

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

© Nomos Verlagsgesellschaft, Baden-Baden 2022. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

Inhaltsverzeichnis

Vorwort	13
Einführung – Das juristische Gutachten im Datenschutz	15
I. Datenschutzrecht	15
1. Aufgabe und Grundrechtsrelevanz des Datenschutzrechts	15
2. Schutzgegenstand des Datenschutzrechts	17
3. Unionsrechtsbezug	18
4. Grundregeln und Schutzziele des Datenschutzrechts	19
II. Rechtsquellen datenschutzrechtlicher Auseinandersetzung	19
1. Vorschriften	19
a) Europäische Datenschutz-Grundverordnung (DS-GVO)	19
b) Europäische Datenschutz-Richtlinie für Justiz und Inneres (JI-RL)	20
c) Europäische ePrivacy-Verordnung (ePrivacyVO)	20
d) Bundesdatenschutzgesetz (BDSG)	20
e) Landesdatenschutzgesetze (LDSG)	21
f) Kirchliche Datenschutzgesetze	21
g) Bereichsspezifischer Datenschutz	21
2. Verträge	22
a) Privatrechtliche Verträge	22
b) Verträge über die Auftragsverarbeitung	22
c) Verträge über die gemeinsame Verantwortlichkeit	23
d) Standarddatenschutzklauseln	23
III. Weitere Textquellen datenschutzrechtlicher Auseinandersetzung	23
1. Kommentarliteratur	23
2. Zeitschriften	24
3. Rechtsprechung	25
4. Tätigkeitsberichte	25
5. Sonstige Behördenpapiere	26
IV. Die Auslegungsmethoden	26
1. Die grammatische Auslegung – Der Wortlaut	26
2. Die systematische Auslegung	28
3. Die historische Auslegung	29
4. Die teleologische Auslegung – Der Sinn und Zweck	30
V. Das Gutachten	30
1. Verwendung	30
2. Vorgehensweise	31
3. Alternative Prüfungsformen neben dem Gutachten	32
a) Fragenklausuren	32
b) Kautelarklausuren	33
VI. Prüfungstaktik	33
1. Schritte bis zum fertigen Gutachten	33
2. Vollständigkeit vs. Schwerpunktsetzung	34
3. Feststellungsstil	35
VII. Zur Arbeit mit diesem Buch	36

Klausur 1 – Datenschutzgrundlagen (Typ: Multiple Choice)	37
I. Multiple-Choice Fragen <input checked="" type="checkbox"/>	37
II. Lösungen	39
Klausur 2 – Recht der Datenschutzbeauftragten (Typ: Gutachten mit Zusatzfragen)	43
I. Sachverhalt	43
II. Bearbeitungsvermerk	43
III. Lösungsskizze	44
IV. Fallbearbeitung	45
1. Voraussetzungen für die Bestellung zur Datenschutzbeauftragten	45
a) Berufliche und fachliche Qualifikation	45
b) Fähigkeit zur Erfüllung der Aufgaben der Datenschutzbeauftragten gem. Art. 37 Abs. 5 DS-GVO	45
c) Ergebnis	47
2. Hinweise zur Information des Geschäftsführers	47
a) Praktische Durchführung der Bestellung	48
b) Rechte des Betriebsrats bei der Bestellung	48
c) Ordnungsgemäße Einbindung der Datenschutzbeauftragten in die Unternehmensorganisation	49
d) Beendigung der Funktion als Datenschutzbeauftragte	50
e) Vor- und Nachteile externer Datenschutzbeauftragter (Zusatzfrage)	53
Klausur 3 – Rechtmäßigkeit einer Visitenkartenbox (Typ: Gutachten)	54
I. Sachverhalt	54
II. Bearbeitungsvermerk	54
III. Lösungsskizze	54
IV. Gutachten	56
1. Anwendbarkeit der DS-GVO	56
a) Personenbezug und Verarbeitung	56
b) Automatisierungsgrad	57
2. Verantwortlichkeit	57
3. Rechtfertigung hinsichtlich der Anschriftendaten	57
a) Einwilligung	57
b) Vorvertragliche Maßnahmen	58
c) Interessenabwägung	59
4. Rechtfertigung hinsichtlich der Telefonnummern	59
a) Einwilligung	59
b) Vorvertragliche Maßnahmen	59
c) Interessenabwägung	59
5. Ergebnis	60
Klausur 4 – Auftragsverarbeitung (Typ: Fragenklausur)	61
I. Fragen (kein Gutachtenstil)	61
II. Antworten	63
1. Privilegierung	63
2. Vor-Ort-Kontrolle	63
3. Kosten	64
4. Zurückbehaltungsrecht	64

5. Fernwartung	65
6. Externe Datenschutzbeauftragte	65
7. Abgrenzung zur gemeinsamen Verantwortlichkeit	65
8. Arbeitnehmerüberlassung	66
Klausur 5 – Datenschutzhinweise einer Behörde (Typ: Gutachten)	67
I. Sachverhalt	67
II. Bearbeitungsvermerk	68
III. Lösungsskizze	68
IV. Gutachten	70
1. Information nach § 55 BDSG	70
a) Anwendbarkeit der §§ 45 ff. BDSG	70
b) Ergebnis	71
2. Information nach Art. 13 DS-GVO	71
a) Anwendbarkeit der DS-GVO	72
b) Direkterhebung	72
c) Umfang der Information	72
d) Zeitpunkt der Information	74
e) Zugänglichkeit der Information	75
3. Ergebnis	75
Klausur 6 – Datenschutzhinweise einer Kindertagesstätte (Typ: Gutachten)	76
I. Sachverhalt	76
II. Bearbeitungsvermerk	76
III. Lösungsskizze	77
IV. Gutachten	78
1. Name des Datenschutzbeauftragten	78
a) Antrag	78
b) Rechtsgrundlage der Verarbeitung	78
c) Widerspruchsgrund	80
d) Gegengründe	81
e) Zwischenergebnis	81
2. Verweis auf Webadresse	81
a) Darreichungsform	81
b) Transparenz	82
c) Leichte Zugänglichkeit	82
d) Zwischenergebnis	83
3. Pflicht zur Übersetzung	83
a) Verständlichkeit	83
b) Klare Sprache	83
c) Zwischenergebnis	84
4. Gesamtergebnis	84
Klausur 7 – Auskunft wegen eines Hinweisgebersystems (Typ: Gutachten)	85
I. Sachverhalt	85
II. Bearbeitungsvermerk	86
III. Lösungsskizze	87

IV. Gutachten	87
1. Anwendungsbereich der DS-GVO	87
a) Personenbezug	87
b) Verarbeitung	88
c) Automatisierungsgrad	88
d) JI-RL-Sphäre	89
2. Anspruchsberechtigter	89
3. Anspruchsgegner	89
4. Antrag und Antragsgegenstand	90
5. Ausnahmen	90
a) § 29 Abs. 1 Satz 2 BDSG	90
b) Art. 15 Abs. 4 DS-GVO	92
c) § 110 Abs. 1 Satz 3 BBG	93
6. Ergebnis	93
Klausur 8 – Auskunft wegen Examensklausuren (Typ: Gutachten)	94
I. Sachverhalt	94
II. Bearbeitungsvermerk	95
III. Lösungsskizze	95
IV. Gutachten	97
1. Anwendbarkeit	97
a) Personenbezug	97
b) Verarbeitung	99
c) Automatisierungsgrad	100
d) Anwendungsbereich des Unionsrechts	100
e) Zwischenergebnis	101
2. Anspruchsberechtigte und Anspruchsgegnerin	101
3. Antrag und Antragsgegenstand	101
4. Ausnahmen	102
a) Rechte und Freiheiten anderer Personen, Art. 15 Abs. 4 DS-GVO	102
b) Exzessiver Antrag, Art. 12 Abs. 5 Satz 2 lit. b DS-GVO	102
c) Fehlende Identifizierung, Art. 11 Abs. 2 Satz 2, Art. 12 Abs. 6 DS-GVO	103
d) Informationen bereits erhalten, Art. 13 Abs. 4, Art. 14 Abs. 5 Nr. 1 DS-GVO (analog)	103
e) Einsichtnahme lex specialis, § 23 Abs. 2 JAG NRW	103
f) Ausschluss für Prüfungseinrichtungen, § 2 Abs. 3 Var. 3 IFG NRW	104
g) Geheimhaltung, § 12 Abs. 2 Satz 1 Nr. 3 DSG NRW	104
5. Erfüllung	105
6. Kosten	105
7. Ergebnis	105
Klausur 9 – Telefonsperlliste in der Marktforschung (Typ: Gutachten)	106
I. Sachverhalt	106
II. Bearbeitungsvermerk	106
III. Lösungsskizze	107
IV. Gutachten	108
1. Anwendungsbereich der DS-GVO	108
2. Betroffene Person & Verantwortlicher	108

3. Antrag	108
4. Grund	108
a) Unrechtmäßige Verarbeitung	108
b) Konkludenter allgemeiner Widerspruch	110
c) Zweckfortfall	111
5. Ausnahmen	111
6. Ergebnis	111

Klausur 10 – Beschäftigtenfotos im Internet (Typ: Gutachten)	112
I. Sachverhalt	112
II. Bearbeitungsvermerk	112
III. Lösungsskizze	113
IV. Gutachten	114
1. Anwendbarkeit der DS-GVO	114
a) Personenbezug	114
b) Verarbeitung	114
c) Ergebnis	115
2. Zulässigkeit der Verwendung der Beschäftigtendaten im Internetauftritt	115
a) Rechtmäßigkeit der Verarbeitung	115
b) Erlaubnisnorm, Art. 6 Abs. 1 lit. b) DS-GVO	115
c) Erlaubnisnorm, § 26 Abs. 1 Satz 1 BDSG	116
d) Erlaubnisnorm, § 26 Abs. 2 BDSG	117
e) Erlaubnisnorm, Art. 6 Abs. 1 lit. f) DS-GVO	119
f) Ergebnis	119
3. Zulässigkeit der Verwendung der Beschäftigtendaten für eine „Geburtstagsliste“	119
a) Anwendbarkeit	120
b) § 26 Abs. 1 Satz 1 BDSG	120
c) Art. 6 Abs. 1 lit. f) DS-GVO	120
d) Ergebnis	121

Klausur 11 – Einschreiten wegen einer Dashcam (Typ: Gutachten)	122
I. Sachverhalt	122
II. Bearbeitungsvermerk	123
III. Lösungsskizze	123
IV. Gutachten	124
1. Ermächtigungsgrundlage	124
a) Einstellen der Aufzeichnung	124
b) Abbau der Kamera	124
2. Formelle Rechtmäßigkeit	125
a) Zuständigkeit	125
b) Verfahren	126
c) Form	126
3. Materielle Rechtmäßigkeit	126
a) Anwendungsbereich der DS-GVO	126
b) Tatbestandsmäßigkeit	128
c) Bestimmtheit	130
d) Ermessen und Verhältnismäßigkeit	130
4. Ergebnis	132

Klausur 12 – Schwarze Liste in einer Behörde (Typ: Gutachten)	133
I. Sachverhalt	133
II. Bearbeitungsvermerk	133
III. Lösungsskizze	134
IV. Gutachten	135
1. Anwendbarkeit DS-GVO	135
a) Personenbezug	135
b) Verarbeitung	135
c) Ergebnis	136
2. Zulässigkeit	136
a) Rechtmäßigkeit der Verarbeitung	136
b) Erlaubnisnorm	137
c) Transparenz	137
d) Speicherdauer	139
e) Integrität und Vertraulichkeit	139
3. Ergebnis	139
Klausur 13 – Forderungs-Management eines Tierarztes (Typ: Gutachten)	140
I. Sachverhalt	140
II. Bearbeitungsvermerk	140
III. Lösungsskizze	141
IV. Gutachten	142
1. Vorgehen der Datenschutzaufsicht	142
a) Ermächtigungsgrundlage	142
b) Materielle Rechtmäßigkeit	142
c) Ergebnis	146
2. Weitergabe der Daten	146
a) Anwendbarkeit der DS-GVO	146
b) Vertragserfüllung	147
c) Interessenabwägung	147
d) Ergebnis	148
Klausur 14 – Marketing und Marktforschung (Typ: Multiple Choice)	150
I. Multiple-Choice Fragen <input checked="" type="checkbox"/>	150
II. Lösungen	153
Klausur 15 – Informationsfreiheit und Datenschutz (Typ: Gutachten)	159
I. Sachverhalt	159
II. Bearbeitungsvermerk	159
III. Lösungsskizze	160
IV. Gutachten	161
1. Anspruchsberechtigter	161
2. Amtliche Information und Behörde	161
3. Antrag	161
4. Ausnahme	161
a) Personenbezug	162
b) Schutzwürdiges Interesse	162
5. Ergebnis	164

Klausur 16 – Verwarnung wegen eines Sichtfensterumschlages	
(Typ: Gutachten)	165
I. Sachverhalt	165
II. Bearbeitungsvermerk	166
III. Lösungsskizze	166
IV. Gutachten	168
1. Zulässigkeit	168
a) Verwaltungsrechtsweg	168
b) Statthaftigkeit	169
c) Klagebefugnis	171
d) Vorverfahren	173
e) Beteiligtenfähigkeit und Passivlegitimation	173
f) Zwischenergebnis	173
2. Begründetheit	173
a) Rechtmäßigkeit des VA	173
b) Rechtsverletzung	177
c) Zwischenergebnis	178
3. Ergebnis	178
Klausur 17 – Schutzverletzungen (Typ: Gutachten mit Zusatzfragen)	179
I. Sachverhalt	179
II. Bearbeitungsvermerk	180
III. Lösungsskizze	180
IV. Gutachten	182
Frage 1 (Verein V)	182
a) Anwendungsbereich der DS-GVO und Verantwortlicher	182
b) Schutzverletzung	182
c) Hohes Risiko	183
d) Ausnahmen	184
e) Ergebnis	184
Frage 2a (Unternehmen U)	184
a) Frist	184
b) Form	185
Frage 2b (Rechtsanwalt R)	185
a) Verschlüsselung	186
b) Berufsgeheimnisträger	186
Frage 2c (Verantwortlicher V)	186
Klausur 18 – Schadensersatz wegen Sperrung eines Nutzer-Accounts	
(Typ: Gutachten mit Zusatzfrage)	187
I. Sachverhalt	187
II. Bearbeitungsvermerk	188
III. Lösungsskizze	188
IV. Gutachten	190
1. Anspruch gem. Art. 82 Abs. 1 DS-GVO	190
a) Anwendbarkeit der DS-GVO	190
b) Anspruchsberechtigter	191
c) Anspruchsverpflichtete	191
d) Schaden	191
e) Pflichtverletzung	193
f) Kausalität	194

g) Verschulden und Beweislast	195
h) Ergebnis	195
2. Anspruch gem. § 823 Abs. 1 BGB in Verbindung mit. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG	195
a) Anwendbarkeit	195
b) Rechtsgutverletzung	195
c) Verletzungshandlung	196
d) Kausalität	196
e) Rechtswidrigkeit	196
f) Verschulden	196
g) Ergebnis	196
3. Anspruch gem. § 826 BGB	196
a) Anwendbarkeit	196
b) Schaden	196
c) Sittenwidrigkeit	197
d) Ergebnis	197
4. Ergebnis	197
Zusatzfrage: Anspruch gegen den Datenschutzbeauftragten der F	197
Ausblick	199
Stichwortverzeichnis	201

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@datenschutzkoментарar.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 Rechts- 1
 wissenschaften im entsprechenden Schwerpunktbereich¹ 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 vorkom-
 men.

Die Rechtsanwendung im Datenschutz bewegt sich dabei an der Schnittstelle von 2
 Recht und Technik und zugleich im Grenzdickicht vielfältiger Rechtsquellen, auf-
 sichtsbehördlicher Zuständigkeiten sowie einer blühenden Kommentarlanschaft. 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.

I. Datenschutzrecht

1. Aufgabe und Grundrechtsrelevanz des Datenschutzrechts

Das Datenschutzrecht schützt – vereinfacht ausgedrückt – natürliche Personen vor 3
 unrechtmäßiger, unrichtiger und missbräuchlicher Verarbeitung ihrer personenbezo-
 genen Daten. Aus der grundlegenden Beschränkung auf natürliche Personen er-
 gibt sich die **Menschzentriertheit** des Datenschutzrechts (klarstellend Erwägungs-
 grund 14 Satz 1 DS-GVO). Juristische Personen werden nur dann in den Schutzbe-
 reich des Datenschutzrechts einbezogen, wenn sich dies unmittelbar kraft gesetz-
 lichen Verweises ergibt, etwa im Telekommunikations-,³ Steuer-⁴ oder Sozialdaten-
 schutz.⁵

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 Zeugnis⁶ 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**): „*Das 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 Lüsterheit 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 bestimmtem 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 verbriefteter 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 **8** 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 Lauschangriffs¹¹) und das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme¹² (sog. Computergrundrecht) gem. Artt. 1 Abs. 1, 2 Abs. 1 GG.

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-Holstein²² und Thüringen²³ 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 Menschenrechtskonvention (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 mitgliedstaatliche 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 Callies/Ruffert/Ruffert, EUV/AEU, 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 ff.).

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 18 (und müssen) nationale Gerichte im Wege des **Vorabentscheidungsverfahrens** gem. Art. 267 AEUV den EuGH anrufen.³¹

4. Grundregeln und Schutzziele des Datenschutzrechts

Die Grundsätze der Verarbeitung sind in Art. 5 DS-GVO niedergelegt und sollen hier 19 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

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 ehemals nach Maßgabe des Volkszählungsurteils) wissen „*wer was wann und bei welcher Gelegenheit über sie weiß*“.

Zweckbindung, Datenminimierung und Speicherbegrenzung (Art. 5 Abs. 1 litt. b, c 21 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

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

II. Rechtsquellen datenschutzrechtlicher Auseinandersetzung

1. Vorschriften

„Ein Blick ins Gesetz erleichtert die Rechtsfindung.“ Diese häufig ironisch gebrauchte 23 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.

a) Europäische Datenschutz-Grundverordnung (DS-GVO)

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

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. „Markortprinzip“).

- 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 BDSG³⁷). **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 AufenthaltsgG 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-GVO⁴³ 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,