären konfrontiert:[25]

- Die DS-GVO-Sphäre erfasst flächendeckend die allgemeine Datenverarbeitung von Privaten, Wirtschaft und Verwaltung.
- Die JI-RL-Sphäre wird betreten, wenn Behörden zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten bzw. der Strafvollstreckung tätig werden.
- Die unionsrechtsfreie Sphäre erfasst diejenigen Tätigkeiten, die gem. Art. 2 Abs. 2 litt. a bis d DS-GVO nicht in den Anwendungsbereich des Unionsrechts fallen bzw. diejenigen Verarbeitungen die nicht hinreichend automatisiert sind.[26] Hier obliegt es allein dem nationalen Gesetzgeber, ein adäquates Datenschutzniveau zu schaffen.

Der unmittelbare Unionsrechtsbezug des Datenschutzes in den ersten beiden Sphären hat für die Rechtsanwendung mehrere Besonderheiten zur Folge.

16 Zunächst gilt der sog. **Anwendungsvorrang** des Unionsrechts. Nationale Vorschriften, die dem Unionsrecht widersprechen, sind von vornherein nicht anwendbar. Der Anwendungsvorrang gehört zu den Grundpfeilern des Gemeinschaftsrechts. Der EuGH stellte fest, dass „es den Staaten unmöglich ist, gegen eine von ihnen auf der Grundlage der Gegenseitigkeit angenommene Rechtsordnung nachträglich einseitige Maßnahmen ins Feld zu führen".[27] Der Vertrag von Lissabon hat inzwischen einen entsprechenden Verweis in den Anhang aufgenommen.[28] Jedes Gericht, jede Behörde und jeder Rechtsanwender muss daher genau prüfen, ob eine einschlägige mitgliedsstaatliche Vorschrift mit dem Gemeinschaftsrecht vereinbar ist.[29]

17 Sofern nationales Recht weiterhin anwendbar bleibt, ist es dennoch stets im Lichte des Unionsrechts auszulegen Aus Art. 4 Abs. 3 EUV ergibt sich das sog. **Effektivitätsgebot** (auch: „effet utile"). Es sorgt dafür, dass das Unionsrecht die höchstmögliche praktische Wirksamkeit entfalten kann.[30]

---

25 Einteilung nach Reimer, Verwaltungsdatenschutzrecht, 2019, Rn. 5 ff.

26 Für den öffentlichen Bereich verhält sich der Bundesgesetzgeber agnostisch, was den Automatisierungsgrad angeht, vgl. § 1 Abs. 1 Satz 1 in Verbindung mit Abs. 8 BDSG.

27 EuGH, Urt. v. 15.7.1964, Az. 6/64, Slg. 1964, 1251 („Costa/E.N.E.L."). Vgl. zuvor EuGH, Urt. v. 5.2.1963, Az. 26/62 („van Gend & Loos"), Slg. 1963, 1. Grundlegend zum Anwendungsvorrang Calliess/Ruffert/*Ruffert*, EUV/AEUV, 5. Aufl. 2016, Art. 1 Rn. 16 ff. sowie Beljin, EuR 2002, 351 (353 ff.) Zum Anwendungsvorrang der DS-GVO vor dem nationalen Datenschutzrecht Sydow/*Sydow*, DS-GVO, 2. Aufl. 2018, Einleitung Rn. 36 ff.

28 Vertrag von Lissabon, Anhang, ABl.EU 2008, Nr. C 115, S. 344.

29 Vgl. EuGH, Urt. v. 9.3.1978 („Simmenthal II"), Az. 106/77, Slg. 1978, 629 zur Nichtanwendung durch nationale Gerichte; EuGH, Urt. v. 22.6.1989, Az. C-103/88, Slg. 1989, 1839 („Constanzo") zur Nichtanwendung durch Kommunalbehörden; EuGH, Urt. v. 9.9.2003, Az. C-198/01, Slg. 2003, I-8055 („CIF") zur Nichtanwendung durch nationale Wettbewerbsbehörden. Kritisch zur Nichtanwendung durch die Exekutive Greve, NVwZ 2017, 737 (743 f.).

30 Überblick bei Schill/Krenn in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 71. EL 2020, Art. 4 EUV Rn. 93 ff.; Voßkuhle/Schemmel JuS 2019, 347 (348 ff.).

Bei Unklarheiten hinsichtlich Auslegung und Gültigkeit des Unionsrechts können (und müssen) nationale Gerichte im Wege des **Vorabentscheidungsverfahrens** gem. Art. 267 AEUV den EuGH anrufen.[31] **18**

4. Grundregeln und Schutzziele des Datenschutzrechts

Die Grundsätze der Verarbeitung sind in Art. 5 DS-GVO niedergelegt und sollen hier nur schlaglichtartig dargestellt werden. Der vielleicht wichtigste Aspekt liegt in der Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 lit. a Var. 1 DS-GVO). Aus der Zusammenschau mit Art. 6 Abs. 1 DS-GVO ergibt sich, dass prinzipiell jede Datenverarbeitung verboten ist, es sei denn, es findet sich einen einschlägiger Erlaubnistatbestand (sog. „Verbot mit Erlaubnisvorbehalt").[32] **19**

Die Betroffenenperspektive rückt mit dem Grundsatz der Transparenz in den Vordergrund (Art. 5 Abs. 1 lit. a Var. 3 DS-GVO). Betroffene Personen verfügen u.a. über weitreichende Interventionsrechte.[33] Diese können jedoch nur sinnvoll wahrgenommen werden, wenn sie (wie ehedem nach Maßgabe des Volkszählungsurteils) wissen *„wer was wann und bei welcher Gelegenheit über sie weiß".* **20**

Zweckbindung, Datenminimierung und Speicherbegrenzung (Art. 5 Abs. 1 litt. b, c und e DS-GVO) haben ähnliche Stoßrichtungen. Der Verantwortliche muss sich im Vorhinein überlegen, welche Daten für ein bestimmtes Vorhaben erforderlich sind. Daten, die nicht (oder nicht mehr) benötigt werden, müssen gelöscht werden. Nur unter erhöhtem Begründungsaufwand können Daten einer Zweckänderung unterzogen werden.[34] **21**

Mit Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) sind zwei primäre Schutzziele der IT-Sicherheit angesprochen. Integrität bedeutet, dass Daten nicht widerrechtlich verändert oder zerstört werden. Vertraulichkeit bedeutet, dass die Daten niemand Unbefugtem zur Kenntnis gelangen. **22**

II. Rechtsquellen datenschutzrechtlicher Auseinandersetzung

1. Vorschriften

„Ein Blick ins Gesetz erleichtert die Rechtsfindung." Diese häufig ironisch gebrauchte Juristenweisheit gerät beim Datenschutzrecht schnell an ihre Machbarkeitsgrenzen. Neben der DS-GVO als der zentralen Säule des Datenschutzrechts findet sich eine bunte Vielfalt an konkretisierenden, in Einzelgesetzen verstreuten Vorschriften. **23**

a) Europäische Datenschutz-Grundverordnung (DS-GVO)

Die DS-GVO (= VO 2016/679/EU) ersetzt gem. Art. 288 Abs. 2 AEUV unmittelbar sämtliche bisherigen Regelungen der EU-Mitgliedsstaaten und belässt den nationalen Gesetzgebern nur enge Regelungsspielräume (sog. „Öffnungsklauseln). Sie gilt **24**

31 Näher hierzu Mächtle, JuS 2015, 314.
32 Zum Verbot mit Erlaubnisvorbehalt in der juristischen Fallprüfung Claus/Reif, RDV 2019, 238 (239).
33 Fünf Säulen der Betroffenenrechte bei Franck in: Gola, DS-GVO, 2. Aufl. 2018, Rn. 5; Franck, RDV 2016, 111 ff.
34 Zur Zweckänderung in der juristischen Fallprüfung Claus/Reif, RDV 2019, 238 (240).

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 (Art. 2 Abs. 1 DS-GVO). Die DS-GVO muss dabei nicht nur innerhalb der EU beachtet werden, sondern auch dann, wenn Unternehmen mit Sitz außerhalb der EU hier Waren und Dienstleistungen anbieten (sog. „Marktortprinzip“).

25 Wegen des Regel-Ausnahmeverhältnisses in Art. 2 Abs. 2 DS-GVO besitzt die DS-GVO-Sphäre zweifelsohne die größte praktische Bedeutung. Daher wird im Folgenden stets zunächst die DS-GVO in den Blick genommen. Das entbindet freilich nicht davon, die übrigen Rechtsquellen zumindest benennen und einordnen zu können.

b) Europäische Datenschutz-Richtlinie für Justiz und Inneres (JI-RL)

26 Zeitgleich mit der DS-GVO wurde die JI-RL (= RL 2016/680/EU) erlassen. Sie macht ausschließlich Vorgaben für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Art. 1 Abs. 1 JI-RL).[35] Im Gegensatz zur Verordnung ist die Richtlinie nicht unmittelbar in den Mitgliedsstaaten anwendbar. Sie muss erst durch den jeweiligen Gesetzgeber gem. Art. 288 Abs. 3 AEUV in nationales Recht umgesetzt werden, was sowohl auf Bundes- als auch auf Landesebene geschehen ist.

c) Europäische ePrivacy-Verordnung (ePrivacyVO)

27 Ursprünglich war auf europäischer Ebene geplant, zeitgleich mit der DS-GVO und der JI-RL eine Verordnung in Kraft zu setzen, die an die Stelle der in die Jahre gekommenen ePrivacy-Richtlinie (RL 2002/58/EG idF der RL 2009/136/EG) treten sollte. Alle bisherigen Vorschläge einer „Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation“ (ePrivacyVO) sind jedoch bislang gescheitert.[36]

d) Bundesdatenschutzgesetz (BDSG)

28 Das BDSG hat wegen des Anwendungsvorranges der DS-GVO stark an Bedeutung verloren. Es gilt für öffentliche Stellen des Bundes (Bundesbehörden) und sämtliche nicht-öffentlichen Stellen (Unternehmen, Vereine etc.), vgl. § 1 Abs. 1 BDSG.

29 Die §§ 22–44 BDSG passen das nationale Recht an die DS-GVO an. Dies umfasst jedoch nur spezifische Themenfelder, in denen die DS-GVO Regelungen in einem nationalen Gesetz überhaupt zulässt (sog. Öffnungsklauseln bzw. Regelungsspielräume).

35 Hierzu Schwichtenberg, DuD 2016, 605 ff.

36 Die Verhandlungen unter der portugiesischen Ratspräsidentschaft dauern unterdessen an, hierzu Etteldorf, MMR-Aktuell 2021, 436848.

Die §§ 45–84 BDSG setzen die Vorgaben der JI-RL um. Ein Teil der BDSG-Normen gilt schließlich für die unionsrechtsfreie Sphäre im Sinne von Art. 2 Abs. 2 DS-GVO (insoweit grundlegend § 1 Abs. 8 BDSG[37]). **30**

e) Landesdatenschutzgesetze (LDSG)

Das erste Datenschutzgesetz überhaupt in Deutschland war 1970 ein LDSG.[38] Die LDSGe gelten für die öffentlichen Stellen der Länder (Landesbehörden, Gemeinden/Kreise etc.). Dem Bundesgesetzgeber fehlt für diese Angelegenheiten die Gesetzgebungskompetenz, vgl. Art. 70 Abs. 1 GG. Wie das BDSG werden die jeweiligen LDSGe aufgrund des Anwendungsvorrangs der DS-GVO weitgehend zurückgedrängt. Dennoch ist auf Länderebene selbstverständlich ebenfalls eine Anpassung an die DS-GVO und eine Umsetzung der JI-RL erforderlich.[39] **31**

f) Kirchliche Datenschutzgesetze

Gem. Art. 91 Abs. 1 DS-GVO dürfen bestehende kirchliche Regeln zum Datenschutz angewandt werden, sofern sie mit der DS-GVO in Einklang gebracht werden. Sowohl das Kirchliche Datenschutzgesetz (KDG) der katholischen Kirche also auch das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) wurden deswegen überarbeitet. Zum Teil bestehen jedoch erhebliche Zweifel an der Europarechtskonformität der neuen Regelungen.[40] **32**

In der Praxis ist darüber hinaus häufig unklar, welches Gesetz zur Anwendung kommen soll, wenn es sich um gemischt staatlich-kirchliche Einrichtungen, ökumenische Einrichtungen oder kirchlich verfasste Stellen handelt, die am Wettbewerb teilnehmen. **33**

g) Bereichsspezifischer Datenschutz

BDSG, LDSGe und die Kirchengesetze sind als vollständige Regelwerke konzipiert. Sie sind dadurch weitgehend allgemein gehalten. Viele Lebensbereiche lassen sich mit diesen allgemeinen Vorschriften nicht zweckmäßig erfassen. Hierfür werden Spezialgesetze erlassen, welche die allgemeinen Regeln ergänzen oder nötigenfalls verdrängen.[41] **34**

Zu den wichtigsten bereichsspezifischen Datenschutzregeln gehören etwa das Telekommunikationsgesetz (§§ 88–107 TKG), der Sozialdatenschutz (§ 35 SGB I; §§ 67–85a SGB X) der Steuerdatenschutz (§§ 29b-32j AO) oder der Personalaktendatenschutz (§§ 106 ff. BBG bzw. landesbeamtenrechtliche Äquivalente). Darüber hinaus finden sich datenschutzrechtliche Einzelvorschriften immer wieder verstreut (etwa im TierschutzG, dem AufenthaltsG oder auch Anlage 6.5 Abs. 5 zur ArbeitsstättenVO, um einmal besonders weit auseinanderliegende Beispiele zu nennen). **35**

---

37 Diese breite Verweisnorm des BDSG wird in bereichsspezifischen Sicherheitsgesetzen wieder ausgeklammert, vgl. § 27 Nr. 1 BVerfSchG; § 32a Nr. 1 lit. a BNDG; § 13 Nr. 1 MADG; § 36 Abs. 1 Nr. 1 SÜG.

38 HessGVBl. 1970 I S. 625.

39 Übersicht über alle derzeit geltenden LDSGe unter https://dsgvo-gesetz.de/ldsg/.

40 Einzelheiten bei Golland, RDV 2018, 8 ff.; Hense, BRJ 2018, 37 ff.; Tinnefeld, ZD 2020, 145 ff.

41 Lat.: „lex specialis derogat legi generali", das speziellere Gesetz verdrängt das allgemeine.

36 Im Dezember 2021 tritt das Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG) in Kraft, welches Regelungsbereiche der einstweilig gescheiterten ePrivacyVO erfasst.[42]

2. Verträge

37 Es entspricht dem Prinzip der Vertragsfreiheit zwischen nominell gleichrangigen Parteien, dass diese das Recht untereinander weitgehend selbst bestimmen dürfen.

a) Privatrechtliche Verträge

38 Durch privatrechtliche Verträge im Sinne von § 311 Abs. 1 BGB verpflichten sich (mindestens) zwei Parteien zu einer Leistung und einer entsprechenden Gegenleistung. Für die Abwicklung des Vertragsverhältnisses, sei es etwa für die Lieferung, Rechnungslegung oder Prüfung von Zahlungseingängen wird stets auch die Verarbeitung personenbezogener Daten erforderlich. Art. 6 Abs. 1 lit. b DS-GVO[43] gestattet diese Verarbeitung. Die Parteien haben es insoweit weitestgehend selbst in der Hand, welche Daten für die Abwicklung erforderlich werden.

39 Sollen hingegen Daten Dritter zur Handelsware werden (etwa durch Adresshandel oder Auskunfteien), müssen andere Rechtfertigungsgründe gefunden werden, um den Datentransfer zu rechtfertigen.

b) Verträge über die Auftragsverarbeitung

40 Entsprechend der eher tautologischen Definition des Art. 4 Nr. 8 DS-GVO ist „Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

41 Der Aufgabenzuschnitt in Richtung des spezifischen Auftrags stellt klar, dass der Auftragnehmer niemals eigene Zwecke mit den Daten verfolgt. Die Auftragsverarbeitung ist eine Form der mehrpoligen Datenverarbeitung. Typischerweise werden Auftragsverarbeiter eingesetzt, weil sie eine Verarbeitungstätigkeit besser, schneller, günstiger oder sicherer ausführen können als der Verantwortliche selbst.

42 Bei der Auftragsverarbeitung rein nach DS-GVO wird ein Dienstleister organisatorisch derart eng an den Verantwortlichen gebunden, dass er rechtlich als Teil des Verantwortlichen gilt. Das geschieht mittels eines Vertrags, der gem. Art. 28 Abs. 3 DS-GVO gewisse Pflichtinhalte aufweisen muss.

43 Die Weitergabe von Daten muss unter der DS-GVO bei der Auftragsverarbeitung nicht gesondert gerechtfertigt werden. Der Unionsgesetzgeber bedient sich dabei eines juristischen Tricks, nämlich demjenigen der sog. „Fiktion": Der Auftragsverarbeiter ist gem. Art. 4 Nr. 10 DS-GVO nicht als „Dritter" anzusehen. Hierdurch ist die Weitergabe von Daten an den Auftragsverarbeiter in gewissem Sinne privilegiert.[44]

---

42 Hierzu näher Hanloser, ZD 2021, 121 f.; Schwartmann/Benedikt/Reif, MMR 2021, 99 ff; Lang, K&R 2020, 2020 (714 ff); GDD, Praxishilfe Das neue TTDSG im Überblick, Version 1.1., 2021.

43 Im Gesundheitsbereich in Verbindung mit Art. 9 Abs. 2 lit. h DS-GVO.

44 Für die Fortgeltung der Privilegierung auch Schmitz/Dall'Armi, ZD 2016, 427 (429); Schmidt/Freund, ZD 2017, 14 (16); Seiter, DuD 2019, 127 (130); Eckhardt CCZ 2017, 111 (113); Hartung/Büttgen, DuD 2017,