

Inhaltsverzeichnis

	Seite
Vorwort	V
Abkürzungsverzeichnis	XXIII
Literaturverzeichnis	XXXI

§ 1. Einführung	1
A. Kommunikationstechnische Entwicklungsstufen	1
B. Das hergebrachte/fortwirkende deutsche Konzept	1
C. Europäische Rechtsentwicklung	3
D. Zur Gesamtdarstellung	4

1. Teil. Grundlagen

1. Abschnitt. Historisch-gesellschaftliche und sozialwissenschaftliche Orientierung

§ 2. Rechtsgeschichte des Datenschutzes	7
A. Vormoderne	8
I. Antike	9
1. Antike Hochkulturen	9
2. Altes Testament	9
3. Griechenland	9
4. Rom	9
II. Mittelalter	10
B. Frühe Neuzeit	10
I. Bürokratisierung	10
II. Faktische Grenzen	11
III. Entdeckung des Persönlichkeitsrechts	11
C. Frühes technisches und bürokratisches Zeitalter (1800–1945)	11
I. Fortschreiten der Bürokratisierung	11
II. Berufrechtliche Verschwiegenheitspflichten	12
III. Beginn privater Datenmacht	12
IV. Anfänge der Telekommunikation	13
D. Nationalsozialistische Zeit	13
E. Nachkriegszeit	14
I. Verwaltung und Sicherheitsbehörden	14
II. Vergrößerung privater Datenmacht	15
III. Entwicklung des Persönlichkeitsrechts in der Rechtsprechung	15
Exkurs: Datenschutz in der DDR	16
1. Ausschließlich staatliche Datenmacht	16
2. Verfassungsrechtliche und einfachgesetzliche Regelungen	17
3. Begriff und Bedeutung des „Datenschutzes“ in der DDR	17
F. Erste Datenschutzgesetze und Volkszählungsurteil	18
I. Vorfeld	18
1. Staat als „Großer Bruder“	18
2. Nicht-öffentlicher Bereich	19

3. Begriff des „Datenschutzrechts“	19
II. Erste Datenschutzgesetze	20
1. Hessisches Datenschutzgesetz von 1970	21
2. Bundesdatenschutzgesetz	21
III. Volkszählungsurteil	22
IV. BDSG 1990 und verfassungsgerichtliche Konturierung	23
V. BDSG-Reformen I, II, III im Jahre 2009	23
G. Datenschutz und Vernetzung	23
I. Telekommunikationsdatenschutz	23
II. Internet	24
H. Europäisierung des Datenschutzrechts	25
I. Europarechtliche Regelungen	26
II. Europäische Rechtsprechung	26
III. Weiterentwicklung des europäischen Rechtsrahmens für den Datenschutz	27
IV. Das BDSG 2018	27
V. Corona-Pandemie	28
§ 3. Leitlinien für den Datenschutz auf informations- und kommunika- tionstheoretischer Grundlage	30
A. Ausgangslage	30
I. Neue Anforderungen	30
II. Informationelle Selbstbestimmung im deutschen Recht	31
III. Personenbezug und Gesellschaft	33
IV. Informationeller „Start“ für das BDSG	33
B. Das Konzept Information	34
I. Entwicklung in neuer Zeit (20. Jahrhundert)	34
II. Information und Kommunikation bei Luhmann	36
III. Information in Sozial- und Rechtswissenschaft	38
1. Kritischer Ansatz bei Albers	38
2. Information im Verwaltungsverfahren und nach IFG	40
3. Folgerung	40
IV. Soziale Vernetzung	41
C. Perspektiven	41
2. Abschnitt. Verfassungsrechtliche Basis in der Bundesrepublik Deutschland	
§ 4. Grundrechtliche Gewährleistung des Datenschutzes – Probleme, Lösungsansätze, Alternativen	43
A. Ausgangslage	43
B. Generalisierender Schutz personenbezogener Informationen	44
C. Sozialcharakter der – personenbezogenen – Information	46
I. Zur Rechtsprechung des BVerfG	46
II. Eingrenzung informationellen Persönlichkeitsschutzes	47
1. Geheimnisse	47
2. Probleme informationeller Zuordnung	48
3. Folgerung	48
D. Privatheit (nebst Intimität) insbesondere	49
E. Grundrechtliche Bedeutung des Persönlichkeitsschutzes und des Rechts auf informationelle Selbstbestimmung im nicht-öffentlichen Bereich (Drittwirkung)	50

I. Persönlichkeitsrecht	50
II. Das Recht auf informationelle Selbstbestimmung insbesondere	52
III. Systematische Folgerungen	54
IV. Weiterreichende verfassungsrechtliche Fragen	55
§ 5. Ausgewählte Probleme des Datenschutzes gemäß Rechtsprechung des BVerfG	57
A. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	58
I. Schutzbereich	58
II. Eingriffe/Schranken	59
III. Parallelen zu anderen Gewährleistungen des Persönlichkeitsbereichs	60
IV. Erweiterte Bedeutung des GRaGVliS	60
V. Abgrenzung zum Recht auf informationelle Selbstbestimmung	61
1. Begründung des BVerfG und Kritik	61
2. Wesentliche Unterscheidung	62
3. Perspektivenwechsel	62
B. Schutz des (unantastbaren) Kernbereichs privater Lebensgestaltung	64
I. Entwicklung	64
II. Neu ausgeprägter Kernbereich	65
III. „Unantastbarkeit“	67
1. Problemstellung	67
2. Herkömmliche Regeln	67
3. Unantastbarkeit im Grundgesetz	68
a) Grundlagen	68
b) Leitlinien in der Rechtsprechung des BVerfG zu Art. 1 Abs. 1 GG	69
c) Einschränkungen der Menschenwürde systematisch betrachtet	70
4. Praktische Ergebnisse für den Kernbereich privater Lebensgestaltung	71
IV. Zweistufiges Kontrollverfahren insbesondere	72
1. Erste Stufe: Abgrenzung im Echtzeit-(Live)Verfahren	72
2. Zweite Stufe: Einschaltung eines Unabhängigen	73
C. Automatisierter Datenabgleich, auch „Rasterfahndung“	75
I. Bedeutung für die Praxis und für das grundrechtliche Verständnis	75
II. (Kein) Grundrechtseingriff bei Nichttreffern?	76
III. Kritische Prüfung der (Nicht-)Eingriffsthese	77
1. Breit angelegte Überwachung?	77
2. Involvierte Daten und/oder personenbezogene Informationen?	78
3. Eingriffsauslösende Qualität des Betroffenseins	78
4. Eingeschlossene Übermittlungsvorgänge	79
5. Hohe Einschreitschwelle?	80
IV. Ausblick	81
D. „Vorratsdatenspeicherung“	82
I. Entwicklung bis hin zu einer Entscheidung des BVerfG	82

II. Die weitere Entwicklung – geprägt durch Urteile des EuGH	83
III. Anzuwendender Grundrechtsschutz	85
IV. Bisherige staatlich verordnete anlasslose Speicherungen	86
V. Das Metadaten-Register: Speicherung/Nutzung, Datensicherung	88
VI. Neue gesetzliche Regelung/verbleibende Bedenken	89

3. Abschnitt. Europarechtliche (primärrechtliche) Basis

§ 6. Art. 8 EMRK in Anwendung auf personenbezogene Informationen durch den EGMR	92
A. Ausgangspunkt: Privatleben i. w. S.	92
B. Beruf, Wirtschaft	93
C. Besondere Arten personenbezogener Informationen	94
D. Öffentlichkeit	95
E. Persönlichkeitsschutz	97
§ 7. Grundrechtliche Gewährleistungen in der EU	98
A. Rechtlicher Rahmen	98
I. Rechtsetzungskompetenz der EU	98
II. Grundrechtlicher Gewährleistungsbereich in der EU und Auswirkung auf die Anwendbarkeit der Grundrechte der Mitgliedstaaten	99
B. Der vor Inkrafttreten der GRCh gewährleistete Schutz	100
I. Persönlichkeitsschutz und Transparenz bei der öffentlichen Hand	100
1. Namen(sliste) von Lobbyisten	100
2. Parlamentarische Aktivitäten	102
II. Persönlichkeitsschutz und Transparenz individueller wirtschaftlicher Verhältnisse	102
1. Überblick zu Einkünften	102
2. Steuergeheimnis in Deutschland	103
3. Einkünfte, Vermögen, Steuern: Transparenz in Europa	104
C. Von der GRCh gewährleisteter Schutz	107
I. Systematik	107
II. Rechtsprechung des EuGH	108
III. Zur weiteren Interpretation des Art. 8 GRCh	110
1. Entstehung der Charta-Bestimmung	110
2. Verfassung(süberlieferung)en der Mitgliedstaaten	110
IV. Folgerungen	111

2. Teil. Harmonisiertes europäisches Datenschutzrecht nach DS-GVO

1. Abschnitt. Geltungsbereich der DS-GVO

§ 8. Sachlicher Geltungsbereich (Art. 2 DS-GVO)	114
A. Rechtssystematische Eingrenzungen	114
I. Grundregeln	114
II. Abgrenzung zum Geltungsbereich der JI-RL und deren Umsetzung im BDSG	114
III. „Öffentlicher Bereich“	116

1. Unterscheidung zwischen öffentlichem und nicht-öffentlichem Bereich	116
2. Deutsche Ausgestaltung im öffentlichen Bereich	116
3. Innerstaatliche Gesetzgebungskompetenzen	117
a) Öffentlicher Bereich	118
b) Nicht-öffentlicher Bereich	119
B. Eingrenzungen von der Sache her	119
I. Technik der Informationsverarbeitung	119
1. Automatisierte Verarbeitung	119
2. Nichtautomatisierte Verarbeitung im „Dateisystem“	120
a) Begriffliches	120
b) Zielsetzung	120
c) Akten insbesondere	121
II. Persönliche oder familiäre Tätigkeiten	122
C. Besonders geregelte Bereiche	124
I. Unionsrecht	124
II. Mitgliedstaatliches Recht	125
1. Nicht-öffentlicher Bereich	125
2. Öffentlicher Bereich	126
a) Bereichsspezifisches Recht und Subsidiarität des allgemeinen Datenschutzrechts	126
b) „Deckungsgleichheit“	127
D. Selbstregulierungsregelungen	127
§ 9. Räumlicher Anwendungsbereich. Datenschutzkollisionsrecht	129
A. Problemstellung des Internationalen Datenschutzrechts	129
B. Räumlicher Anwendungsbereich	129
I. Niederlassung	129
II. Marktort	130
III. Erfolgte Drittlandübermittlung?	131
IV. Diplomatische Vertretungen. Schiffe und Flugzeuge	131
C. Beschränkung grenzüberschreitender Datenübermittlung	131
I. Keine Beschränkungen innerhalb des Binnenmarkts	132
II. Keine Datenimportbeschränkungen	132
III. Datenexportbeschränkungen	132
1. Angemessenheitsentscheidung	133
2. Geeignete Garantien	133
3. Informationelle Amts- und Rechtshilfe. Registerauskunft	134
4. Situative Ausnahmen	134
IV. Keine Datenlokalisierung	134
D. Kollision von Datenschutzrechtsordnungen	135
E. Internationale Datenschutzharmonisierung	136
 2. Abschnitt. Rechtlich vorgegebene Grundstruktur für die Verarbeitung personenbezogener Informationen	
§ 10. Betroffene. Personenbezogene Informationen	137
A. Einführung	137
B. Personenbezogene Informationen (Merkmale)	138
C. Mehrfacher bzw. eingeschränkter Personenbezug	140

I. Grundmodell	140
II. Gesteuerter Personenbezug	141
III. Sachdaten. Geodaten	143
D. Identifizierte oder identifizierbare Betroffene	144
I. Die Einzelnen im Fokus	144
II. Die Bedeutung des informationellen Umfelds	145
III. Zusatzwissen im rechtlichen Rahmen	146
IV. Zusatzwissen Dritter	147
1. Relativer/absoluter Personenbezug	147
2. Dynamische IP-Adresse als personenbezogenes Datum?	148
V. Abstufung zwischen identifizierten und identifizierbaren Betroffenen	149
1. Pseudonymität	149
2. Eingeschränkte Anwendung datenschutzrechtlicher Bestimmungen gemäß Art. 11 DS-GVO	150
E. Zusammenfassung, Ausblick	152
§ 11. Verantwortliche und andere im Rahmen der Verarbeitung mitwirkende Stellen	153
A. „Verantwortlicher“	153
B. Beschäftigte	154
C. „Auftragsverarbeiter“	154
I. Rechtliche Grundlagen	154
II. Anwendungen	156
D. „Gemeinsam Verantwortliche“ (Art. 26 DS-GVO)	157
I. Vorangegangene Regelungen gemeinsamer Verantwortlichkeit	157
II. Inhalt und Ausprägungen gemeinsamer Verantwortlichkeit	157
III. Besondere Verarbeitungskonstellationen im Internet	159
IV. Telemediendienste (Hostprovider/Portale), Nutzer und Betroffene	160
V. Résumé	161
1. Öffnung zu neuem Lösungsweg	161
2. Hemmnisse?	162
E. Unterstellte Person	163
F. Dritte und Empfänger	163
§ 12. Rechtsgrundlagen der Verarbeitung	165
A. Datenschutzrechtlicher Regelungsansatz in der DS-GVO	165
B. Informationsverarbeitung auf gesetzlicher Grundlage (Art. 6 Abs. 1 lit. b–f DS-GVO)	166
I. Vertragsrechtliche Beziehungen	166
II. Erfüllung von Rechtspflichten	166
III. Wahrnehmung öffentlicher Aufgaben	167
IV. Wahrung berechtigter Interessen Privater	168
V. Schutz lebenswichtiger Interessen	170
C. Erforderlichkeit/Verhältnismäßigkeit	170
I. Kausalzusammenhang?	171
II. Diskrepanzen der Interpretation	172
III. Erforderlichkeit/Verhältnismäßigkeit im (alten) Polizeirecht	173
IV. Rechtsprechungspraxis	175

V. Ausgewählte Folgerungen	178
1. Vertragsverhältnis	178
2. Verbundene Unternehmen	178
3. Öffentliche Verwaltung	179
D. Zweckbindung	179
§ 13. Einwilligung und andere Willensäußerungen	182
A. Willensäußerungen im Datenschutzrecht	182
I. Rechtsnatur	183
1. Datenschutzrechtliche Einordnung	183
2. Zivilrechtliche Einordnung	183
a) Mitgliedstaatliche oder europäische Rechtsgeschäfts- lehre?	183
b) Willenserklärung oder Realakt?	184
3. Kein Grundrechtsverzicht	185
II. Begrifflichkeit	186
1. Legaldefinitionen, Gesetzesbegriffe und Lücken	186
2. Umfassende Nomenklatur	187
III. (Kommendes) Datenrecht?	188
B. Allgemeine Anforderungen an Willensäußerungen	188
I. Modi der Willensäußerung	188
II. Freiwilligkeit	190
1. Grenzen des willensäußerungsbasierten Konzepts	190
a) Macht- und Wissensasymmetrien	190
b) Rationale Apathie	191
c) Individualität der Willensäußerung und soziale Aspekte von Datenverarbeitung	192
2. Asymmetrien und Abhängigkeitsverhältnisse	193
3. Kopplungsverbote	193
4. Einwilligungsverbot und Unbeachtlichkeit der Willens- äußerung	194
III. Willensäußerungen von Minderjährigen und beschränkt Geschäftsfähigen	195
1. Allgemeine Einsichtsfähigkeit und typische Altersgrenzen ...	195
2. Datenschutzrechtliche Rechtsgeschäftsfähigkeit	196
IV. Spezialgesetzliche Regelungen und mitgliedstaatliche Abweichungsmöglichkeiten	198
C. Datenschutzrechtliche Willenserklärungen	198
I. Einwilligung	198
1. Informiertheit und Transparenz	199
a) Vorangehende Unterrichtung	199
b) Vorangehende Belehrung	199
c) Verständlichkeit und Zugänglichkeit	200
2. Bestimmtheit	200
3. Form	201
a) Grundsatz der Formfreiheit	201
b) Formvorgaben	201
aa) AGB	201
bb) Ausdrücklichkeit bei sensiblen und Gesund- heitsdaten	202

cc) Ausdrücklichkeit bei automatisierten Einzelentscheidungen	203
dd) Schriftform bei Einwilligungen im Beschäftigungsverhältnis	203
c) Nachweisbarkeit	203
4. Rechtswirkungen	203
a) Konstitutiver Erlaubnistatbestand	203
b) Zeitpunkt und Wirksamkeitsdauer	204
c) Folgen ungenügender Einwilligung	204
II. Widerspruch	205
1. Transparenz als Voraussetzung	205
2. Bestimmtheit	205
3. Formfreiheit	205
4. Rechtswirkungen	206
III. Widerruf von Einwilligung und Widerspruch	207
1. Beschränkungen und Bedingungen	207
2. Informiertheit	208
3. Bestimmtheit	208
4. Formfreiheit	208
5. Rechtswirkungen	208
a) Rückgriff auf gesetzliche Erlaubnisnormen	208
b) Rückwirkung auf Vertragsverhältnisse	208
6. Verhältnis zur Anfechtung	209
IV. Stellvertretung	209
1. Gewillkürte Vertretung	209
2. Gesetzliche Vertretung, Minderjährige	210
3. Einwilligungsmanagementsysteme	211
V. Genehmigung	211
VI. Verzicht auf Betroffenenrechte	211
VII. Verhältnis datenschutzrechtlicher Ansprüche zur Unwirksamkeit des Rechtsgeschäfts	212
D. Bloße Willensäußerungen im Datenschutzrecht	212
I. Formfreiheit von Einverständnis und Einwand	213
II. Kenntnis des Verantwortlichen	213
III. Wegfall des Einverständnisses und des Einwands	213
IV. „Vertretung“ und „Genehmigung“ bei Einverständnis und Einwand	213
§ 14. Datenklassen	214
A. Allgemein zugängliche Quellen	214
B. Äußerer Umgang/Kontakt einerseits und Inhalte andererseits	215
C. Wirtschafts- und Finanzinformationen	216
D. Verarbeitung „besonderer Kategorien personenbezogener Daten“ (sensitive Information)	217
I. Normative Grundlagen	217
II. Rückschlussproblematik bei doppelunktionalen Daten	217
E. Personenkenneichen	219
§ 15. Informationspflichten und Betroffenenrechte	221
A. Informationsfluss vom Verantwortlichen zum Betroffenen	221

I. Regelmäßige Informationspflichten des Verantwortlichen	221
1. Die Pflichten im einzelnen	221
2. Einschränkungen der Informationspflicht	223
a) Fälle nachträglicher Zweckänderung	223
b) Fälle der Erhebung nicht beim Betroffenen	223
aa) DS-GVO	223
bb) BDSG	224
c) Übersicht	225
3. Data Breach Notification	225
4. Wertung	226
II. Auskunftsrecht des Betroffenen	226
1. Grundlagen	226
2. Charakteristika der Auskunftspflicht	227
3. Einschränkungen des Rechts auf Auskunftserteilung	228
a) DS-GVO	228
b) BDSG	229
III. Datenportabilität	229
B. Interventionsrechte des Betroffenen	231
I. Berichtigung	231
II. Löschung	232
1. Systematik	232
2. Information an Dritte	232
III. Einschränkung der Verarbeitung (Sperrung)	233
C. Verbraucherschutzrechte	234

3. Abschnitt. Steuerung riskanter Verfahren

§ 16. Automatisierte Einzelentscheidung. KI-Systeme	237
A. Automatisierte Entscheidung im Einzelfall	238
I. Begriff	238
1. Automatisierte Verarbeitung	239
3. Ausschließlichkeit der automatisierten Verarbeitung	239
2. Rechtliche Wirkung und erhebliche Beeinträchtigung	240
II. Verbot der Automatisierten Entscheidung im Einzelfall	241
III. Ausnahmen vom Verbot der Automatisierten Einzelent-	
scheidung	241
1. Tatbestand der Ausnahmen (Abs. 2)	241
2. Schutz der Rechte der betroffenen Personen (Abs. 3)	242
3. Ausschluss besonderer Kategorien personenbezogener	
Daten (Abs. 4)	243
4. Einschränkung nach Art. 23 DS-GVO	243
IV. Informationspflichten in Bezug auf die Automatisierte Einzel-	
entscheidung	244
B. Profiling	245
I. Zulässigkeit des Profiling	246
II. Transparenz in Bezug auf das Profiling	246
III. Profiling zur Direktwerbung	247
C. Scoring nach dem BDSG	248
D. Künstliche Intelligenz	249
I. Das Phänomen KI	249

II. Anforderungen der DS-GVO an KI-Systeme	251
1. Keine direkte KI-Regulierung in Art. 22 DS-GVO	251
2. Indirekte Regelungen in der DS-GVO	252
III. KI-Bezogene Regelungen außerhalb der DS-GVO	252
IV. AI Act und Digital Services Act	253
1. KI-Verordnung (KI-VO-E)	254
2. Digital Services Act (DSA-E)	256
§ 17. Verzeichnis von Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung, Vorherige Konsultation	258
A. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)	258
I. Überblick	259
II. Regelung in der DS-GVO	260
1. Verpflichtung zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten	260
2. Gegenstand und Inhalt des Verzeichnisses	260
a) Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen	260
b) Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters	261
3. Form und Bereitstellung des Verzeichnisses	262
4. Befreiung vom Führen des Verzeichnisses	262
5. Sanktionierung eines Verstoßes	264
B. Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)	264
I. Überblick	265
II. Regelung in der DS-GVO	266
1. Verpflichtung zur Datenschutz-Folgenabschätzung	266
2. Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung	266
a) Zweistufigkeit der Regelung in Art. 35 DS-GVO	267
b) Gegenstand der Datenschutz-Folgenabschätzung	267
c) Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung	267
3. Durchführung einer Datenschutz-Folgenabschätzung	269
4. Datenschutz-Folgenabschätzung im Rahmen von Gesetzgebungsverfahren	271
5. Verhaltensregelungen und Zertifizierungen	271
6. Übergangsregelung für die Datenschutz-Folgenabschätzung	272
7. Sanktionierung eines Verstoßes	272
C. Vorherige Konsultation (Art. 36 DS-GVO)	273
I. Überblick	273
II. Regelung in der DS-GVO	273
1. Verpflichtung zur Vorherigen Konsultation	273
2. Voraussetzungen und Inhalt einer Vorherigen Konsultation	273
a) Aufgabe des Verantwortlichen	275
b) Aufgabe der Aufsichtsbehörde	275
3. Übergangsregelung für die Vorherige Konsultation	276
4. Sanktionierung eines Verstoßes	276

§ 18. Telekommunikations- und Teledienstedatenschutzrecht	277
A. Datenschutzrichtlinie für elektronische Kommunikation (EK-DSRL)	278
B. Verhältnis der DS-GVO zur EK-DSRL und mitgliedstaatlichen Regelungen	280
I. Verhältnis der DS-GVO zur EK-DSRL	280
II. Verhältnis der DS-GVO zu mitgliedstaatlichen Datenschutz- bestimmungen	281
1. Datenschutzbestimmungen des TKG	282
2. Datenschutzbestimmungen des TTDSG	282
3. E-Commerce-Richtlinie	285
III. Zusammenfassung	286
C. Datenschutz nach dem TTDSG und dem TKG	286
I. Schutzbereich	286
1. Anwendungsbereich	286
2. Persönlicher Schutzbereich	286
II. Dienstespezifischer Anwendungsbereich	287
III. Verpflichteter Personenkreis	288
1. Diensteanbieter und geschäftsmäßiges Erbringen von Telekommunikationsdiensten	288
2. Abgrenzung zum Erbringen von Telekommunikations- diensten	288
3. Einordnung von OTT-Diensten	289
IV. Inhalt der Verpflichtung und Rechtmäßigkeitstatbestände	290
1. Informationspflichten	291
2. Einwilligung	291
3. Gesetzliche Rechtmäßigkeitstatbestände des TTDSG	291
a) Bestandsdaten	291
b) Verkehrs- und Nutzungsdaten	292
c) Dienst mit Zusatznutzen und Standortdaten	294
d) Einzelverbindungsnachweis	294
e) Weitere telekommunikations- und telemedienspezifische Regelungen	295
f) Technische Schutzmaßnahmen und Daten- und Informa- tionssicherheit	297
V. Schutz des Fernmeldegeheimnisses	297
VI. Telekommunikationsüberwachung und Vorratsdatenspeiche- rung	299
D. Datenschutz in den Telemedien	299

4. Abschnitt. Datensicherheit. Technischer/organisatorischer Datenschutz

§ 19. Sicherheit der Verarbeitung	304
A. Überblick	305
B. Verpflichteter und Inhalt der Verpflichtung	306
I. Verpflichteter	306
II. Inhalt der Verpflichtung	307
1. Gegenstand der Bewertung	307
2. Pflicht zu technischen und organisatorischen Maßnahmen (Abs. 1)	308

3. Kriterien zur Beurteilung der Angemessenheit des Schutzniveaus (Abs. 2)	310
4. Verhaltensregeln und Zertifizierungen (Abs. 3)	311
5. Verpflichtung der Personen mit Zugang zu personenbezogenen Daten	311
6. Sicherheit der Verarbeitung nach DS-GVO und IT-Sicherheit	312
III. Datenschutz als Grenze der Sicherheit der Verarbeitung	313
IV. Relevanz im Rahmen der Festsetzung einer Sanktion	314
V. Bußgeldsanktion	314
C. Weitere Regelungen	314
I. Telekommunikations- und telemedienrechtliche Spezialregelungen	314
II. Kritische Infrastrukturen	315
III. NIS-Richtlinie	316
VI. CybersecurityVO	317
§ 20. Datenschutz durch Technikgestaltung und Voreinstellung	319
A. Überblick über die historische Entwicklung	319
B. Überblick und Ziel	320
C. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung	320
I. Regelungsadressat des Art. 25 DS-GVO	321
II. Datenschutz durch Technikgestaltung (Data Protection by Design)	321
III. Datenschutzfreundliche Voreinstellung (Data Protection by Default)	323
IV. Genehmigte Zertifizierungsverfahren	323
V. Technisch-organisatorische Maßnahmen	324
VI. Relevanz im Rahmen der Festsetzung einer Sanktion	324
VII. Sanktionierung eines Verstoßes	325
D. Bewertung des Ansatzes	325

5. Abschnitt. Datenschutzkontrolle

§ 21. Interne (Selbst-)Kontrolle. Insbes. Datenschutzbeauftragter	326
A. Benennung eines Datenschutzbeauftragten	328
I. Unionsweite Benennung eines Datenschutzbeauftragten	329
1. Behörden und öffentliche Stellen	329
2. Benennungspflicht aufgrund der Kerntätigkeit	331
II. Pflicht zur Benennung eines Datenschutzbeauftragten nach mitgliedstaatlichem Recht	333
III. Freiwillige Benennung eines Datenschutzbeauftragten	335
IV. Qualifikation des Datenschutzbeauftragten	336
V. Modalitäten der Benennung eines Datenschutzbeauftragten	338
VI. Sanktion der Nichtbenennung	339
B. Stellung des Datenschutzbeauftragten	339
I. Einbeziehung des Datenschutzbeauftragten	340
II. Pflicht zur Unterstützung des Datenschutzbeauftragten	341
III. Weisungsfreiheit	342

IV. Benachteiligungs- und Abberufungsverbot	342
V. Direkte Berichtslinie	343
VI. Anrufungsrecht der betroffenen Person	343
VII. Pflicht zur Geheimhaltung und Vertraulichkeit	344
VIII. Weitere Aufgaben des Datenschutzbeauftragten	344
IX. Verbot der Interessenkollision	345
C. Aufgaben des Datenschutzbeauftragten	346
I. Unterrichtung und Beratung	346
II. Überwachung der Einhaltung des Datenschutzrechts	347
1. Überwachungs- und Handlungssystem des Verantwortlichen	347
2. Pflicht des Datenschutzbeauftragten	348
III. Beratung im Zusammenhang mit der Datenschutz-	
Folgenabschätzung	349
IV. Zusammenarbeit mit und Ansprechpartner der Aufsichts-	
behörde	349
V. Risikobasierter Ansatz	350
D. Datenschutz durch Mitarbeitervertretung	350
§ 22. Fremdkontrolle	353
A. Allgemeines	353
B. System der Datenschutzaufsicht	354
I. Allgemeine Datenschutzbehörden	354
1. Europäischer Datenschutzbeauftragter	354
2. Mitgliedstaatliche Datenschutzaufsichtsbehörden	355
a) Bundesbeauftragter für den Datenschutz und die	
Informationsfreiheit (BfDI)	355
b) Landesdatenschutzbeauftragte	355
II. Koordinierungsgremien und Netzwerke	355
1. Europäischer Datenschutzausschuss	356
2. Koordinierungsgremien bundesstaatlicher Datenschutz-	
aufsicht	356
a) Konferenz der Datenschutzbeauftragten des Bundes und	
der Länder	356
b) Düsseldorfer Kreis	356
c) Vertretung im Europäischen Datenschutzausschuss	357
III. Sektorielle Aufsicht	357
1. Medien	358
2. Kirchen und Religionsgemeinschaften	358
3. Berufsgeheimnissen unterliegende Bereiche	359
4. Gerichte	359
IV. Europäische Kommission	360
V. „Konkurrierende“ Aufsichtsbehörden	360
VI. Stiftung Datenschutz	361
C. Zuständigkeit der Aufsichtsbehörden	361
I. Europarechtliches Territorialitätsprinzip	361
II. Innerstaatliche Zuständigkeitsabgrenzung von BfDI und	
Landesdatenschutzbehörden	362
D. Stellung der Aufsichtsbehörden	363
I. „Völlige Unabhängigkeit“ der Aufsichtsbehörden	363
II. Ausstattung der Aufsichtsbehörde	364

1. Personelle Ausstattung	364
2. Sachliche Ausstattung	364
3. Finanzielle Ausstattung	364
III. Leitung der Aufsichtsbehörde	365
1. Persönliche und fachliche Anforderungen	365
2. Wahl und Ernennungsverfahren	365
3. Amtszeit	365
4. Verschwiegenheitspflicht	366
5. Aussageverweigerungsrecht	366
E. Handeln der Aufsichtsbehörde	367
I. Aufgaben der Aufsichtsbehörde	367
1. Klassische Aufsichtstätigkeit	367
2. Informationelle Aufgaben	367
a) Hinweise an Betroffene, Verantwortliche und die Öffentlichkeit	367
b) Tätigkeitsbericht	367
3. Beratende Aufgaben	368
4. Untersuchungen	368
5. Beobachtende Aufgabe	368
6. Beschwerdestelle	368
7. Datenschutz Zertifizierung	368
8. Genehmigungen	369
9. Sonstige Aufgaben	369
10. Aufgaben nach JI-RL	369
II. Befugnisse der Aufsichtsbehörde	369
1. Untersuchungsbefugnisse	369
2. Abhilfebefugnisse	370
3. Genehmigungsbefugnisse	371
4. Beratende Befugnisse	371
5. Weitere Befugnisse	371
6. Befugnisse nach der JI-RL	371
7. Umsetzung in mitgliedstaatliches Recht	372
8. Ausübung der Befugnisse	372
F. Zusammenarbeit der Aufsichtsbehörden	372
I. Formen der Zusammenarbeit	372
1. Kooperationsgebote und Amtshilfe	372
2. Kohärenzverfahren	374
3. Dringlichkeitsverfahren	375
II. Zusammenarbeit und Unabhängigkeit	376
III. Netzwerk und Legitimation	377
G. Rechtsschutz gegen Aufsichtsbehörden	377
I. Vorgaben der DS-GVO und verwaltungsgerichtlicher Rechts- schutz	377
II. Staatshaftung	379
III. Entscheidungen des Europäischen Datenschutzausschusses	379

6. Abschnitt. Haftung, Sanktionen

§ 23. Haftung	380
A. Schadenersatz	380

I. Anwendbare Normen	381
1. Datenschutzrecht	381
2. Zivilrechtliche Haftung	382
a) Vertragliche und vorvertragliche Ansprüche	382
b) Deliktische Ansprüche	382
3. Öffentlich-rechtliche Haftungsansprüche	383
II. Anspruchsberechtigter	383
III. Anspruchsverpflichtete	383
IV. Anspruchsvoraussetzungen	384
1. Rechtswidriges Handeln (Datenschutzverstoß)	384
2. Verschulden	384
3. Kausalität	385
4. Schaden	385
V. Modifikationen des Anspruchs	387
VI. Schadenersatzhöhe	387
VII. Beweislast	388
VIII. Keine Versicherungspflicht	389
IX. Rechtsweg und Geltendmachung	389
X. Übertragbarkeit, Vererblichkeit	390
Exkurs: Bereicherungsausgleich	390
B. Verbandsklage	391
C. Wettbewerbliche Haftung	392
I. Lauterkeitsrecht	392
1. Anwendungsbereich des Wettbewerbsrechts	392
2. Datenschutzverstoß als Wettbewerbsverstoß	393
a) Wettbewerbsbezug des Datenschutzrechts	393
b) Wettbewerbsrechtliche Unlauterkeit	395
3. Geltendmachung/Rechtsfolgen	396
II. Datenschutzverstöße im Kartellrecht	396
§ 24. Sanktionen bei Datenschutzverstößen	398
A. Rechtstaatliche Grenzen des Datenschutzsanktionsrecht	399
I. Verweisungstechnik	399
II. Unverständlichkeit	400
III. Fehlende Bestimmtheit	401
IV. Folgen von Unionsrechtswidrigkeit oder Verfassungswidrig- keit	401
B. Datenschutzordnungswidrigkeiten	402
I. Bußgeldtatbestände	403
1. Verstoß gegen Pflichten der Verantwortlichen bzw. der Auftragsverarbeiter	403
2. Verstöße gegen Pflichten der Zertifizierungs- und Über- wachungsstellen	403
3. Verstöße im Rahmen der konkreten Verarbeitung	404
4. Behinderung der Aufsichtsbehörden	404
5. Weitere Bußgeldtatbestände nach dem BDSG	404
II. Täter	405
III. Tatbegehungsformen	405
IV. Bußgeldverfahren	406
V. Sanktionen	407

1. Verwarnungen	407
2. Bußgeld	408
a) Höhe des Bußgelds	408
b) Maßstäbe der Bußgeldbemessung	409
C. Datenschutzstraftaten	410
I. Strafnormen des allgemeinen Datenschutzrechts	411
II. Strafnormen im bereichsspezifischen Datenschutzrecht	412
III. Allgemeines Strafrecht	413
Sachverzeichnis	415