

Handbuch Europäisches und deutsches Datenschutzrecht

Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor

Bearbeitet von

Herausgegeben von Prof. Dr. Louisa Specht, und Dr. Reto Mantz, Dipl.-Inf., Richter am Landgericht, Unter Mitarbeit von Kirsten Bock, Prof. Dr. Benjamin Bodungen, LL.M., Dr. Tobias Born, Dr. Christoffer Bortz, Dr. Sebastian Bretthauer, Dr. Malte Engeler, Dr. Sebastian Golla, Dr. Dennis Heinson, LL.M., Dr. Moritz Hennemann, M.Jur. (Oxford), Dr. Gerd Kiparski, MBA, Dr. Dennis-Kenji Kipker, Dr. Stefan Krätschmer, PD Dr. Bernhard Kreße, LL.M., Prof. Dr. Anne Lauber-Rönsberg, LL.M., Johannes Marosi, Dr. Anne Paschke, Maren Pollmann, Prof. Dr. Jan Dirk Roggenkamp, Elke Sassenberg, Adrian Schneider, Dr. Jan Spittka, Prof. Dr. Eric Steinhauer, Dr. Björn Steinrötter, Dr. Lukas Ströbel, Dr. Mirko Wiczorek, und Tim Wybitul

1. Auflage 2019. Buch. XLII, 788 S. Hardcover (In Leinen)

ISBN 978 3 406 72539 5

Format (B x L): 16,0 x 24,0 cm

[Recht > Handelsrecht, Wirtschaftsrecht > Telekommunikationsrecht, Postrecht, IT-Recht > Datenschutz, Postrecht](#)

Zu [Leseprobe](#) und [Sachverzeichnis](#)

schnell und portofrei erhältlich bei

The logo for beck-shop.de features the text 'beck-shop.de' in a bold, red, sans-serif font. Above the 'i' in 'shop' are three red dots of varying sizes, arranged in a slight arc. Below the main text, the words 'DIE FACHBUCHHANDLUNG' are written in a smaller, red, all-caps, sans-serif font.

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung [beck-shop.de](#) ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Specht / Mantz

Handbuch Europäisches und deutsches Datenschutzrecht


beck-shop.de
DIE FACHBUCHHANDLUNG

beck-shop.de
DIE FACHBUCHHANDLUNG

Handbuch Europäisches und deutsches Datenschutzrecht

Bereichsspezifischer Datenschutz in
Privatwirtschaft und öffentlichem Sektor

Herausgegeben von

Prof. Dr. Louisa Specht

Lehrstuhl für Bürgerliches Recht,
Daten- und Informationsrecht an der
Rheinische Friedrich-Wilhelms-Universität
Bonn

Dr. Reto Mantz

Dipl.-Inf., Richter am Landgericht
Frankfurt a.M.

beck-shop.de
DIE FACHBUCHHANDLUNG

2019





beck-shop.de
DIE FACHBUCHHANDLUNG

www.beck.de

ISBN 978 3 406 72539 5

© 2019 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München
Druck: Beltz Grafische Betriebe GmbH
Am Fliegerhorst 8, 99947 Bad Langensalza

Satz: 3w+p GmbH, Rimpfing
Umschlaggestaltung: Druckerei C.H. Beck, Nördlingen

Gedruckt wird auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Vorwort

Datenschutzrecht ist (nicht erst) seit Verabschiedung der Datenschutzgrundverordnung (DS-GVO) in aller Munde. Die in immer geringeren Abständen auftretenden Datenkandale lassen das Datenschutzrecht immer deutlicher auch in das Bewusstsein derer treten, die bislang keinen rechten Bezug zu diesem Rechtsgebiet finden konnten. Mit der Geltungserlangung der DS-GVO am 25.5.2018 und der Änderung des nationalen Datenschutzrechts kommt es nun zu teils erheblichen Rechtsänderungen.

Diese Rechtsänderungen fallen jedoch bereichsspezifisch sehr verschieden aus. Die Bereichsspezifität besteht dabei nicht nur zwischen dem privaten Wirtschaftssektor und dem öffentlich-rechtlichen Bereich. Auch innerhalb des privaten und des öffentlich-rechtlichen Sektors differieren die datenschutzrechtlichen Herausforderungen erheblich. Die Spanne reicht hier im Privatrecht von Automotive und Arbeitsrecht über Finanzen, Versicherungen, Medizin, Energie, TK und IT bis zum Datenschutz bei Anwaltschaft und Presse, im öffentlich-rechtlichen Bereich von Schulen und Universitäten sowie Forschung und Wissenschaft über die Verwaltung, Strafverfolgung, Kultureinrichtungen, Bibliotheken, Museen und Archiven bis hin zu Sozialdatenschutz und Kirchen.

Für den Praktiker stellt sich hier die Frage, welche Vorgaben für ihn konkret (und ggf. erstmals) zu beachten sind, wenn er Akteure aus den spezifischen Bereichen berät, welche Fragen und Probleme er bedenken muss und welche Maßnahmen konkret zu ergreifen sind. Hierbei kann bereits die Ermittlung der anwendbaren Normen (DS-GVO, JI-RL, ePrivacy-Richtlinie bzw. -Verordnung sowie bundes- und/oder landesrechtlich zu berücksichtigende Normen wie Umsetzungsregelungen oder Normen zur Ausgestaltung der Öffnungsklauseln) eine erhebliche Schwierigkeit darstellen. Die bisher erschienenen, zweifellos hervorragenden Werke zum neuen Datenschutzrecht erörtern das Datenschutzrecht in der Regel im Allgemeinen und häufig einzig aus Sicht von DS-GVO und BDSG, zT mit landesdatenschutzrechtlichen Bezügen. Übersichtliche Aufarbeitungen insbesondere in Handbüchern, die die für die verschiedenen Sektoren spezifisch relevanten Probleme herausarbeiten und Lösungen vorschlagen, liegen derzeit nur sehr vereinzelt vor, außerdem behandeln diese einzelne Bereiche in der Regel nur für sich. Für den Anwender bedeutet dies, dass er allgemeine Ausführungen auf den für ihn relevanten Bereich übertragen und zurückführen muss, ohne dass er zwangsläufig zu den ihn betreffenden, ganz konkreten Fragestellungen auf Hinweise hoffen kann.

Diese Lücke zu schließen ist die Aufgabe dieses Handbuchs. Für dieses Unterfangen haben wir ausgewiesene Praktiker und Wissenschaftler versammelt, die das europäische und deutsche Datenschutzrecht bereichsspezifisch aufarbeiten, wobei zunächst einführend die verfassungsrechtlichen Grundlagen, Grundzüge der DS-GVO und des neuen BDSG, Grundlagen der Compliance sowie von ePrivacy, ferner das Straf- und Ordnungswidrigkeitenrecht dargestellt werden.

Wir bedanken uns herzlich bei den Autoren für die großartige Zusammenarbeit, ohne die eine so zeitnahe Anfertigung des Handbuchs nicht gelungen wäre. Ein besonderer Dank gilt auch den Mitarbeitern des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht an der Rheinischen Friedrich-Wilhelms-Universität Bonn und hier insbesondere Frau Rebecca Rohmer, die die redaktionelle Bearbeitung der Beiträge vollständig übernommen hat und deren Genauigkeit, Fleiß und Einsatz nicht genug gelobt werden können.

Bonn/Frankfurt am Main im August 2018
Louisa Specht/Reto Mantz

beck-shop.de
DIE FACHBUCHHANDLUNG

Inhaltsübersicht

Vorwort	V
Inhaltsverzeichnis	IX
Autorenverzeichnis	XXIX
Abkürzungsverzeichnis und Verzeichnis der abgekürzt zitierten Literatur	XXXI

Teil A. Datenschutzrechtliche Grundlagen

§ 1 Einführung (<i>Specht/Mantz</i>)	1
§ 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht (<i>Bretthauer</i>)	7
§ 3 Vorgaben der Datenschutz-Grundverordnung (<i>Mantz/Marosi</i>)	38
§ 4 BDSG und andere sondergesetzliche Datenschutzregelungen (<i>Lauber-Rönsberg</i>)	95
§ 5 ePrivacy (<i>Steinrötter</i>)	129
§ 6 Compliance (<i>Krätschmer</i>)	143
§ 7 Internationaler Datentransfer (<i>Wieczorek</i>)	166
§ 8 Datenschutz und Straf- und Ordnungswidrigkeitenrecht (<i>Born</i>)	210

Teil B. Datenschutzrecht in der Privatwirtschaft

§ 9 Verbraucherdatenschutz (<i>Specht</i>)	233
§ 10 Beschäftigendatenschutz (<i>Ströbel/Wybitul</i>)	279
§ 11 Datenschutz in der Anwaltschaft (<i>Bortz</i>)	308
§ 12 Datenschutz in der Privatversicherung (<i>Spittka</i>)	336
§ 13 Datenschutz im Medizinsektor (<i>Paschke</i>)	365
§ 14 Datenschutz im Finanzwesen (<i>Heinson</i>)	391
§ 15 Datenschutz in der Informationstechnik (<i>Schneider</i>)	418
§ 16 Datenschutz im Automotive-Sektor (<i>von Bodungen</i>)	450
§ 17 Datenschutz im Energiesektor (<i>Kreße</i>)	479
§ 18 Datenschutz im Telekommunikationssektor (<i>Kiparski</i>)	505
§ 19 Datenschutz in Presse und anderen Medien (<i>Hennemann</i>)	530

Teil C. Datenschutzrecht im öffentlichen Sektor

§ 20 Datenschutz in der Verwaltung von Bund, Ländern und Kommunen (<i>Bock</i>)	559
§ 21 Datenschutz und präventive Tätigkeit der Polizei (<i>Roggenkamp</i>)	599
§ 22 Datenschutz in der Justiz (<i>Engeler</i>)	623
§ 23 Datenschutz in Forschung und Hochschullehre (<i>Golla</i>)	646
§ 24 Datenschutz in Schule und Schulverwaltung (<i>Sassenberg</i>)	672
§ 25 Datenschutz in Kultureinrichtungen, Bibliotheken und Archiven (<i>Steinhauer</i>) ...	699
§ 26 Sozialdatenschutz (<i>Kipker/Pollmann</i>)	718
§ 27 Kirchliches Datenschutzrecht (<i>Paschke</i>)	762
Sachverzeichnis	769

beck-shop.de
DIE FACHBUCHHANDLUNG

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Autorenverzeichnis	XXIX
Abkürzungsverzeichnis und Verzeichnis der abgekürzt zitierten Literatur	XXXI

Teil A. Datenschutzrechtliche Grundlagen

§ 1 Einführung	1
I. Bedeutung des bereichsspezifischen Datenschutzrechts	1
II. Allgemeiner Teil des Handbuchs	2
III. Besonderer Teil des Handbuchs	3
§ 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht	7
I. Einleitung	8
1. Hintergrund	8
2. Historische Entwicklung des Datenschutzes	9
3. Gegenwart des Datenschutzes	11
II. Anwendbare Vorschriften	12
1. Art. 7 GRCh	12
2. Art. 8 GRCh	13
a) Schutzbereichsdimension, Eingriff und Rechtfertigung	13
b) Verfassungsrechtliche Grundprinzipien des Datenschutzes	17
3. Art. 16 AEUV	22
4. Art. 8 EMRK	23
5. Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG	24
a) Recht auf informationelle Selbstbestimmung	25
b) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	27
III. Einzelprobleme	28
1. Verhältnis der datenschutzrechtlichen Normen im grundrechtlichen Mehrebenensystem	28
2. Grundrechtsberechtigte & Grundrechtsverpflichtete	30
a) Grundrechtsberechtigte	30
b) Grundrechtsverpflichtete	31
3. Dogmatische Einordnung der Einwilligung	31
4. Einschlägige Schrankenregelung des Datenschutzgrundrechts	32
5. Drittwirkung des Datenschutzgrundrechts	33
6. Rolle der Gerichte im Mehrebenensystem des Datenschutzes	34
7. Rechtsschutz	35
IV. Fazit	37
§ 3 Vorgaben der Datenschutz-Grundverordnung	38
I. Einleitung	40
II. Anwendbare Normen	40
III. Anwendungsbereich	41
1. Sachlicher Anwendungsbereich	41

a) Identifizierung natürlicher Personen	42
b) Anonyme und pseudonyme Daten	43
c) Automatisiert oder in einem Dateisystem gespeichert	44
2. Persönlicher Anwendungsbereich	44
a) Verantwortlicher	44
b) Auftragsverarbeiter	45
c) Dritter	46
d) Empfänger	46
e) Betroffener	46
f) Ausschließlich persönliche oder familiäre Tätigkeiten	46
3. Räumlicher Anwendungsbereich	47
a) Niederlassungsprinzip	47
b) Marktortprinzip	48
c) Völkerrecht	49
4. Unanwendbarkeit und Verhältnis zu anderen Rechtsakten	49
IV. Zulässigkeit der Verarbeitung	51
1. Rechtmäßigkeit	51
a) Allgemeines	51
b) Einwilligung	52
c) Gesetzliche Rechtfertigungstatbestände	53
d) Werbung	56
e) Daten von Kindern	56
f) Verarbeitung besonderer Kategorien personenbezogener Daten	57
g) Daten über strafrechtliche Verurteilungen und Straftaten	58
h) Automatisierte Entscheidungen im Einzelfall und Profiling	58
2. Verarbeitung nach Treu und Glauben	59
3. Transparenz	59
4. Zweckbindung	60
a) Grundlagen	60
b) Zweckfestlegung	60
c) Zweckänderung	61
d) Ausnahmen für wissenschaftliche, historische, statistische Zwecke ..	62
5. Datenminimierung	62
6. Informationspflichten und Betroffenenrechte	63
a) Informationspflichten	63
b) Auskunftsrecht	67
c) Berichtigung	68
d) Löschung	68
e) Einschränkung der Verarbeitung	69
f) Datenübertragbarkeit (Art. 20 DS-GVO)	70
g) Widerspruch	70
7. Rechenschaftspflicht	71
V. Gemeinsam Verantwortliche und Auftragsverarbeitung	71
1. Gemeinsam Verantwortliche	71
a) Definition	71
b) Abgrenzung	72
c) Pflichten	72
2. Auftragsverarbeiter	73
a) Allgemeines	73
b) Abgrenzung	73
c) Pflichten und Anforderungen	73
VI. Risikobeherrschung: Datenschutz durch Technik, Sicherheit und Folgenabschätzung	75

1. Grundsätze	75
2. Risikoabschätzung	76
3. Datenschutz durch Technik	77
4. Sicherheit	77
5. Meldung von Verletzungen	78
6. Benachrichtigung bei Verletzungen	79
VII. Datenschutzbeauftragter	79
1. Rolle	79
2. Pflicht zur Benennung	79
3. Stellung und Aufgaben	81
a) Stellung	81
b) Aufgaben	81
4. Haftung	82
VIII. Selbstregulierung	82
1. Verhaltensregeln	82
2. Berechtigte, Inhalt	83
3. Genehmigung, Allgemeinverbindlichkeit	83
4. Anwendung und Wirkung	83
5. Zertifizierung	84
IX. Internationale Datentransfers	84
X. Aufsichtsbehörden, Europäischer Datenschutzausschuss	85
1. Stellung	85
2. Aufgaben	86
3. Befugnisse	86
4. Zuständigkeit und Zusammenarbeit	87
a) Zuständigkeit	87
b) Zusammenarbeit	88
5. Europäischer Datenschutzausschuss	90
a) Organisation und Vertretung	91
b) Aufgabe: Einheitliche Anwendung der DS-GVO	91
c) Verfahren	91
XI. Rechtsbehelfe, Haftung und Sanktionen	92
1. Sanktionsmöglichkeiten der Aufsichtsbehörde	92
2. Recht auf Beschwerde	92
3. Recht auf gerichtliche Durchsetzung	93
4. Schadenersatzansprüche der betroffenen Personen	93
5. Verbände, Wettbewerber	94
a) Verbandsklage	94
b) Klagebefugnis von Wettbewerbern?	94
§ 4 BDSG und andere sondergesetzliche Datenschutzregelungen	95
I. Einleitung	96
1. Verhältnis der DS-GVO zu nationalen Regelungen	96
a) Anwendungsvorrang der Verordnung	96
b) Mitgliedstaatliche Regelungsspielräume	98
c) Normwiederholungsverbot hinsichtlich der Vorgaben der DS-GVO	99
2. Umsetzung der JI-RL 2016/680	100
3. Reform des deutschen Datenschutzrechts	100
II. Das neue BDSG	102
1. Konzept und Struktur	102
a) Gliederung des BDSG	103

b) Auswirkungen des Mehrebenensystems	103
2. Anwendungsbereich des BDSG	105
a) Sachlicher Anwendungsbereich	105
b) Adressaten des BDSG	108
c) Zeitlicher Anwendungsbereich	109
d) Räumlicher Anwendungsbereich	110
3. Rechtmäßigkeit der Datenverarbeitung	110
a) Allgemeine Grundsätze der Datenverarbeitung	110
b) Öffnungsklauseln der DS-GVO und ihre Ausgestaltung	111
c) Vorgaben zur Rechtmäßigkeit der Verarbeitung im Anwendungsbereich der JI-RL	120
4. Betroffenenrechte	120
a) Ausgestaltung des Art. 23 Abs. 1 DS-GVO im nationalen Recht ...	120
b) Vorgaben der JI-RL	125
5. Rechtsbehelfe, Haftung, Sanktionen	125
6. Datenschutzbeauftragte	125
7. Aufsichtsbehörden	126
8. Zusammenarbeit und Kohärenz	126
III. Anpassung weiterer Bundesgesetze	127
IV. Landesrechtliche Regelungen	128
V. Fazit	128
§ 5 ePrivacy	129
I. Einleitung	129
II. Anwendbare Vorschriften	131
III. Einzelprobleme	132
1. Verhältnis zur DS-GVO	132
2. Anwendungsbereich	132
a) Intertemporal	132
b) Sachlich	133
c) Räumlich und persönlich	135
3. Inhaltliche Grundstruktur	136
a) Verbot mit Erlaubnisvorbehalt: Einwilligung	136
b) Verbot mit Erlaubnisvorbehalt: Gesetzliche Legitimationstatbestände	139
c) Lösungs- und Anonymisierungsgebote	141
4. Aufsichtsarchitektur und Durchsetzungsmechanismen	141
5. Unerwünschte Anrufe	142
6. Direktwerbung	142
§ 6 Compliance	143
I. Einleitung	143
II. Allgemeine Compliance-Anforderungen	144
1. Der Begriff der „Compliance“	144
2. Verantwortung für Compliance im Unternehmen	145
3. Compliance-Pflichten und Compliance-Management-System	145
III. Anwendbare Vorschriften: Compliance iRd DS-GVO	147
1. Compliance-Verantwortung iRd DS-GVO	147
a) Verantwortung im Unternehmen: Datenschutzbeauftragter	147
b) Verantwortung zwischen Unternehmen: Verantwortlicher und Auf- tragsverarbeiter	149
2. Organisationspflichten: TOM und Risikomanagement	150
a) Technische und organisatorische Maßnahmen (TOM)	150
b) Risikomanagement	153

3. Dokumentationspflicht: Nachweis der Compliance	154
4. Informationspflicht	157
5. Überprüfungspflicht: Audits	158
IV. Einzelprobleme	159
1. Projektmanagement und Compliance-Methode	159
2. Definition und Dokumentation der Anforderungen	160
3. Bestandsanalyse	161
4. Lücken- und Risikoanalyse	162
5. Lösungsentwicklung und Kontrolle	163
V. Fazit	164
§ 7 Internationaler Datentransfer	166
I. Einleitung	168
II. Anwendbare Vorschriften	168
III. Einzelprobleme	169
1. Angemessenheitsbeschlüsse (Art. 45 DS-GVO)	169
a) Anwendungsbereich	169
b) Anforderungen	170
c) Verfahren	171
d) Sonderfälle	172
2. Genehmigungsfreie Garantien	174
a) Vereinbarungen im öffentlichen Bereich (Art. 46 Abs. 2 lit. a DS-GVO)	175
b) Verbindliche interne Datenschutzvorschriften – Binding Corporate Rules (BCR) (Art. 46 Abs. 2 lit. b, 47 DS-GVO)	176
c) Standarddatenschutzklauseln der Kommission (Art. 46 Abs. 2 lit. c DS-GVO)	184
d) Standarddatenschutzklauseln der Aufsichtsbehörden (Art. 46 Abs. 2 lit. d DS-GVO)	188
e) Genehmigte Verhaltensregeln – Codes of Conduct (CoC) (Art. 46 Abs. 2 lit. e, 40, 41 DS-GVO)	189
f) Zertifizierungen (Art. 46 Abs. 2 lit. f, 42, 43 DS-GVO)	190
3. Genehmigungspflichtige Garantien	191
a) Ad-hoc-Vertragsklauseln (Art. 46 Abs. 3 lit. a DS-GVO)	192
b) Bestimmungen in Verwaltungsvereinbarungen (Art. 46 Abs. 3 lit. b DS-GVO)	193
4. Rechtshilfeabkommen/internationale Übereinkünfte (Art. 48 DS-GVO)	193
5. Ausnahmen vom Rechtfertigungserfordernis	195
a) Ausdrückliche Einwilligung (Art. 49 Abs. 1 UAbs. 1 lit. a, Abs. 3 DS-GVO)	196
b) Verträge zwischen Betroffenen und Verantwortlichen (Art. 49 Abs. 1 UAbs. 1 lit. b, Abs. 3 DS-GVO)	198
c) Verträge im Interesse der Betroffenen (Art. 49 Abs. 1 UAbs. 1 lit. c, Abs. 3 DS-GVO)	199
d) Öffentliches Interesse (Art. 49 Abs. 1 UAbs. 1 lit. d, Abs. 4 DS-GVO)	200
e) Rechtsansprüche (Art. 49 Abs. 1 UAbs. 1 lit. e DS-GVO)	201
f) Lebenswichtige Interessen (Art. 49 Abs. 1 UAbs. 1 lit. f DS-GVO)	202
g) Öffentliche Register (Art. 49 Abs. 1 UAbs. 1 lit. g), Abs. 2 DS-GVO)	202

h) Auffangtatbestand der „zwingenden berechtigten Interessen“ des Verantwortlichen (Art. 49 Abs. 1 UAbs. 2, Abs. 3 und 6 DS-GVO)	202
6. Sonstiges und Sonderfälle	205
a) Europäische und nationale Beschränkungen (Art. 49 Abs. 5 DS-GVO)	205
b) Internationale Zusammenarbeit (Art. 50 DS-GVO)	205
c) Internationaler Datentransfer im Konzern	205
d) Outsourcing	207
e) Discovery	207
f) Datentreuhändermodelle	208
g) Datenschutzrechtliche Folgen des Ausscheidens aus der EU/des EWR	209
§ 8 Datenschutz und Straf- und Ordnungswidrigkeitenrecht	210
I. Einleitung	211
1. EU-Recht	211
2. Bundesrecht	211
3. Landesrecht	211
II. Bußgeld-/Ordnungswidrigkeitenverfahren unter der DS-GVO	211
1. Das aufsichtsbehördliche Bußgeldverfahren	211
a) Anwendbares Verfahrensrecht	211
b) Zuständigkeit	212
c) Verfahren	213
d) Form	215
2. Bußgeldtatbestände der DS-GVO	215
a) Verantwortliche und Auftragsverarbeiter als Täter/Adressat	215
b) Zurechnung des Handelns natürlicher Personen	216
c) Personal und Dritte als Nebentäter	217
d) Verstoß gegen DS-GVO-Norm	217
e) Verschuldenserfordernis?	220
f) Versuch	221
g) Entscheidung über Verhängung Geldbuße und deren Höhe	221
h) Einziehung	226
i) Verjährung	226
j) Eintragung von Bußgeldbescheiden in das Gewerbeverzeichnis	226
III. Ordnungswidrigkeiten im nationalen Recht	226
1. Das aufsichtsbehördliche Bußgeldverfahren	226
2. Bußgeldtatbestände	227
IV. Strafverfahren	227
1. Verfahrensrecht	228
2. Einzelne Straftatbestände	228
3. Strafzumessung	228
V. Rechtsschutz	228
1. Ordnungswidrigkeiten	228
a) Rechtsbehelf: Einspruch	228
b) Rechtsmittel: Rechtsbeschwerde	230
2. Strafverfahren	231
Teil B. Datenschutzrecht in der Privatwirtschaft	
§ 9 Verbraucherdatenschutz	233
I. Einleitung	235
1. Grundlagen	235
2. Aktuelle Entwicklungen	236

II. Anwendbare Vorschriften	237
1. DS-GVO	238
2. BDSG	239
3. ePrivacy-VO E	239
4. Bereichsspezifische Regelungen	242
III. Einzelprobleme	242
1. Verarbeitungsgrundsätze	242
a) Insbes. Grundsatz der Datensparsamkeit (Datenminimierung)	243
b) Grundsatz der Zweckbindung	243
2. Einwilligungserfordernis	244
a) Koppelungsverbot	246
b) Form (keine Schriftlichkeit, Einwilligung in AGB etc)	248
c) Opt Out/Opt In/Double Opt In/Triple Opt In	249
d) Einwilligung durch Do-not-Track-Einstellungen	250
e) Anforderungen des § 7 UWG	250
f) Stellvertretung	251
g) Widerruflichkeit	252
h) Einwilligung von Kindern, Art. 8 DS-GVO	252
i) Fortgeltung von Alteinwilligungen	253
3. Erlaubnistatbestände	253
a) Vertragserfüllung, Art. 6 Abs. 1 lit. b DS-GVO	254
b) Interessenabwägung	256
c) Regelungen des BDSG	257
4. Betroffenenrechte	258
a) Auskunft (Art. 15 DS-GVO)	258
b) Berichtigung (Art. 16 DS-GVO)	259
c) Löschung (Art. 17 DS-GVO)	259
d) Einschränkung der Verarbeitung (Art. 18 DS-GVO)	259
e) Mitteilungspflicht (Art. 19 DS-GVO)	260
f) Datenübertragbarkeit (Art. 20 DS-GVO)	260
g) Widerspruch (Art. 21 DS-GVO)	260
h) Automatisierte Einzelfallentscheidungen (Art. 22 DS-GVO)	261
5. Spezifische Anwendungsfälle	261
a) Scoring und Bonitätsauskünfte	261
b) Cookie-Tracking	262
c) Webanalytics, Webtracking	265
d) Profiling	267
e) E-Mail-Werbung	269
f) Telefonmarketing	270
g) Soziale Netzwerke	270
h) Gewinnspielteilnahme	273
i) Kundenkartenprogramme	273
j) Big Data-Analysen	274
k) Adresshandel	275
6. Durchsetzung des Datenschutzrechts	275
a) Befugnisse der Aufsichtsbehörden	275
b) Sanktions- und Klagemöglichkeiten	276
§ 10 Beschäftigtendatenschutz	279
I. Einleitung	280
II. Anwendbare Vorschriften	280
1. Art. 88 DS-GVO	280

a) Übersicht	280
b) Anwendungsbereich	281
c) Verhältnis der Ausführungsgesetze zum Beschäftigtendatenschutz zur DS-GVO	283
d) Anforderung an nationale und kollektivrechtliche Regelungen zum Beschäftigtendatenschutz	283
2. § 26 BDSG	285
a) Übersicht	285
b) Anwendungsbereich	287
c) Erlaubnistatbestände	287
III. Einzelprobleme	292
1. Einwilligung in Datenverarbeitung im Arbeitsverhältnis	292
a) Zulässigkeit der Einwilligung auch im Beschäftigungsverhältnis	292
b) Freiwilligkeit und Transparenz der Einwilligung	293
c) Schriftform und Information	293
d) Checkliste zur Einwilligung im Arbeitsverhältnis	295
e) Fazit	296
2. Ermöglichung und Ausübung der Beteiligungsrechte des Betriebsrats	296
3. Stellung des Betriebsrats	298
4. Kollektivvereinbarungen als Erlaubnistatbestand	299
a) Allgemeiner Regelungsrahmen von datenschutzrechtlichen Kollektivvereinbarungen	300
b) Schutzmaßnahmen	301
c) Typische Regelungspunkte in datenschutzrechtlichen Betriebsvereinbarungen	301
5. Beweisverwertungsverbote	304
a) Grundlagen	304
b) Bisherige Rechtsprechung zu Beweisverwertungsverboten	306
IV. Fazit	307
§ 11 Datenschutz in der Anwaltschaft	308
I. Einleitung	309
II. Bedeutung des Datenschutzrechts für die Anwaltschaft	310
III. Rechtlicher Regelungsrahmen	310
1. EU-Recht	310
2. Bundesrecht	311
IV. Datenverarbeitung innerhalb der Anwaltskanzlei	312
1. Erlaubnistatbestände für die Verarbeitung	312
2. Mandatsbezogene Daten	313
a) Daten bei Erstanfragen	313
b) Korrespondenz mit dem Mandanten und der Gegenseite	314
c) Handakte, Schriftsätze, Beweismittel	315
d) Notizen und andere Hilfsinformationen	315
e) Zeiterfassung, Rechnungsstellung und Honorardurchsetzung	316
3. Die zulässige Speicherdauer	317
4. Datenverarbeitung innerhalb verschiedener Organisationsformen	318
a) Bürogemeinschaften	318
b) Sozietät, Partnerschaft und GmbH	319
V. Datenverarbeitung außerhalb der Anwaltskanzlei	319
1. Non-legal Outsourcing	319
a) Reichweite des Geheimnisschutzes von § 203 StGB	320
b) Die strafrechtlich zulässige Einbeziehung Dritter	320

c) Die berufsrechtlichen Regelungen des § 43e BRAO	321
d) Die datenschutzrechtliche Bewertung	321
2. Legal Outsourcing	322
VI. Grenzüberschreitende Informationsverarbeitung	322
1. Die internationale Kanzlei	322
2. Das internationale Mandat	323
3. Der Geheimnisschutz im internationalen Kontext	323
VII. Datenschutzrechtliche Pflichten einer Anwaltskanzlei	324
1. Informationspflichten	324
a) Erhebung beim Betroffenen	324
b) Erhebung nicht beim Betroffenen	325
2. Auskunftspflichten	325
3. Melde- und Benachrichtigungspflichten	326
a) Meldepflichten gegenüber Aufsichtsbehörden	326
b) Benachrichtigungspflichten gegenüber Betroffenen	326
4. Pflichten hinsichtlich der Datenübertragbarkeit	326
5. Bestellung eines Datenschutzbeauftragten	327
a) Pflicht zur Bestellung gemäß § 38 Abs. 1 BDSG	327
b) Pflicht zur Bestellung gemäß Art. 37 Abs. 1 DS-GVO	328
c) Anforderungen an Datenschutzbeauftragte	330
d) Der Anwalt als Datenschutzbeauftragter	330
6. Sicherheit der Datenverarbeitung	331
a) Verschlüsselung	331
b) Stabilität	331
c) Wiederherstellbarkeit	332
d) Regelmäßige Überprüfung	332
7. Verarbeitungsverzeichnis	332
8. Folgenabschätzung	333
VIII. Kontrolle des Datenschutzes und Rechtsschutz	334
1. Zuständige Aufsichtsbehörde	334
2. Befugnisse der Aufsichtsbehörde	334
3. Rechtsmittel gegen Aufsichtsmaßnahmen	335
§ 12 Datenschutz in der Privatversicherung	336
I. Einleitung	337
II. Anwendbare Vorschriften	337
III. Einzelprobleme	339
1. Risikobeurteilung vor Vertragsschluss	339
a) Allgemeine Bonitätsprüfungen	339
b) Risikoeinschätzung hinsichtlich potentieller Versicherungsfälle	339
2. Bearbeitung von Versicherungsfällen	341
a) Abwicklung von Versicherungsfällen	341
b) Verhinderung und Aufklärung von Versicherungsbetrug	342
3. Datenaustausch mit anderen Versicherern sowie Versicherungsvertretern und -maklern	343
a) Vorversicherer	343
b) Rückversicherer	343
c) Versicherungsvermittler	344
4. Verarbeitung von Gesundheitsdaten	345
a) Gesetzliche Erlaubnistatbestände	345
b) Einwilligung und Entbindung von der Schweigepflicht	347
5. Smarte Versicherungstarife	353

a) Pay-as-you-drive	353
b) Pay-as-you-live	355
6. Outsourcing in der Versicherungswirtschaft	355
a) Datenschutzrechtliche Anforderungen	356
b) Anforderungen nach § 32 VAG und Art. 274 DVO (EU) Nr. 2015/35	357
c) Anforderungen nach § 203 StGB	358
7. Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft (Code of Conduct)	359
8. IT-Sicherheit und technische und organisatorische Maßnahmen	359
a) Datensicherheit	359
b) IT-Sicherheit	361
9. Sonstige Verarbeitung von Kundendaten	362
a) Beratung und Werbung	362
b) Bestandsübertragung	362
10. Aufsicht über Kranken-, Unfall- oder Lebensversicherer	363
§ 13 Datenschutz im Medizinsektor	365
I. Einleitung	366
II. Akteure und Datenkategorien im Gesundheitsbereich	367
1. Medizinsektor und Gesundheitswesen	367
2. Gesundheitsdaten und Gesundheitsverwaltungsdaten	367
3. Der Datenumgang im Gesundheitswesen	368
a) Datenumgang in der Arztpraxis	368
b) Datenumgang im Krankenhaus	368
c) Datenumgang im Pharmawesen	369
d) Datenumgang bei sonstigen Trägern von Heilberufen	369
4. Datenumgang bei gesetzlichen Krankenkassen und anderen Sozialversicherungsträgern	369
5. Sonderfall: Datenerhebung durch patienteneigene Geräte	369
6. Sonderfall: Auswertung von Gesundheitsdaten durch private IT-Dienstleister	369
a) Der Gesundheitsdatenmarkt	369
b) Big Data-Analysen zu wissenschaftlichen Zwecken	370
c) Das Interesse von Netzwerkbetreibern an Gesundheitsdaten	370
III. Rechtliche Rahmenbedingungen	370
1. Europäischer Normkontext für Gesundheitsdaten	371
2. Datenschutz-Grundverordnung	371
a) Verarbeitungsverbot für Gesundheitsdaten	371
b) Spielräume und Konkretisierungsmöglichkeiten für den nationalen Gesetzgeber	371
3. Grundrechtlicher Normenkontext und Gesetzgebungskompetenz	372
4. Bundesdatenschutzrechtliche Spezifizierung von Art. 9 DS-GVO	373
5. Bereichsspezifische Regelungen zum Schutz von Gesundheits- und Sozialdaten	374
a) Krankenkassen und Gesundheitsdatenschutz	374
b) Landesrecht: Datenschutz und Krankenhausgesetze	374
c) Kirchlicher Datenschutz	375
6. Übersicht über die anwendbaren Datenschutzvorschriften	375
7. Datenschutzrechtliche Spezialvorschriften	376
8. Straf- und zivilrechtliche Regelungen für den Medizinsektor	376
IV. Besondere Herausforderungen für den Datenschutz im Medizinsektor	376
1. Gesundheitsdaten als sensitive Daten	376

2.	Digitalisierung des Medizinsektors	377
3.	Rechtmäßige Verarbeitung von Gesundheitsdaten	377
	a) Der Grundsatz der Patientensouveränität	378
	b) Die Einwilligung im Gesundheitswesen	378
	c) Die „Interessenabwägung“ als Maßstab für die Datenverarbeitung	380
	d) Die Selbstdetermination durch Gesundheitsapps	380
4.	Übermittlung von Gesundheitsdaten	381
	a) Der Medizinsektor als notwendig vernetztes System von Leistungserbringern und weiteren Akteuren	381
	b) Rechtsgrundlagen für die Datenübermittlung	382
	c) Vernetzung als Chance und Risiko	382
5.	Sorgfaltspflichten bei der Verarbeitung von Gesundheitsdaten	383
6.	Datenspeicherung und Datenlöschung	384
7.	Die Betroffenenrechte im Medizinsektor	384
8.	Nicht-medizinische Akteure im Medizinsektor	385
V.	Sonderfragen zum Datenschutzrecht im Medizinsektor	385
	1. Der Patient im Mittelpunkt von Überwachungsmaßnahmen	385
	2. Das Datenschutzrecht von Leistungserbringern	386
	a) Sozialversicherungspflichtig Beschäftigte im Medizinsektor	386
	b) Arztbewertungen im Internet	386
	3. Praxisübernahme und Übernahme von Patientendaten	387
	a) Einwilligung der Patienten	388
	b) Das sog „Zwei-Schrank-Modell“	388
	c) Gemeinschaftspraxis/angestellter Arzt	388
VI.	Rechtsschutz	389
	1. Datenschutzaufsichtsbehörden	389
	2. Datenschutzrechtliche Kontroll- und Rechtsschutzinstrumente	389
	3. Straf- und zivilrechtliche Rechtsschutzinstrumente	389
§ 14	Datenschutz im Finanzwesen	391
	I. Einleitung	392
	II. Anwendbare Vorschriften und Einzelprobleme	392
	1. Das Bankgeheimnis	392
	2. Rechtsgrundlagen für Datenverarbeitung bei Bankgeschäften	394
	a) Einwilligung	394
	b) Interessenabwägung	395
	3. Rating und Bonitätsauskünfte	396
	4. Kredithandel und Risikosteuerung	396
	a) Forderungsabtretung	396
	b) Übertragung bei Kreditkonsortien und Verbriefungen	398
	c) Unterbeteiligungen und Kreditderivate	399
	5. Marktregulierung und Marktordnung im Kreditwesen	400
	a) Das Refinanzierungsregister	400
	b) Das Deckungsregister	402
	c) Das Kontenabrufverfahren	402
	6. Zahlungsverkehr	404
	7. Finanzmarkt und Finanzdienstleistungen, insbesondere Wertpapierhandel	407
	a) Bereichsspezifische Pflichten zur Datenerhebung	408
	b) Dokumentations- und Aufzeichnungspflichten, insbesondere Aufzeichnung von Telefongesprächen	408
	c) Weiterverwendung der Aufzeichnungen	410
	d) Ergänzende Anforderungen der DS-GVO	411

8. Bekämpfung von Geldwäsche und Terrorismusfinanzierung	412
a) Rechtsgrundlage im Sinne der DS-GVO	412
b) Identifizierung	413
c) Auskünfte an Behörden	414
d) Auslagerung von Sicherungsmaßnahmen	414
e) Die Geldtransfer-Verordnung	415
§ 15 Datenschutz in der Informationstechnik	418
I. Einleitung	419
II. Anwendbare Vorschriften	419
III. Einzelprobleme	420
1. Datenschutz durch Technikgestaltung	420
a) Grundsatz und Zielrichtung	420
b) Umsetzung in der Praxis	421
2. Technische Anforderungen an Datenminimierung und Speicherbeschränkung	424
a) Speicher- und Löschkonzepte	425
b) Löschung vs. Anonymisierung	427
3. Datenmanagement	428
a) Allgemeines	428
b) Datenqualitätsmanagement	428
c) Testdatenmanagement	430
4. Technische Anforderungen an Anonymisierung und Pseudonymisierung	432
a) Rechtliche Einordnung	433
b) Technische Anforderungen und Methodik	433
5. IT-Sicherheit und Datenschutz	440
6. Recht auf Datenportabilität	441
a) Bedeutung und Schutzrichtung	441
b) Voraussetzungen und Umfang des Anspruchs	442
c) Technische Anforderungen	444
d) Ausnahmen und Konflikte innerhalb der DS-GVO	445
e) Weitere Praxisempfehlungen	448
§ 16 Datenschutz im Automotive-Sektor	450
I. Einleitung	452
II. Rechtlicher Regelungsrahmen	452
1. Regulierungsebenen des Kfz-Datenschutzes	452
2. Abgrenzung zum TK-Datenschutz und Telemedien-Datenschutz	452
III. Datenschutzrechtliche Relevanz von Fahrzeugdaten	454
1. Datenhypertrophie in der Automobilwirtschaft	454
2. Bezug von Kfz-Daten zum Fahrzeughalter	455
a) Relevanz technischer Daten	455
b) Identifizierbarkeit des Fahrzeughalters	456
3. Weitere Betroffene	457
a) Fahrzeugeigentümer	457
b) Fahrzeugführer	458
c) Sonstige Verkehrsteilnehmer	458
IV. Adressaten der datenschutzrechtlichen Pflichten	459
1. Mögliche Verantwortliche	459
2. Unterscheidung zwischen Offline-Autos und Online-Autos	459
3. Gemeinsame Verantwortlichkeit	460
V. eCall	461

1. Einführung des eCall	461
2. Datenschutzrechtliche Implikationen	462
a) Notruffunktion	462
b) TPS-eCall und Zusatzdienste	463
VI. DS-GVO und Verarbeitung von Kfz-Daten	464
1. Gesetzlich erlaubte Datenverarbeitung	464
a) Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO)	464
b) Vertrag (Art. 6 Abs. 1 lit. b DS-GVO)	466
c) Berechtigte Interessen (Art. 6 Abs. 1 lit. f DS-GVO)	467
2. Technischer Datenschutz	469
a) Vermeidung personenbezogener Daten	469
b) Transparenz	471
c) Datensicherheit	473
VII. StVG-Novelle zum automatisierten Fahren	474
1. Einführung der Blackbox	474
2. Speicherpflicht (§ 63a Abs. 1 StVG)	474
a) Gesetzliche Regelung	474
b) Offene Fragen	475
3. Datenübermittlung (§ 63a Abs. 2, 3 StVG)	476
a) Übermittlung an Behörden	476
b) Übermittlung an Unfallbeteiligte	476
4. Löschung (§ 63a Abs. 4 StVG)	477
5. Ausblick	477
§ 17 Datenschutz im Energiesektor	479
I. Einleitung	480
II. Rechtlicher Regelungsrahmen	480
1. EU-Recht	480
a) DS-GVO	480
b) Binnenmarkttrichtlinien Strom und Gas	481
c) EnEff-RI	483
2. Bundesrecht	483
a) BDSG	483
b) MsbG	483
c) GPKE und GeLi Gas	486
III. Personenbezug von Messdaten und ableitbaren Daten	487
1. Notwendigkeit einer Differenzierung zwischen Einbau und Betrieb von Messsystemen	487
2. Begriff der personenbezogenen Daten	488
a) Bezug zu identifizierter natürlicher Person	488
b) Bezug zu identifizierbarer natürlicher Person	488
3. Personenbezug von Messdaten	491
a) Zuordnung zum Anschlussnutzer	491
b) Zuordnung zu Haushaltsmitgliedern	491
4. Personenbezug ableitbarer Daten	495
IV. Nebeneinander von DS-GVO und MsbG	496
1. Datenschutzrelevante Vorschriften des MsbG als zulässige Spezifikationen	496
a) Öffentliches Interesse	497
b) Begriff der Spezifizierung	498
c) VO-Konformität und Verhältnismäßigkeit der im MsbG enthaltenen datenschutzrelevanten Vorschriften	498

2. Zulässigkeit der Beschränkungen der Rechte der betroffenen Personen	502
a) Anschlussnutzer	502
b) Haushaltsangehörige	503
V. Rechtsschutz	504
§ 18 Datenschutz im Telekommunikationssektor	505
I. Einleitung	506
II. Anwendbare Vorschriften	506
III. Anwendbarkeit des TK-Datenschutzes	506
1. Verhältnis des TK-Datenschutzes zur DS-GVO	506
2. Abgrenzung des TK-Datenschutzes vom Telemedien-Datenschutz	509
IV. Durch den TK-Datenschutz Verpflichtete	510
V. Durch den TK-Datenschutz Geschützte	511
VI. Fernmeldegeheimnis	511
1. Adressat	511
2. Schutzzumfang	511
3. Geschützte des Fernmeldegeheimnisses	513
4. Pflichten aus dem Fernmeldegeheimnis	513
VII. TK-Datenschutz	513
1. Hintergrund des TK-Datenschutzes	513
2. Bestandsdaten	514
3. Verkehrsdaten	515
4. Standortdaten	516
5. Leitfaden zur datenschutzgerechten Speicherung von Verkehrsdaten ..	517
VIII. Datenspeicherung zur Missbrauchsbekämpfung	518
IX. Vorratsdatenspeicherung	519
1. Hintergrund und aktueller Stand der Vorratsdatenspeicherung	519
2. Verpflichtung zur Vorratsdatenspeicherung	519
3. Entscheidungen zur Vorratsdatenspeicherung	520
X. Outsourcing von TK-Leistungen	522
1. Outsourcing des Entgelteinzugs an Dritte	522
2. Outsourcing von Leistungen durch Dritte an TK-Anbieter	523
XI. Entwurf einer ePrivacy-VO	524
1. Anwendungsbereich der ePrivacy-VO E	524
2. Elektronische Kommunikationsdaten	525
3. Verarbeitung elektronischer Kommunikationsdaten	526
4. Datenlöschung	528
5. Einwilligung	528
6. Fernmeldegeheimnis	528
7. Outsourcing von TK-Leistungen	529
§ 19 Datenschutz in Presse und anderen Medien	530
I. Einleitung	532
II. Anwendbare Vorschriften	533
1. Datenschutzrecht in der EMRK	533
2. Datenschutzrecht auf unionaler Ebene	534
a) GRCh	534
b) AEUV	534
c) DS-GVO	534
d) Bisherige sekundärrechtliche Regelung in der DS-RL	535
3. Datenschutzrecht auf nationaler Ebene	535
a) Verfassungsrecht	535
b) Einfachgesetzliches Bundesrecht	536

c) Staatsverträge	537
d) Sonstiges Landesrecht	538
III. Einzelfragen	538
1. Presse und andere (Tele-)Medien	538
a) Presse	538
b) Rundfunk sowie Telemedien mit journalistisch-redaktionellen Inhalten	539
c) Neuere Erscheinungsformen	540
2. Datenschutzrechtliche Medienprivilegien	541
a) Unionsrechtliche Vorgaben	542
b) Nationale Ebene	545
3. Betroffenenrechte	550
a) Rundfunk	550
b) Telemedien mit journalistisch-redaktionellen Inhalten	551
c) Presse	552
4. Aufsicht	552
a) Rundfunk	552
b) Telemedien mit journalistisch-redaktionellem Inhalt	554
c) Presse	554
5. Sanktionen	554
6. Online-Archive	555
a) Stand der europäischen und nationalen Rechtsprechung	555
b) Insbesondere: Die Löschung von personenbezogenen Daten nach der DS-GVO	557
7. Rechtsschutz	558
IV. Fazit	558

Teil C. Datenschutzrecht im öffentlichen Sektor

§ 20 Datenschutz in der Verwaltung von Bund, Ländern und Kommunen ...	559
I. Einleitung	560
II. Anwendbare Vorschriften	562
1. Anwendung der DS-GVO auf die Datenverarbeitung der Verwaltung	563
2. Anwendung der JI-RL im Kontext der Datenverarbeitung öffentlicher Stellen	564
3. Die Anwendung des BDSG auf die Datenverarbeitung der Verwaltung	565
4. Besonderes Bundesrecht betreffend die Datenverarbeitung öffentlicher Stellen	566
5. Landesrechtliche Regelungen im Datenschutzrecht	568
III. Einzelfragen	569
1. Rechtsgrundlagen für die Datenverarbeitung in der Verwaltung	569
a) Die Einwilligung in Datenverarbeitungen öffentlicher Stellen	570
b) Verarbeitung personenbezogener Daten durch öffentliche Stellen im öffentlichen Interesse und zur Erfüllung öffentlicher Aufgaben	571
c) Zweckbindung und Verarbeitung zu kompatiblen Zwecke	572
d) Verarbeitung besonderer Kategorien personenbezogener Daten	574
e) Datenübermittlungen an öffentliche und nicht-öffentliche Stellen ..	576
2. Videoüberwachung bei und durch öffentliche Stellen	579
3. Einlasskontrollen	581
4. Informations- und Auskunftspflichten	582
5. Die digitale Organisation der Verwaltung	584

a) Rollen und Verantwortlichkeiten	584
b) Auftragsverarbeitung im Bereich der Verwaltung	585
6. Einsatz zertifizierter Produkte, Verfahren und Dienstleistungen – Ausschreibung und Vergabe	586
7. Einzelfragen der IT-gestützten Verwaltung	587
a) Zentralisierung der IT und gemeinsame Nutzung	587
b) Kommunikation mit Bürgerinnen und Externen via E-Mail	588
8. Open Data und Informationsfreiheit	589
9. Öffentlichkeits- und Pressearbeit der Verwaltung	590
a) Die fehlende Umsetzung des Art. 85 DS-GVO	590
b) Social Media-Nutzung durch öffentliche Stellen	591
10. Die behördliche Datenschutzbeauftragte	592
a) Benennung	593
b) Aufgaben, Rechte und Pflichten	594
c) Beteiligung und Mitwirkung bei Datenschutz-Folgenabschätzungen	595
11. Aufsichtsbehördliche Kontrolle der Verwaltung	596
IV. Fazit	598
§ 21 Datenschutz und präventive Tätigkeit der Polizei	599
I. Einleitung	600
II. Anwendbare Vorschriften	601
1. Bereichsspezifisches Datenschutzrecht im Polizeirecht	601
2. Europäische Einflüsse – JI-RL und DS-GVO	601
a) Die JI-RL	601
b) Abgrenzung der Anwendungsbereiche JI-RL/DS-GVO	601
c) Vorgaben zur Rechtmäßigkeit der Datenverarbeitung	603
d) Verarbeitung aufgrund von Einwilligung	603
e) Datenschutzfreundliche Technikgestaltung	604
f) Datenschutzfolgenabschätzung	604
g) Informationspflichten und Auskunftsrecht	604
h) Umsetzungs- und Anpassungsaktivitäten	604
III. Ausgewählte Einzelfragen	605
1. Erhebung	605
a) Datenerhebungsgeneralklausel	605
b) Identitätsfeststellung	605
c) Online-Streife	607
d) Verdeckte Datenerhebung	607
e) Einsatz von Videokameras	612
2. Speicherung, Veränderung und Nutzung	615
a) Grundsätze	615
b) Erfordernis rechtmäßiger Datenerhebung?	615
c) Zweck Aufgabenerfüllung	615
d) Zweckänderungen	616
3. Übermittlung	617
a) Datenübermittlungen zwischen Polizeibehörden	617
b) Datenübermittlungen an ausländische Polizeibehörden	617
c) Datenübermittlungen an öffentliche Stellen	618
d) Datenübermittlungen an nicht-öffentliche Stellen	619
3. Betroffenenrechte	620
a) Informationspflichten und Benachrichtigung	620
b) Auskunft	621

c) Berichtigung	622
d) Löschung	622
IV. Ausblick	622
§ 22 Datenschutz in der Justiz	623
I. Einleitung	623
II. Anwendbare Vorschriften	624
1. Anwendung der DS-GVO auf die Datenverarbeitung der Justiz	625
2. Anwendung JI-Richtlinie auf justizielle Datenverarbeitung	625
3. Konkretisierung der DS-GVO für den Bereich der Justiz durch die Mitgliedstaaten	627
a) Nationales Sonderrecht für die Datenverarbeitung der Justiz	628
b) Die Regelungen des neuen BDSG hinsichtlich der Datenverarbeitung der Justiz	628
c) Landesrechtliche Vorgaben hinsichtlich der Datenverarbeitung der Justiz	629
III. Einzelfragen	630
1. Datenschutzrechtliche Verantwortlichkeit in der Justiz	630
a) Selbständige Verantwortlichkeit	630
b) Gemeinsame Verantwortlichkeit	632
c) Verantwortlichkeit für justiznahe Auftragsverarbeiter	633
2. Der Erforderlichkeitsgrundsatz in der Justiz	634
3. Betroffenenrechte im Rahmen der justiziellen Datenverarbeitung	636
a) Justizielle Transparenzpflichten nach der DS-GVO	636
b) Akteneinsichtsrechte nach dem Prozessrecht	639
c) Konkurrenz der Transparenzpflichten	639
4. Datenschutz und eJustice	639
a) Datenschutz bei der elektronischen Aktenführung	640
b) Datenschutz im elektronischen Rechtsverkehr	641
5. Der justizielle Datenschutzbeauftragte	642
6. Aufsichtsbehördliche Kontrolle und Selbstkontrolle der Justiz	643
7. Justizielle Unabhängigkeit und Zentralisierung der Datenverarbeitung	644
IV. Ausblick	645
§ 23 Datenschutz in Forschung und Hochschullehre	646
I. Einleitung	647
II. Forschung	649
1. Anwendbare Vorschriften	649
2. Einzelprobleme	650
a) Begriff der Forschung	650
b) Erlaubnistatbestände zur Datenverarbeitung	651
c) Geeignete Garantien und technische und organisatorische Maßnahmen	658
d) Sonderregelungen zu den Verarbeitungsgrundsätzen (Art. 5 Abs. 1 DS-GVO)	660
e) Sonderregelungen zu Betroffenenrechten	661
III. Lehre an Hochschulen	664
1. Anwendbare Vorschriften	665
2. Einzelprobleme	665
a) Erlaubnistatbestände zur Datenverarbeitung	665
b) Ausgewählte Aspekte der Hochschullehre	667
IV. Fazit	670

§ 24 Datenschutz in Schule und Schulverwaltung	672
I. Einleitung	673
II. Rechtsquellen des schulischen Datenschutzes	674
1. DS-GVO	674
2. Ermächtigungen und Konkretisierungen im Landesrecht	676
III. Schwerpunkte des Schuldatenschutzes	679
1. Die betroffenen Personen	679
a) Schüler	680
b) Eltern/Erziehungsberechtigte	680
c) Lehrer	680
d) Schulleiter	680
e) Mitarbeiter der Schulverwaltung	680
2. Sachlicher Schutzzumfang	681
a) Besondere persönliche Merkmale	681
b) Identifizierbarkeit	681
c) Profiling	682
3. Der Verantwortliche	683
a) Entscheidungsgewalt und fachaufsichtliche Weisungen	683
b) Entscheidungsbefugnis	684
c) Übertragung der datenschutzrechtlichen Verantwortlichkeit auf den Schulleiter	684
d) Transparenz	684
4. Die Einwilligung	684
a) Allgemeine Anforderungen an die Einwilligung	685
b) Freiwilligkeit	685
c) Einwilligung im Einzelfall (Zweckbezogenheit)	686
d) Form der Einwilligung	687
e) Einwilligungen bei Minderjährigen	687
5. Bedeutung der Datenschutzfolgenabschätzung für die Noten- und Zeugnisverwaltung	689
6. Auftragsdatenverarbeitung im schulischen Umfeld (insbes. Nutzung von Online-Diensten, Webanwendungen, Cloud-Diensten)	689
7. Schulwebsite	690
8. Datenschutzbeauftragter an Schulen	691
9. Vergleichsarbeiten (Lernstandserhebungen)	692
10. Datengestütztes Bildungsmonitoring	695
11. Datenschutzrechtliche Fragen bei der Schulbuchzulassung	695
12. Elektronisches Klassenbuch	695
13. Tablet-Klassen	695
14. Dienstgeräte von Lehrern	696
15. Lern-Apps	696
IV. Aufsicht, Maßnahmen und Rechtsschutz	697
1. Aufsicht	697
2. Rechte der Schüler	697
3. Rechte der Lehrer (insbes. Remonstration)	698
4. Haftungsfragen (insbes. Grad der Verantwortung des Verantwortlichen)	698
§ 25 Datenschutz in Kultureinrichtungen, Bibliotheken und Archiven	699
I. Einleitung	699
II. Rechtsgrundlagen	700
1. EU-Recht	701

2. Bundesrecht	702
3. Landesrecht	702
III. Bestandsdatenschutz in Archiven und Bibliotheken	703
1. Sammeln	704
2. Erschließen	707
3. Zugänglichmachen	709
IV. Nutzerdatenschutz in Archiven und Bibliotheken	710
1. Zulassung zur Benutzung	710
2. Erfassung von Benutzungsvorgängen	712
V. Datenschutz in anderen Kultureinrichtungen	715
VI. Datenschutz im Denkmalschutz	716
VII. Rechtsschutz	716
§ 26 Sozialdatenschutz	718
I. Einleitung	719
II. Bedeutung und Entwicklung des Sozialdatenschutzes	719
1. Ausgestaltung als Vollregelung	720
2. Abgrenzungsfragen und Systematik im Sozialdatenschutz	720
a) Systematik innerhalb des SGB	720
b) Abgrenzung zu anderen nationalen Datenschutzvorschriften	721
c) Sozialdatenschutz und europäisches Recht	721
III. Sozialgeheimnis	723
1. Sozialdatum	724
2. Leistungsträger	725
IV. Allgemeine sozialgesetzliche Datenverarbeitungsmodalitäten und Begriffsbestimmungen	726
1. Anwendungsbereich	727
2. Allgemeine Grundsätze: §§ 67 ff. SGB X	727
a) Erhebung von Sozialdaten	728
b) Sonstige Verarbeitungsmodalitäten	731
c) Übermittlung von Sozialdaten: §§ 67 d – 77 SGB X	732
d) Besondere Datenverarbeitungsarten	738
e) Betroffenenrechte, Datenschutzkontrolle	739
f) Sanktionierung von Datenschutzverstößen	743
V. Der bereichsspezifische Schutz von Sozialdaten	744
1. Grundsicherung für Arbeitsuchende (§§ 50–52 SGB II)	745
2. Arbeitsförderung (§§ 394–397 SGB III)	749
3. Sozialversicherung (§§ 18 f, 18 g SGB IV)	750
4. Gesetzliche Krankenversicherung/GKV (§§ 284–305 SGB V)	751
5. Gesetzliche Rentenversicherung (§§ 145–152 SGB VI)	756
6. Gesetzliche Unfallversicherung (§§ 199–208 SGB VII)	757
7. Kinder- und Jugendhilfe (§§ 61–68 SGB VIII)	758
8. Soziale Pflegeversicherung (§§ 93–109 SGB XI)	759
VI. Rechtsschutz	759
§ 27 Kirchliches Datenschutzrecht	762
I. Einleitung	762
II. Religionsgemeinschaftliches Selbstbestimmungsrecht	763
III. Rechtlicher Regelungsrahmen	763
1. Die DS-GVO im Lichte des religionsgemeinschaftlichen Selbstbestimmungsrechts	763
2. Gesetz über den Kirchlichen Datenschutz der römisch-katholischen Kirche in Deutschland (KDG)	764

3. Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)	765
4. Spezialgesetzliche staatliche Datenschutzregelungen	765
IV. Sonderfragen zum kirchlichen Datenschutzrecht	765
1. Datenschutz bei kirchlichen Dienst- und Arbeitsverhältnissen	765
2. Videoüberwachung in Kirchen und die Aufzeichnungen und Übertragungen von Gottesdiensten und kirchlichen Veranstaltungen ..	766
V. Rechtsschutz	766
1. Betroffenenrechte	766
2. Recht auf Beschwerde	766
3. (Kirchen-)Gerichtliche Rechtsbehelfe	767
4. Schadensersatz	767
5. Sanktionen	767
Sachverzeichnis	769



beck-shop.de
DIE FACHBUCHHANDLUNG